V-Valley

enhancing your business

Mejores prácticas para la seguridad en Azure

Rafael Barbas Melchor

Technical Presales

rafael.barbas@v-valley.com

David Pestaña Garrido

BDM Soluciones Microsoft CLOUD

david.pestana@v-valley.com

V-Valley
enhancing your business

Agenda

Procedimientos de seguridad operativa en Azure

¿Cuál es el enfoque de Microsoft?

V-Valley
enhancing your business

Microsoft Zero Trust

Un **enfoque proactivo** de la **seguridad** que **utiliza controles adaptativos** y una **verificación continua** para **prevenir** y **responder** a las **amenazas** con **mayor rapidez y eficacia**

Basado en:

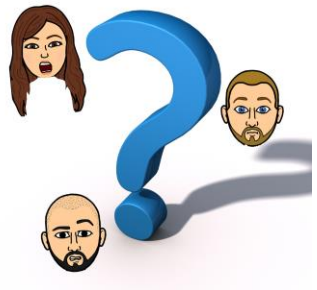
- **Verificación Explicita.**
- **Uso de mínimos privilegios.**
- **Asumir las brechas.**

Procedimientos de seguridad operativa

¿Qué deberíamos hacer para mejorar nuestra seguridad operativa?

Definir e implementar procedimientos recomendados que *un fabricante líder en el mercado de la seguridad* como *Microsoft nos da para* **mejorar nuestra postura de seguridad**

Recomendaciones: https://learn.microsoft.com/es-es/azure/security/fundamentals/operational-best-practices



¿Qué entiende Microsoft por eso de la "seguridad operativa"?

Son los **servicios**, **controles** y **características disponibles** que los usuarios tienen disponibles para **proteger** sus **datos**, **Apps** y **otros recursos** desplegados **en Azure**

¿En qué está basada la seguridad operativa disponible en Azure?

Se engloba en el **marco** que incluye el **conocimiento adquirido** a través de diversas **funcionalidades exclusivas de Microsoft**, *tales como*, el ciclo de vida de desarrollo de seguridad (SDL), el programa Microsoft Security Response Center y un **conocimiento en profundidad del panorama de amenazas de ciberseguridad**.

Microsoft Security Response Center

Protection, detection, and response

The **Microsoft Security Response Center** is part of the defender community and on the front line of security response evolution. For over twenty years, we have been engaged with security researchers working to protect customers and the broader ecosystem.

Report an issue

Security Update Guide

Bounty programs

Who we are

Blogs

V-Valley
enhancing your business

Agenda

Procedimientos de seguridad operativa

Gestionar/supervisar contraseñas de usuario

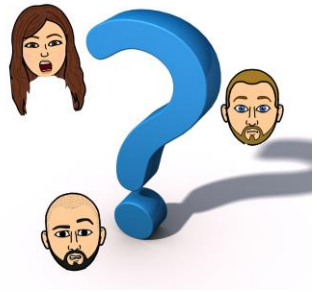
Tener el nivel adecuado de protección de contraseñas en la nube

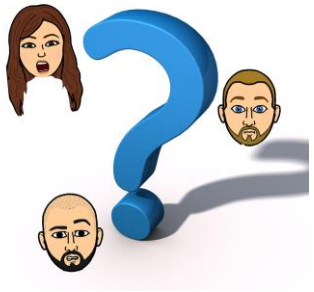
Prácticas recomendadas por Microsoft, dirigidas a usuarios de las plataformas de identidad de Microsoft *(Azure Active Directory, Active Directory y cuenta de Microsoft).*

Microsoft Password Guidance

Supervisar las acciones sospechosas relacionadas con nuestros usuarios

Supervisar tanto los usuarios en riesgo **como** los inicios de sesión en riesgo mediante los **informes de seguridad de Azure AD**.





Detectar y corregir de forma automática las contraseñas de alto riesgo

Con Azure AD Identity Protection *(Azure AD Premium P2)* podemos **detectar** posibles **vulnerabilidades**, **configurar respuestas automáticas** a **acciones sospechosas detectadas** e **investigar incidentes** y tomar **medidas adecuadas para resolverlos**

https://www.microsoft.com/en-us/research/publication/password-guidance/

Password Guidance

Robyn Hicock
May 2016

Download BibTex

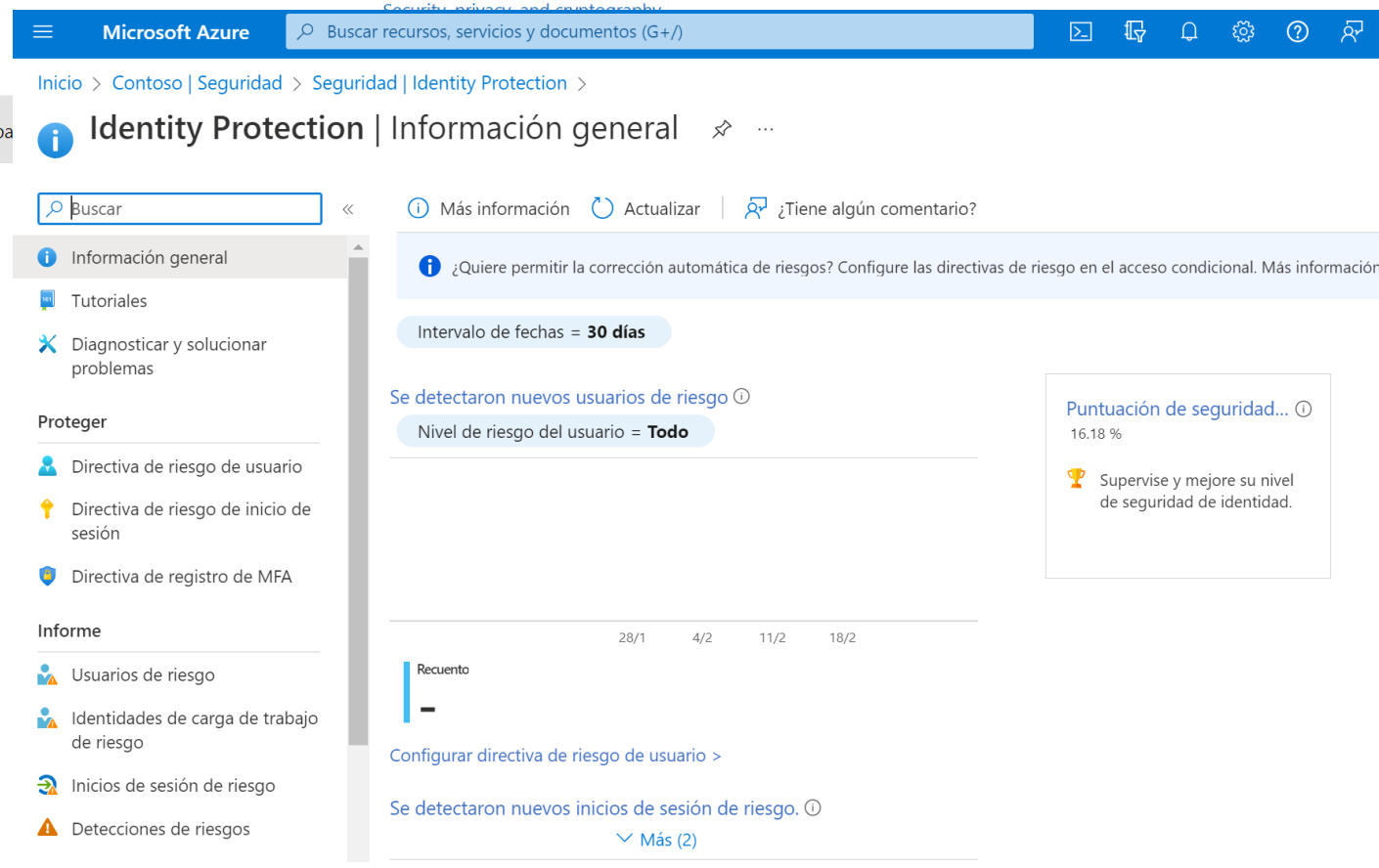
View Publication

This paper provides Microsoft's recommendations for password management based on current research and lessons from our own experience as one of the largest Identity Providers (IdPs) in the world. It covers recommendations for end users and identity administrators.

Microsoft sees over 10 million username/password pair attacks every day. This gives us a unique vantage point to understand the role of passwords in account takeover. The guidance in this paper is scoped to users of Microsoft's identity platforms (Azure Active Directory, Active Directory, and Microsoft account) though it generalizes to other platforms.

Research Areas

Security, privacy, and cryptography



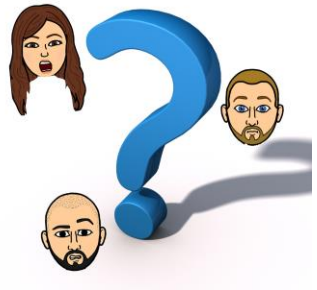
Gobierno de suscripciones en nuestra tenant

¿Cómo puedo tener el control de todas mis suscripciones?

Usando un **grupo de administración raíz** *(NO crear otros grupos de administración en el directorio raíz)* para asignar **elementos de seguridad aprobados por nuestra empresa** *(directivas, permisos, etc)* y aplicarlos de **manera uniforme a todos los recursos de Azure** estén en la suscripción que estén

¿Qué elementos de seguridad se aplicarán a toda la empresa?

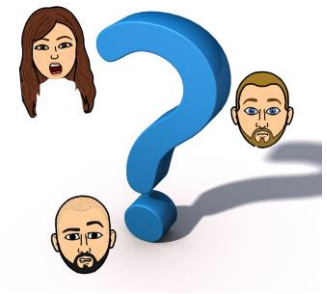
Tenemos que **definir cuidadosamente que elementos comunes** aplicaremos en todas las suscripciones de nuestro **grupo de administración raíz**



Planificar y probar cualquier cambio administrativo que realicemos a este nivel

Ahí que tener **mucho cuidado** con los "*falsos positivos*" que podamos tener cuando implementemos **nuestros cambios a nivel del grupo de administración raíz**, ya que estos afectarán a todos los recursos desplegados en *nuestras suscripciones de Azure*

Blueprints

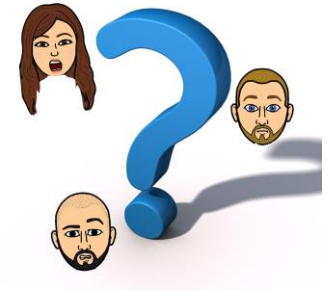


¿Cómo puedo tener el control de todas mis suscripciones?

El servicio Azure Blueprints permite a los *arquitectos Cloud* y **personal de TI definir** un **conjunto repetible de recursos de Azure a implementar** y que **cumplen con los estándares**, **patrones** y **requisitos de la empresa**.

¿Para que los puedo usar?

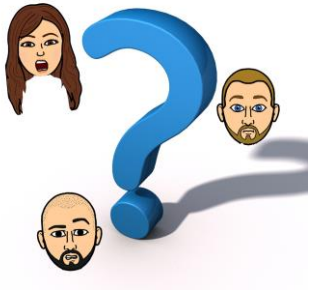
Azure Blueprints permite a los **equipos de desarrollo aprovisionar y crear rápidamente entornos con un conjunto de componentes integrados**, con la confianza de que se crean de acuerdo a la normativa de la organización.



¿En que se diferencia Azure Blueprints de las plantillas ARM de despliegue?

Azure Blueprints crea una **relación continúa** entre la **definición del plano técnico** *(lo que debe implementar)* y su **asignación** *(lo que se ha implementado)*. Con esta relación tenemos un **seguimiento** y **auditoría** de *cada implementación*. **Azure Blueprints** también puede actualizar varias suscripciones a la vez que se rigen por el mismo plano técnico.

Supervisar los servicios de almacenamiento



Detectar cambios inesperados en nuestras Apps

Tenemos que **supervisar continuamente el almacenamiento que usa** nuestra **App** para detectar cualquier **cambio inesperado de comportamiento** *(tiempos de respuesta más lentos, etc)*.

¿Cómo podemos detectar problemas en nuestras Apps?

Con **Analytics** podríamos **detectar** de forma temprana **posibles errores** en nuestras **Apps desplegadas en Azure**.

Por poner un ejemplo, con la herramienta Azure Storage Analytics obtendremos **métricas** de los **datos almacenados** en nuestras **cuentas de almacenamiento** de Azure.

Microsoft recomienda usar estos datos para hacer un **seguimiento de solicitudes**, **analizar tendencias de uso** y **diagnosticar problemas** con nuestras **cuentas de almacenamiento**.

V-Valley
enhancing your business

Agenda

Prevenir/detectar/responder a las amenazas

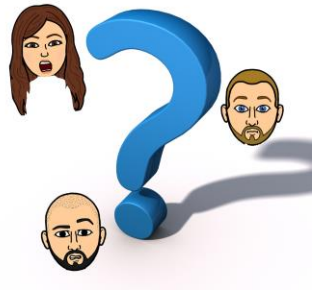
Microsoft Defender for Cloud

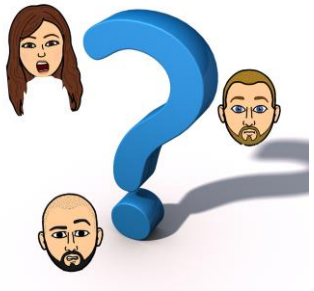
¿Cómo puedo tener el control de la seguridad sobre los objetos en Azure?

Microsoft Defender for Cloud ayuda a **detectar**, **evitar** y **responder** contra **amenazas**, dándonos **más visibilidad** y **control** sobre la **seguridad** de nuestros recursos de Azure.

¿Qué nos ofrece Microsoft Defender for Cloud?

Identificar y **corregir vulnerabilidades de seguridad**, aplicar **controles de acceso** y de **App** para **bloquear actividades malintencionadas**, detectar **amenazas** mediante análisis e inteligencia global y **responder rápidamente** en caso de sufrir un **ataque**



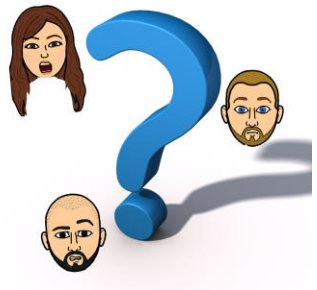


Tener la información de un solo vistazo

Defender for Cloud nos permite **visualizar desde un único lugar el estado de seguridad de todos nuestros recursos on-premise**, en **Azure** y/o en **otras Clouds**.
Comprobaremos sí se han **configurado/implementado** nuestros **controles** e **identificar** *cualquier recurso que demande atención*

Microsoft Defender for Endpoint

¿Microsoft Defender for Cloud se integra con Defender for Endpoint?
Sí, proporcionándonos **funcionalidades completas de detección y respuesta EDR**.
Podemos **detectar anomalías y vulnerabilidades**, **respondiendo** a **ataques avanzados** en **nuestros servidores supervisados por Defender for Cloud** *(por ejemplo)*



Secure Score

Revisar la puntuación de nuestra implementación en Azure, para obtener **recomendaciones** resultantes de las **iniciativas y directivas de Azure integradas en Microsoft Defender for Cloud**.
Recomendaciones sobre posibles riesgos *(actualizaciones de seguridad, protección de puntos de conexión, cifrado, configuraciones de seguridad, ausencia de WAF, máquinas virtuales conectadas a Internet, etc)*

Secure Score se basa en **controles del Centro de seguridad de Internet (CIS)** y nos permite realizar **pruebas comparativas de la seguridad de Azure** de nuestra empresa con otros orígenes externos *(empresas que realizar una actividad económica parecida la nuestra, con mismo número de usuarios, etc)*.

Inicio
Incidentes y alertas
Búsqueda
Acciones y envíos
Análisis de amenazas
Puntuación de seguridad
Centro de aprendizaje
Pruebas
Catálogo de asociado

Activos
Dispositivos
Identidades

Extremos
Administración de vulnerabi...
Asociados y API

Inicio

Recorrido guiado
Novedades
Comunidad
Agregar tarje

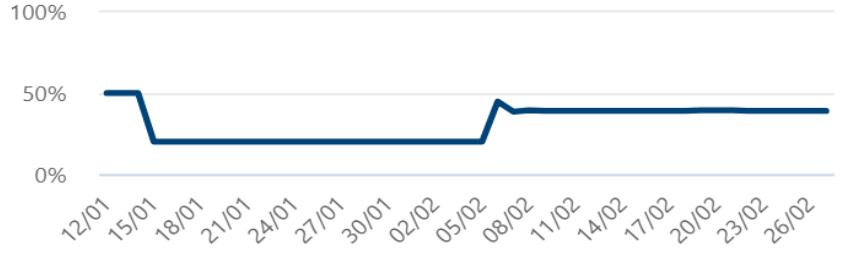
Microsoft Secure Score

Puntuación de seguridad: 39...

103.06/264 puntos obtenidos

La puntuación de seguridad de Microsoft es una representación de la posición de seguridad de su organización, y una oportunidad de mejorarla.

Último cálculo de la puntuación: 27/02

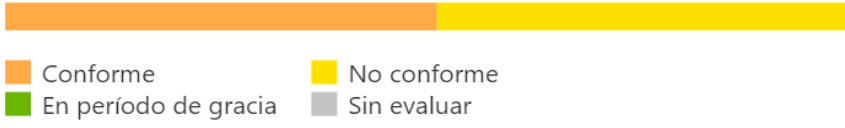


Identidad	**16.18%**
Datos	**77.78%**
Dispositivo	**100%**

Cumplimiento de dispositivos

50 % no conformes.

Estado de cumplimiento del dispositivo de Intune



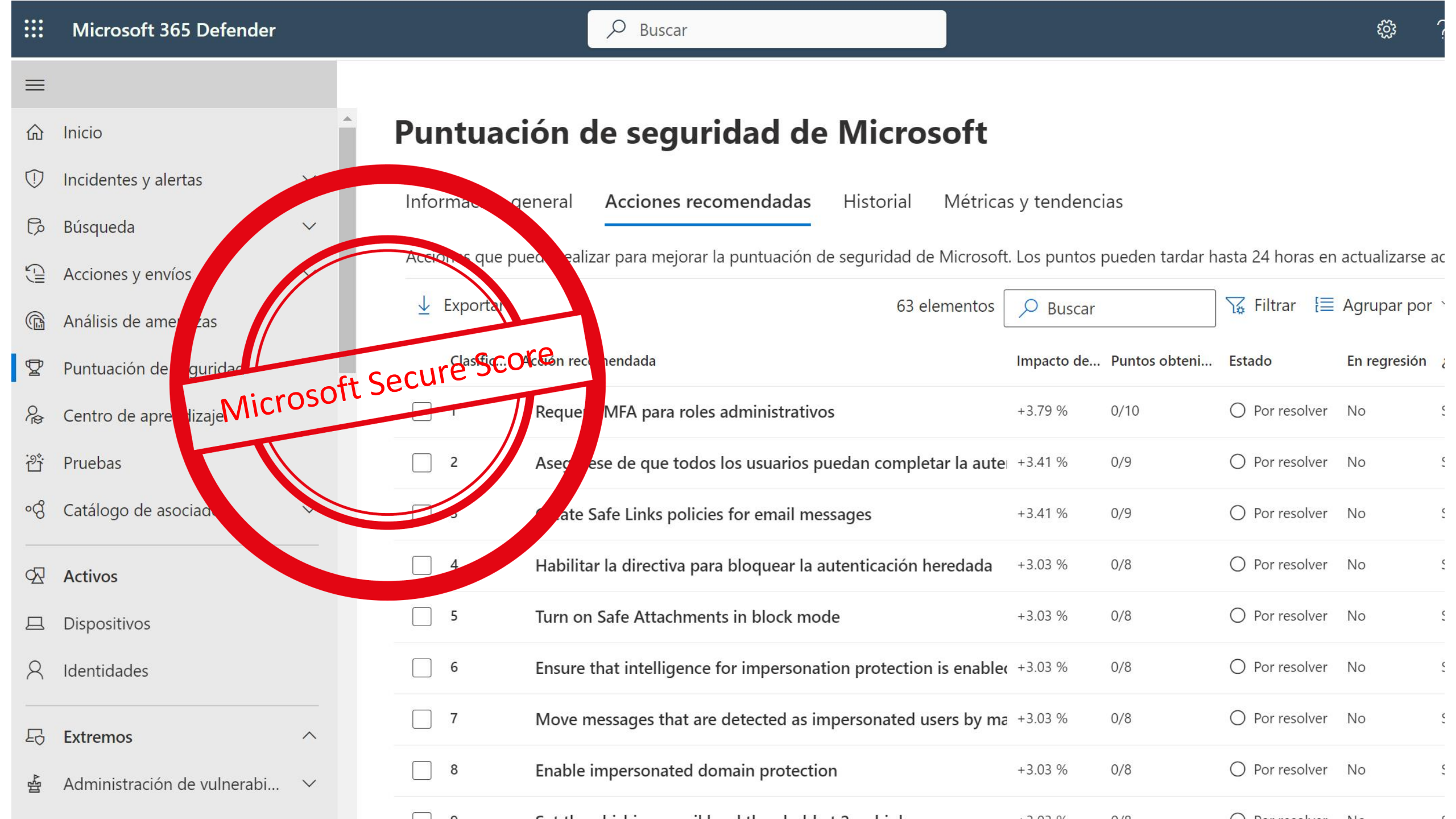
Conforme
No conforme
En período de gracia
Sin evaluar

Ver detalles

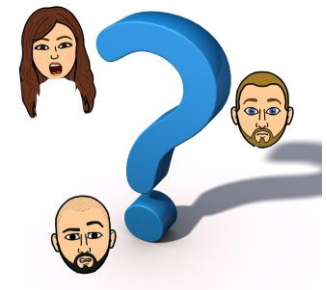
Dispositivos con malware activo

Malware corregido

El malware encontrado en los dispositivos se ha corregido correctamente


Microsoft 365 Defender
Buscar
Inicio
Incidentes y alertas
Búsqueda
Acciones y envíos
Análisis de ame zas
Puntuación de guridad
Centro de apre dizaje
Pruebas
Catálogo de asociad
Activos
Dispositivos
Identidades
Extremos
Administración de vulnerabi...
Puntuación de seguridad de Microsoft
Informac general
Acciones recomendadas
Historial
Métricas y tendencias
Acciones que pued ealizar para mejorar la puntuación de seguridad de Microsoft. Los puntos pueden tardar hasta 24 horas en actualizarse ac
Exportar
63 elementos
Buscar
Filtrar
Agrupar por
Clasific...
Acción rec endada
Impacto de...
Puntos obteni...
Estado
En regresión
1 Reque MFA para roles administrativos +3.79 % 0/10 Por resolver No
2 Aseg ese de que todos los usuarios puedan completar la aute +3.41 % 0/9 Por resolver No
3 ate Safe Links policies for email messages +3.41 % 0/9 Por resolver No
4 Habilitar la directiva para bloquear la autenticación heredada +3.03 % 0/8 Por resolver No
5 Turn on Safe Attachments in block mode +3.03 % 0/8 Por resolver No
6 Ensure that intelligence for impersonation protection is enable +3.03 % 0/8 Por resolver No
7 Move messages that are detected as impersonated users by ma +3.03 % 0/8 Por resolver No
8 Enable impersonated domain protection +3.03 % 0/8 Por resolver No
Microsoft Secure Score

Microsoft Sentinel

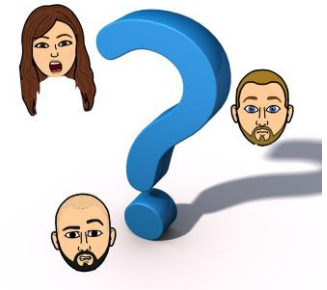


¿Qué es Microsoft Sentinel (SIEM)?

Es una **solución** de **administración de eventos** e **información de seguridad** *(SIEM)* y **respuesta automatizada de orquestación de seguridad** *(SOAR)* **escalable** y **nativa Cloud**.
Análisis de seguridad inteligentes frente a **amenazas vía detección de alertas**, **visibilidad de amenazas**, **búsqueda proactiva** y **respuesta automatizada** antes amenazas

Podemos habilitar la integración nativa con…

Podemos **integrarnos con el resto de soluciones de Microsoft** Defender for Cloud, Microsoft Defender for Endpoint, etc



¿Integraciones de Microsoft Sentinel con otros servicios?

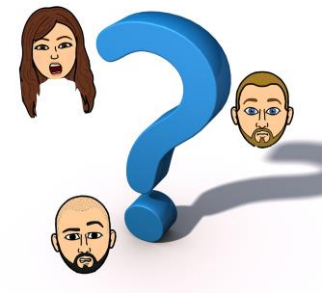
Podemos **integrar tanto soluciones de Microsoft** *(Azure Active Directory, Azure Web Application Firewall, Azure Monitor)* **como de terceros** *(prácticamente con cualquier otro tipo de origen de dato)*

V-Valley
enhancing your business

Agenda

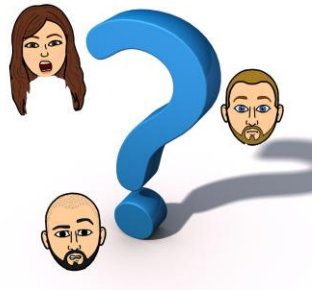
Supervisar nuestros elementos de Red

Ciclo de Vida de las Apps en Azure



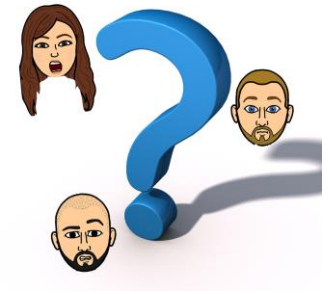
¿En qué metodología nos basamos?

La **seguridad** tiene que estar **en el centro durante todo el ciclo de vida de una App**, desde *su diseño e implementación hasta la implementación y las operaciones*.
Para **proteger** un **Servicio/App en Azure** tenemos que *conocer bien la arquitectura de la App* y centrarlas en los cinco pilares de la calidad del software *(Recomendado por Microsoft)*



¿Ciclo de vida del Desarrollo de la Seguridad (SDL)?

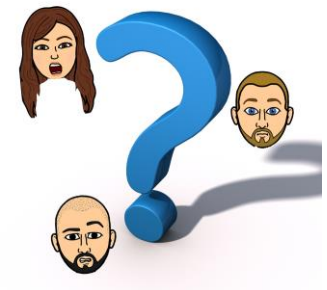
La **seguridad** y la **privacidad** están **integradas en la plataforma Azure**, comenzando por el ciclo de vida del desarrollo de la seguridad (SDL). El **SDL** aborda la **seguridad** en **cada fase de desarrollo e actualización continua seguro** de la misma en todo su ciclo de vida



Ponme un ejemplo… ¿Qué podemos hacer para frenar ataques DDoS?

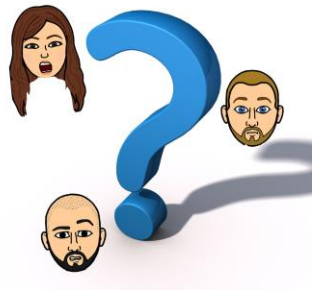
Podemos **escalar** *los objetos que forman nuestras Apps* **horizontalmente** *(varias instancias en Azure App Service, Conjunto de disponibilidad en VMs)*. Podemos usar **AGSs** *(grupos de seguridad a nivel de Apps)*, **etiquetas de servicio**, **IPs privadas**, **Puntos de conexión de servicio**, **Azure Policy**, **Locks**, etc.

Azure Policy



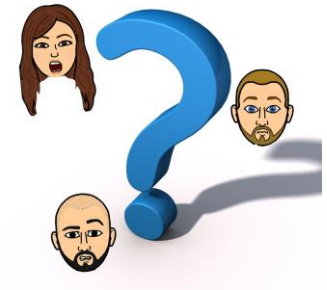
¿Qué es Azure Policy?

Es un servicio de Azure que **crea**, **asigna** y **administrar directivas**. Estas directivas **aplican reglas** y **efectos a los recursos**, para **cumplir con los estándares corporativos y los SLAs**. **Evaluación continua de** los **recursos** que **incumplen las directivas asignadas** y los **roles de los usuarios**, dentro de nuestra empresa que **deben crearlos**, **implementarlos** y **evaluar su impacto**



¿Qué nos aporta Azure Policy?

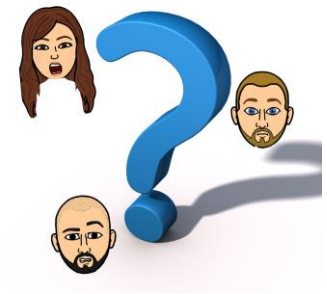
Es la **representación técnica** de las **directivas escritas de la empresa**. Para reducir la confusión y aumentar la coherencia, asigne todas las definiciones de Azure Policy a las directivas de la organización. Primero con **efecto Audit** y una vez que **comprobemos** que **todo funciona como queremos** y *sólo entonces* lo cambiaremos por los **efectos deny y/o remediate**



Azure Locks… ¿Puedo bloquear el acceso a los objetos de Azure?

Como **administradores**, podemos **bloquear** una **suscripción**, un **grupo de recursos** o un **recurso** concreto *en el portal de Azure* para **protegerlos** contra **eliminaciones** y **modificaciones accidentales** de *nuestros usuarios*. El **bloqueo invalida** los **permisos** que el *usuario* pueda tener.

Supervisar nuestra conectividad

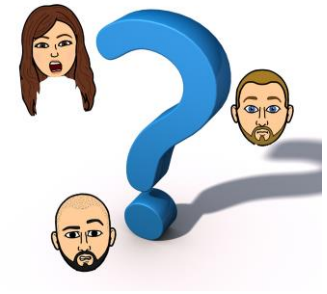


¿Cómo puede saber que pasar en la red, desde o a Azure?

Con Azure Network Watcher es un **servicio regional**. Con herramientas de **diagnóstico y visualización** para **supervisar y diagnosticar problemas** en nuestra **red** tanto **hacia y desde Azure**

Logs del tráfico de red que viajan a través de nuestros NSGs

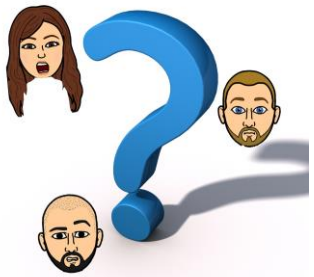
Ver al detalle los patrones de tráfico de red mediante los registros de flujo del grupo de seguridad de red. La *información de los registros de flujo le ayuda a recopilar datos para el cumplimiento, la auditoría y la supervisión del perfil de seguridad de red*.



¿Problemas de conexión y con nuestra VPN?

Con **Network Watcher** podemos diagnosticar los problemas más comunes de conexión y VPN Gateway. No solo puede **identificar el problema**, **sino** también usar **registros detallados para investigar más allá**.

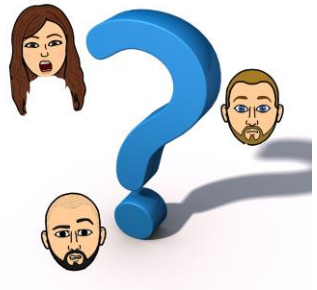
Valores predeterminados de seguridad en Azure Active Directory



¿Microsoft habilita alguna medida de seguridad cuándo creamos una tenant?

Sí, *Microsoft* en el **momento de la creación de una nueva tenant**, que **implementa por defecto una serie de medidas predeterminadas de seguridad a nivel de Azure Active Directory**. Para empresas que **no saben cómo ni por dónde empezar** pero quieren **más seguridad** y que usan las **licencias gratuitas de Azure Active Directory**.

¿Por qué y cuáles son los valores predeterminados implementados por defecto?



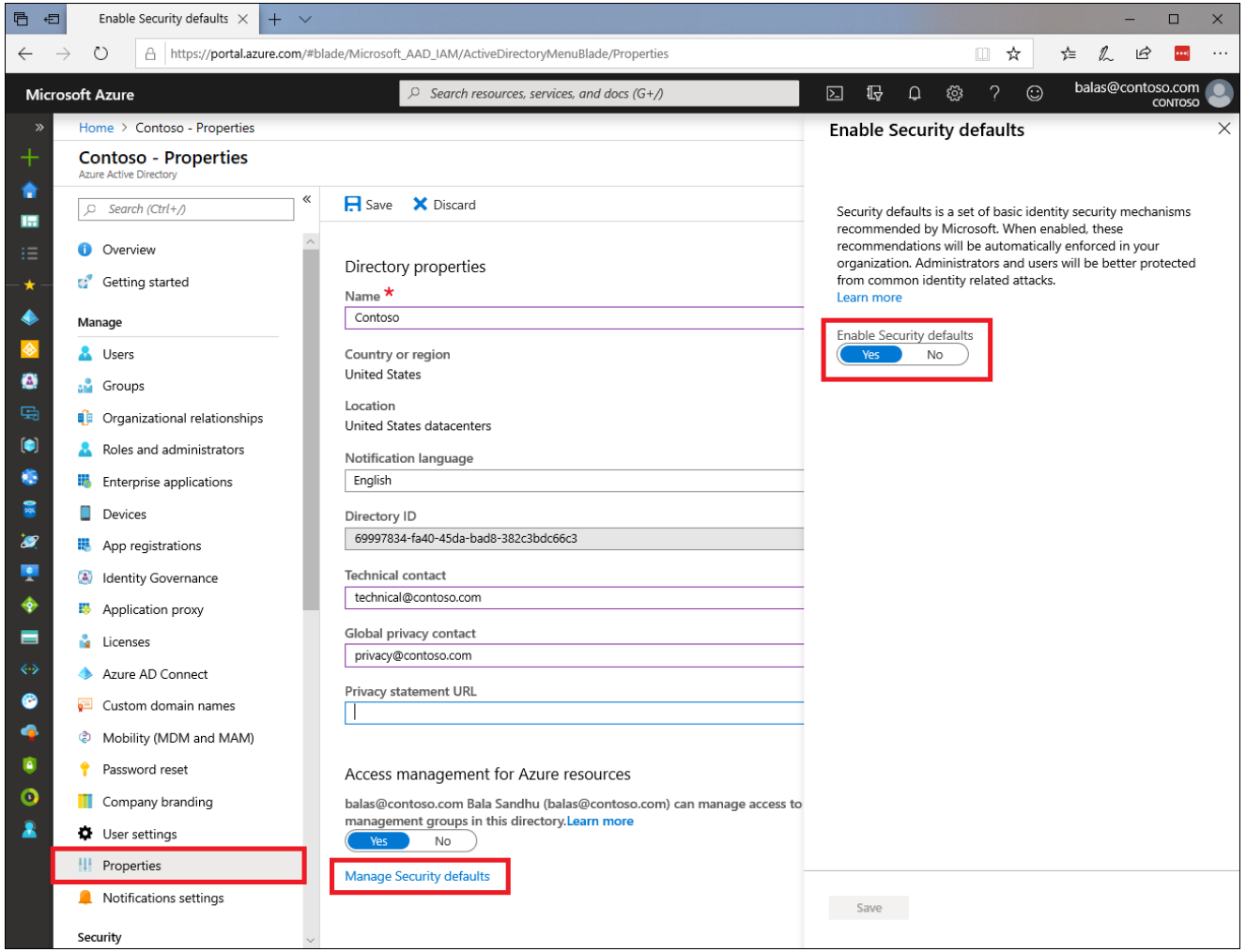
Los valores predeterminados de seguridad **nos dan protección contra ataques** de **identidad** con opciones preconfiguradas por *Microsoft*:

- **Exigir** que **todos los usuarios** se **registren** en **Azure AD Multi-Factor Authentication**.
- **Exigir** que los **administradores** realicen la **autenticación multifactor**.
- **Exigir** que los **usuarios** realicen la **autenticación multifactor cuando sea necesario**.
- **Bloquear** los **protocolos de autenticación heredados**.
- **Proteger las actividades con privilegios** *(p.e. El acceso a Azure Portal, etc)*.

Valores predeterminados de seguridad en Azure Active Directory

¿Cómo podemos **habilitar** los **valores de seguridad predeterminados** en nuestro *Azure Active Directory*?:

1. *Inicie sesión* en Azure Portal como administrador de seguridad, administrador de acceso condicional o administrador global.
2. Vaya a **Azure Active Directory** > **Propiedades**.
3. Seleccione **Administrar valores predeterminados de seguridad**.
4. Establezca **Habilitar valores predeterminados de seguridad** en **Sí**.
5. Seleccione **Guardar**.



URL: https://learn.microsoft.com/es-es/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#enabling-security-defaults

Procedimientos recomendados de seguridad

Para diseñadores, arquitectos, desarrolladores que compilen e implementen soluciones seguras de Azure.

- Servicios en la nube de Microsoft y seguridad de red
- Procedimientos recomendados para la seguridad de las bases de datos de Azure
- Procedimientos recomendados de cifrado y seguridad de datos en Azure
- Procedimientos recomendados de administración de identidades y la seguridad del control de acceso en Azure
- Procedimientos recomendados de seguridad de la red de Azure
- Procedimientos recomendados de seguridad operativa de Azure
- Procedimientos recomendados de PaaS de Azure
- Procedimientos recomendados de seguridad de Azure Service Fabric
- Procedimientos recomendados de seguridad para las máquinas virtuales de Azure
- Implementación de una arquitectura de red híbrida segura en Azure
- Procedimientos recomendados de seguridad de Internet de las cosas
- Protección de bases de datos PaaS en Azure
- Protección de aplicaciones web y móviles PaaS con Azure App Service
- Protección de aplicaciones web y móviles PaaS con Azure Storage
- Procedimientos de seguridad recomendados para cargas de trabajo de IaaS de Azure

Thank you

GRAZIE • GRACIAS • OBRIGADO • DANKE • MERCI • 감사 • 謝謝 • 感謝

V-Valley is the Advanced Solutions Distributor of the Esprinet Group

V-Valley | esprinet

Rafael Barbas Melchor
Technical Presales
rafael.barbas@v-valley.com

David Pestaña Garrido
BDM Soluciones Microsoft CLOUD
david.pestana@v-valley.com