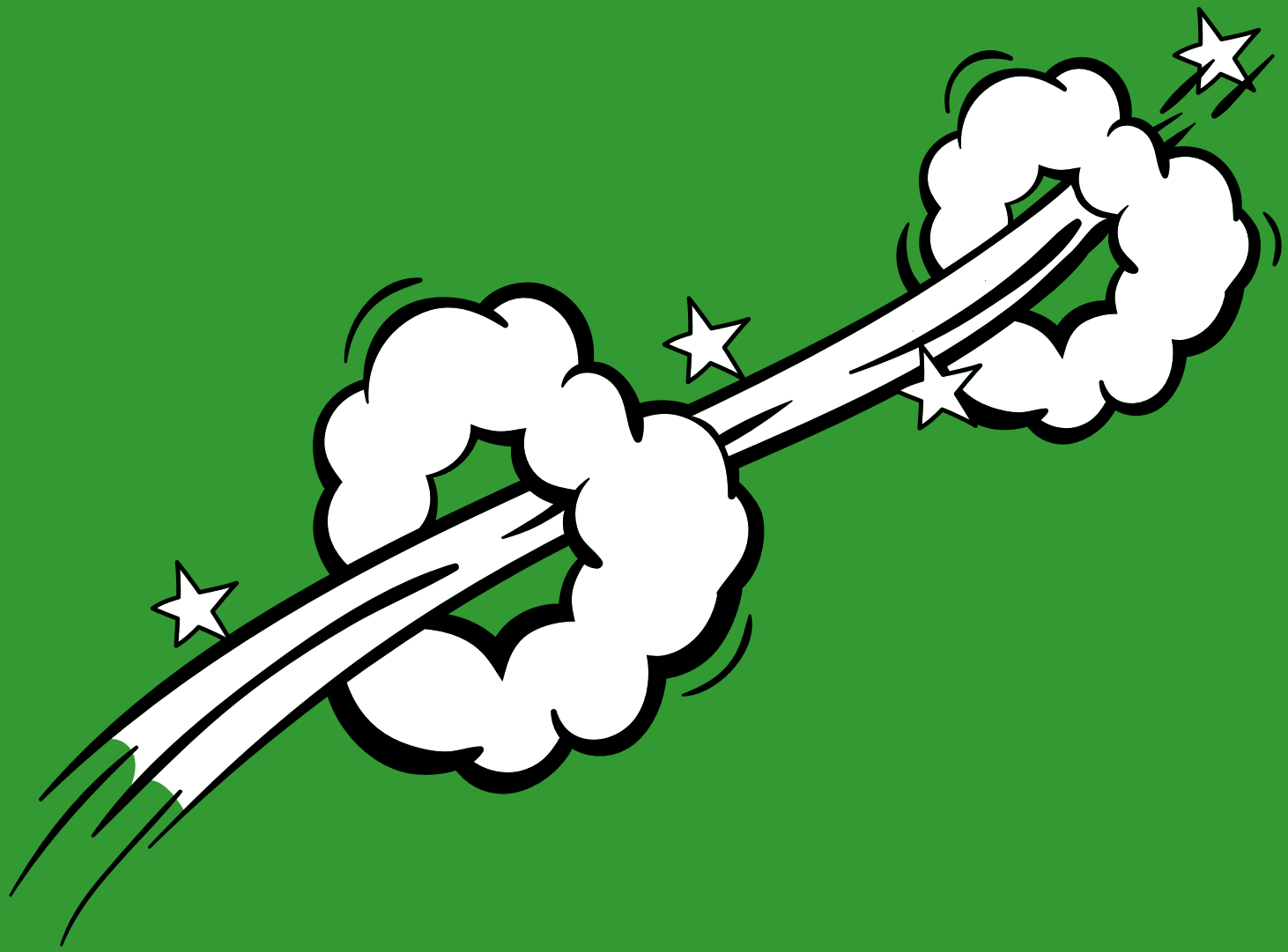
LOS IMPRESCINDIBLES

SEGURIDAD EN AZURE Y OFFICE 365

encamina



En el mundo de la tecnología no hay nada más vulnerable que la **seguridad**. Las organizaciones se ponen en nuestras manos para que las protejamos, identifiquemos posibles brechas y respondamos rápidamente ante una amenaza…¡menudo reto!

Alberto Díaz, **Dani Alonso** y **Pablo Ortiz** se han enfrentado miles de veces a los villanos disfrazados de malwares, ransomwares y ataques varios, y los han combatido con la ayuda de los sistemas de **Protección de la Información** basados en Azure.

En esta nueva colección de *Imprescindibles* te cuentan cómo puedes hacerlo tú también.

Happy Codding! :)

Índice de contenidos

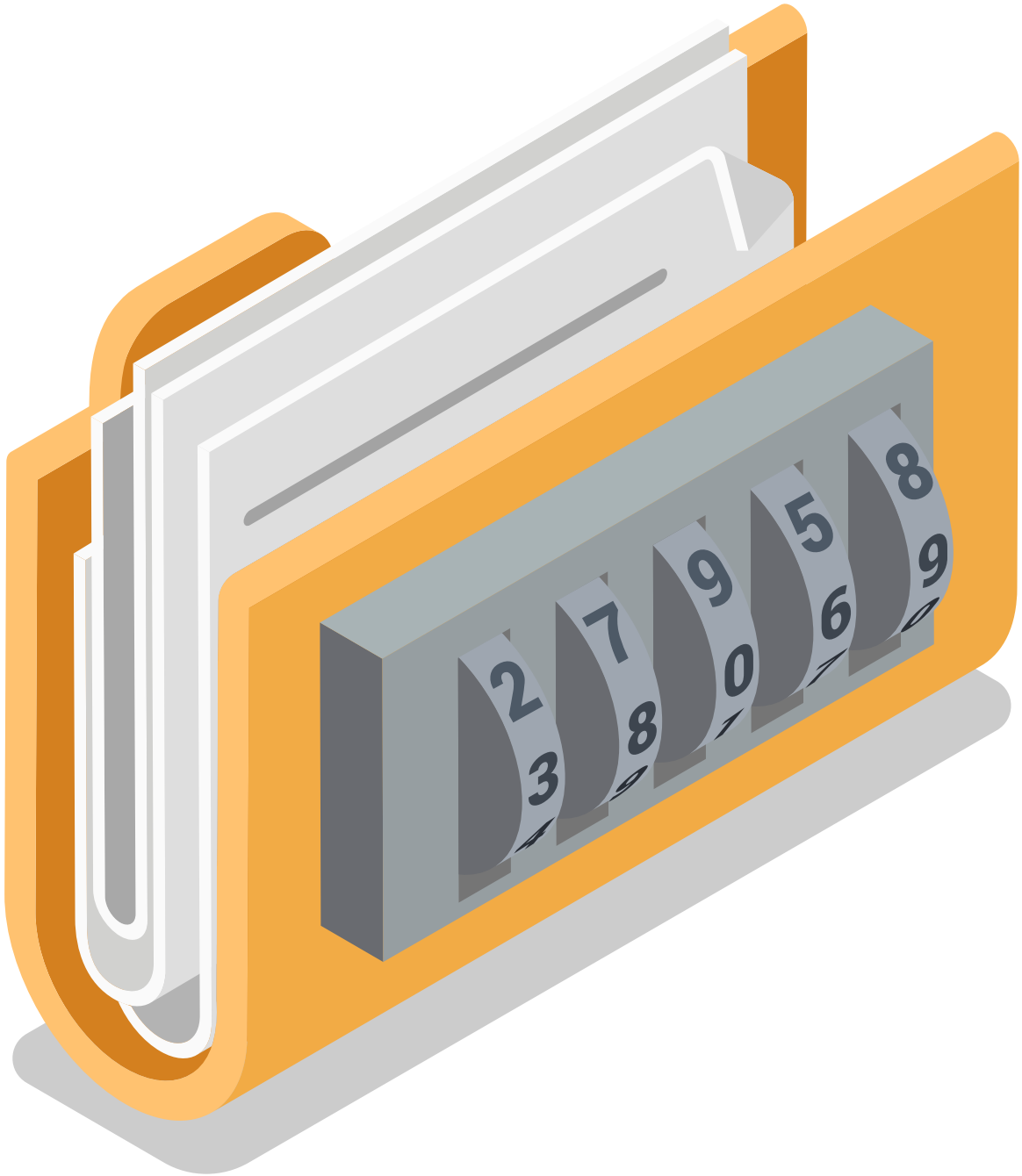
IMPRESCINDIBLES de Seguridad en Azure y Office 365

- FIM (File Integrity Monitoring): llega a Azure Security Center
- Generar certificados SSL de Let'sEncrypt con azure Automation
- AIP Scanner: la madurez de Azure Information Protection
- Azure Information Protection: acceso Condicional a documentos
- Azure Advanced Threat Protection
- Cómo erradicar la sesión activa de un usuario en Office 365
- Algunos elementos de seguridad en Azure
- Protege tus sesiones de Skype Empresarial

IMPRESCINDIBLES de .NET Core

IMPRESCINDIBLES de SharePoint

IMPRESCINDIBLES de Azure Services


2
3
7
8
9
0
5
6
8
9

Imprescindibles de Azure Services y Office 365

FIM (File Integrity Monitoring): llega a Azure Security Center

Imagina un servicio que monitorice cualquier cambio en tus ficheros y registros del sistema operativo, así como en tus aplicaciones u otro tipo de archivo para detectar cualquier indicio de ataque o infección… Esto existe y ya está disponible como preview en **Azure Security Center**.

FIM (**Supervisión de Integridad de Archivo** en español) utiliza el método de comparación para detectar variaciones entre el estado actual y el estado del anterior escaneo del archivo, de modo que nos puede ayudar a determinar si se trata de una modificación autorizada y

segura, o de lo contrario, si estamos ante una modificación sospechosa.

La integración de FIM en Security Center garantiza la integridad de los archivos y registro de Windows, así como los archivos de Linux. Es tan sencillo como seleccionar los ficheros que deseamos tener monitorizados de manera granular activando FIM, y Security Center se encargará proveernos el control de:

> Creación y eliminación de archivos y registros.
> Modificación de archivos (cambios de tamaño, listas de control de acceso y hash del contenido).
> Modificaciones de registro (cambios de tamaño, listas de control, tipo de contenido, etc.).
> FIM cuenta con sus propias políticas predefinidas para permitirnos una puesta en marcha del servicio de manera rápida y sencilla, pero también nos permite definir nuestras propias políticas o entidades para monitorizar. En este artículo te explicamos cómo hacerlo.

Nota: FIM utiliza la solución Azure Change Tracking para rastrear e identificar cambios en nuestro entorno. Cuando FIM está habilitado, tenemos un recurso de Change Tracking de tipo Solución. Si eliminamos el recurso Change Tracking, se deshabilitará la función File Integrity Monitoring en Security Center.

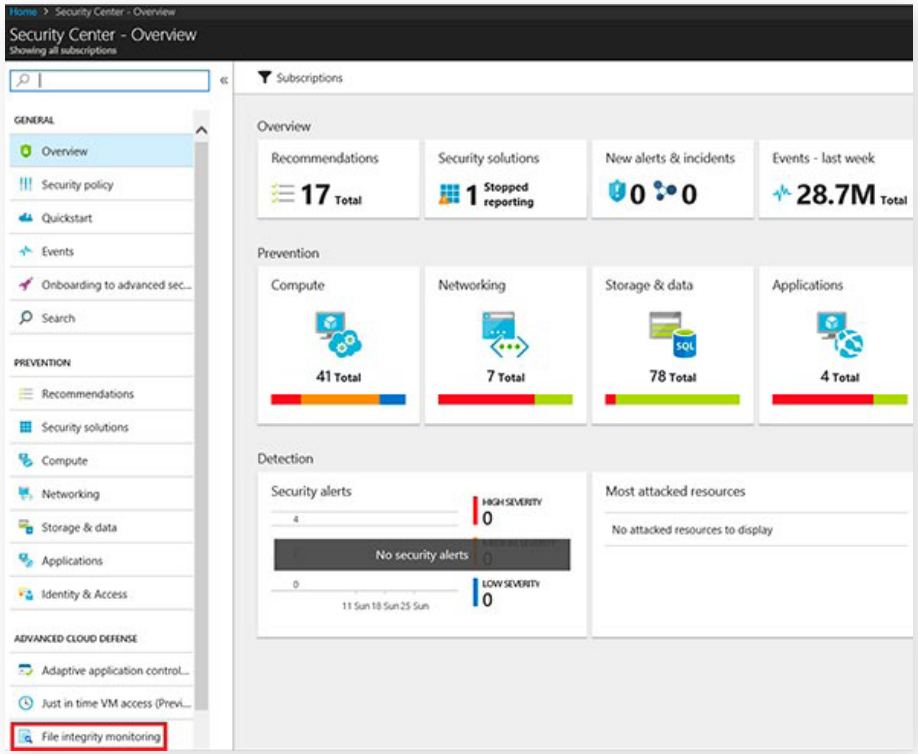
¿Qué archivos debería monitorizar?

Cuando vayamos a elegir archivos para monitorizar, lo primero que debemos hacer es pensar en los archivos que son críticos para nuestro sistema y aplicaciones. Consideremos elegir archivos que no esperamos recibir cambios sin previa planificación, debemos tener en cuenta que elegir archivos de aplicaciones o Sistema Operativo que tienen cambios frecuentemente (como archivos de registro y texto) pueden generar mucho ruido y dificultarnos la identificación de un ataque.

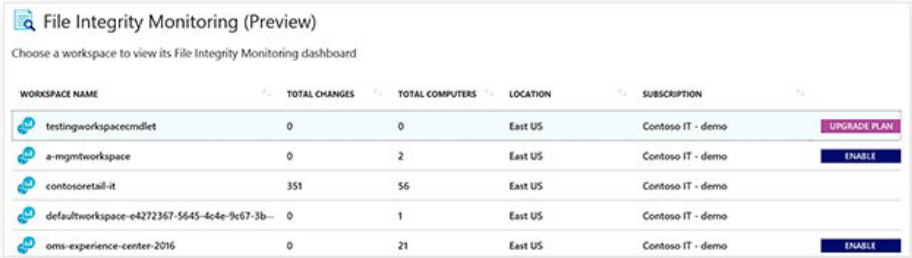
El mismo Security Center nos recomendará qué archivos debemos supervisar de manera predeterminada según los patrones de ataques conocidos que incluyen cambios de archivo y registro.

Cómo utilizar FIM

1. Nos vamos al dashboard de Azure Security Center.
2. En el menú izquierdo encontraremos Advanced Cloud Defense > File integrity monitoring.



Tras acceder a FIM podremos ver información muy relevante por cada área de trabajo formado por equipos con Windows, Linux o máquinas virtuales. Información como el número de cambios detectados durante la última semana, o un guión si se encuentra deshabilitado. También nos indicará la cantidad de equipos o máquinas virtuales de cada área, ubicación geográfica y bajo qué suscripción de Azure se encuentra.



En la última columna podemos encontrar unos botones que indican:

ENABLE Indica que FIM no se encuentra habilitado para esa área de trabajo. Para activarlo sólo tenemos que hacer clic sobre el botón.

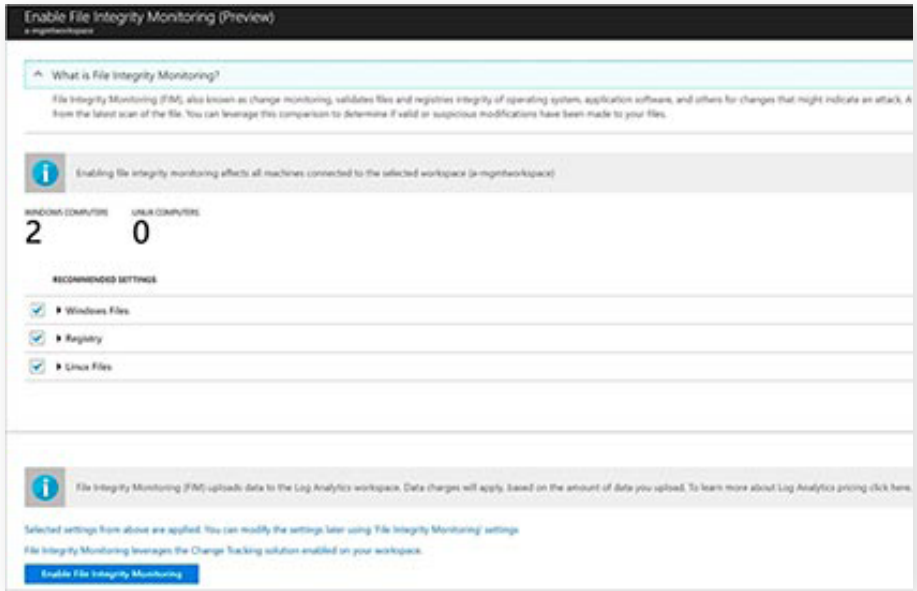
UPGRADE PLAN Indica que el área de trabajo está bajo la suscripción gratuita de Security Center, de modo que **necesitaremos subir nuestra**

UPGRADE PLAN **suscripción al plan Estándar**. Desde aquí mismo podemos hacer el upgrade de plan. Más info sobre cómo subir los niveles de Security Center para mejorar la seguridad.

Si no tenemos ninguno de los dos botones anteriores, significa que FIM ya está correctamente habilitado en el área de trabajo.

Activar FIM

Desde el mismo File Integrity Monitoring debemos pulsar sobre el botón Enable, y se nos abrirá una nueva vista donde podremos ver el número de máquinas con Windows y Linux, así como una serie de configuraciones recomendadas para esta área de trabajo.



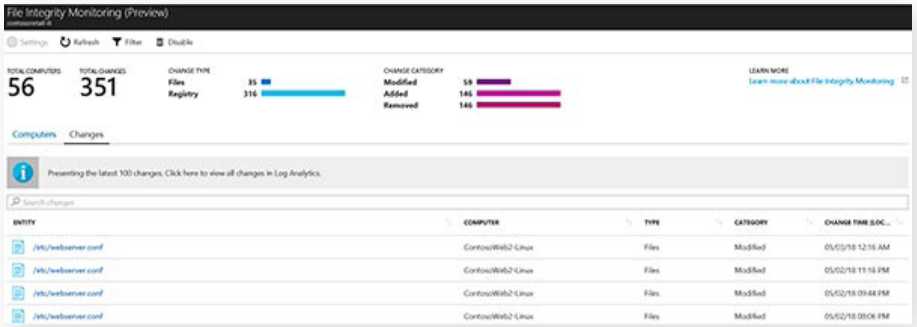
Sobre las configuraciones recomendadas, podemos expandir “Archivos Windows, Registro y Archivos Linux” para ver la lista completa de recomendaciones. Estos ajustes los podrás cambiar en cualquier momento.

Desmarcamos el *check* de cualquier recomendación que no deseamos aplicar FIM, y pulsamos sobre “Enable File Integrity Monitoring”

Conozcamos el panel de FIM

El panel de control de FIM se nos mostrará sobre las áreas de trabajo con FIM habilitado. Al abrirlo, podremos ver un sencillo resumen de los equipos conectados al área de trabajo, pero si pulsamos sobre “Cambios”, veremos información más detallada de los siguientes puntos:

- Número total de máquinas conectadas al área de trabajo.
- Número total de cambios que se han producido durante un periodo de tiempo determinado.
- Últimos 30 minutos, últimas 1, 6 ó 24 horas, o últimos 7 ó 30 días.
- Desglose de tipo de cambios (archivos, registros).
- Desglose de la categoría de cambio (modificado, añadido, eliminado).



También contamos con la opción de **Búsqueda**, la cual nos permitirá encontrar información de manera más exhaustiva, y si pulsamos sobre algún cambio, nos mostrará información más detallada. Por ejemplo, aquí vemos un cambio realizado en el registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllRemoveS... ×
Change details

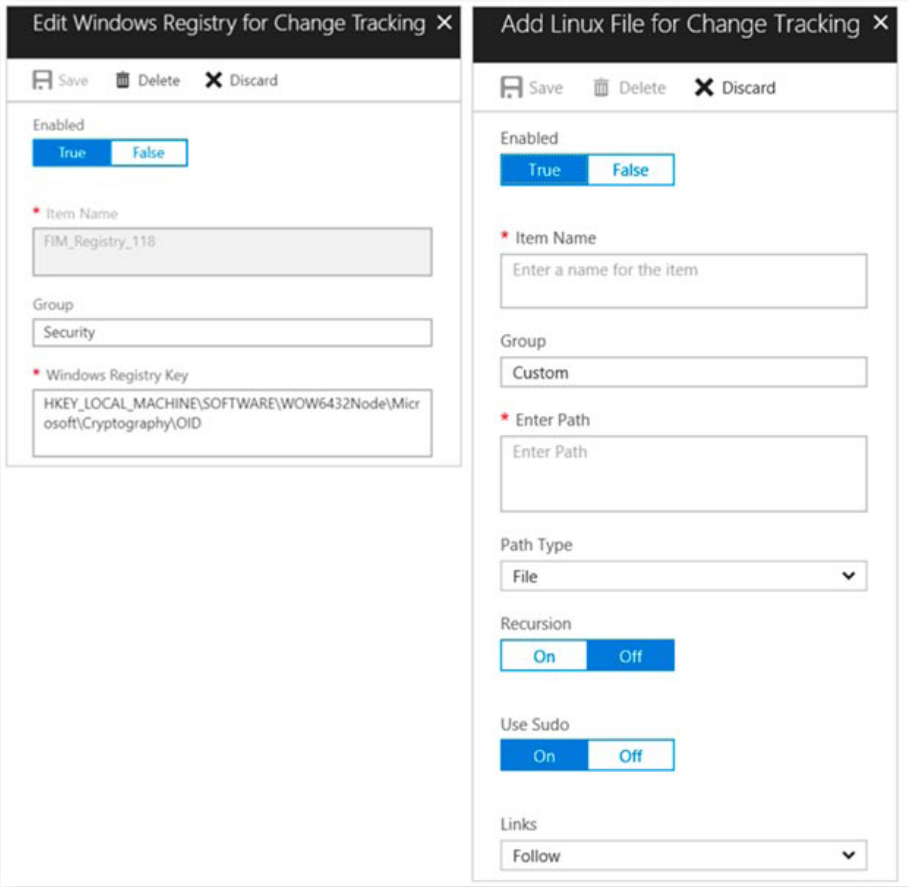
PROPERTY	VALUE BEFORE	VALUE AFTER
Acls	[{ "Name": "owner" "Value": "NT AUTHORITY\\SYSTEM" } { "...	[{ "Name": "owner" "Value": "NT AUTHORITY\\SYSTEM" } { "...
ValueData	C:\Windows\System32\WINTRUST.DLL	C:\Windows\SysWOW64\WINTRUST.DLL
Unchanged prope...		
SourceComput...	cda27197-3886-4fbb-8720-1f2304d1ae1d	No Change
RegistryKey	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptograph...	No Change
Hive	HKEY_LOCAL_MACHINE	No Change
ValueName	Dll	No Change
ValueType	REG_SZ	No Change
Size	32	No Change
SourceSystem	OpsManager	No Change
MG	00000000-0000-0000-0000-000000000001	No Change
ManagementG...	AOI-5bc7c24b-ad6c-4f7f-905c-3ac3f3259938	No Change
TenantId	5bc7c24b-ad6c-4f7f-905c-3ac3f3259938	No Change
VMUUID	c14ded1b-054b-4483-9fd1-1829eb76c406	No Change

podremos añadir entidades de monitorización nuevas, o editar las ya existentes.

3. Veremos tres pestañas Registros de Windows, Archivos de Windows y Archivos de Linux. Pulsemos la pestaña sobre la que queremos añadir una nueva entidad, y luego pulsamos en Add (Añadir).
4. Ahora sólo debemos completar los campos con la información solicitada, algunos son campos requeridos. Vamos a mostrar dos ejemplos, Windows Registry y Linux Files.

Añadir, editar o eliminar una regla de monitorización

1. Añadir, editar o eliminar una regla de monitorización
2. Desde el panel de FIM, pulsamos sobre **Settings (Configuración)** en la parte superior, y se nos abrirá el Workspace Configuration, donde



Es importante que recordemos cómo hemos llegado hasta ahí, ya que si deseamos eliminar, editar o simplemente deshabilitar una de estas reglas, debemos hacerlo justo ahí.

Así de sencillo es como lograremos ese plus de seguridad en nuestras máquinas Windows y Linux, dónde en todo momento podremos tener controlada la integridad de nuestros archivos de Windows y Linux, así como los registros de Windows.

Daniel Alonso Sanchis
Cloud Solutions Principal Advisor

Generar certificados SSL de LetsEncrypt con Azure Automation

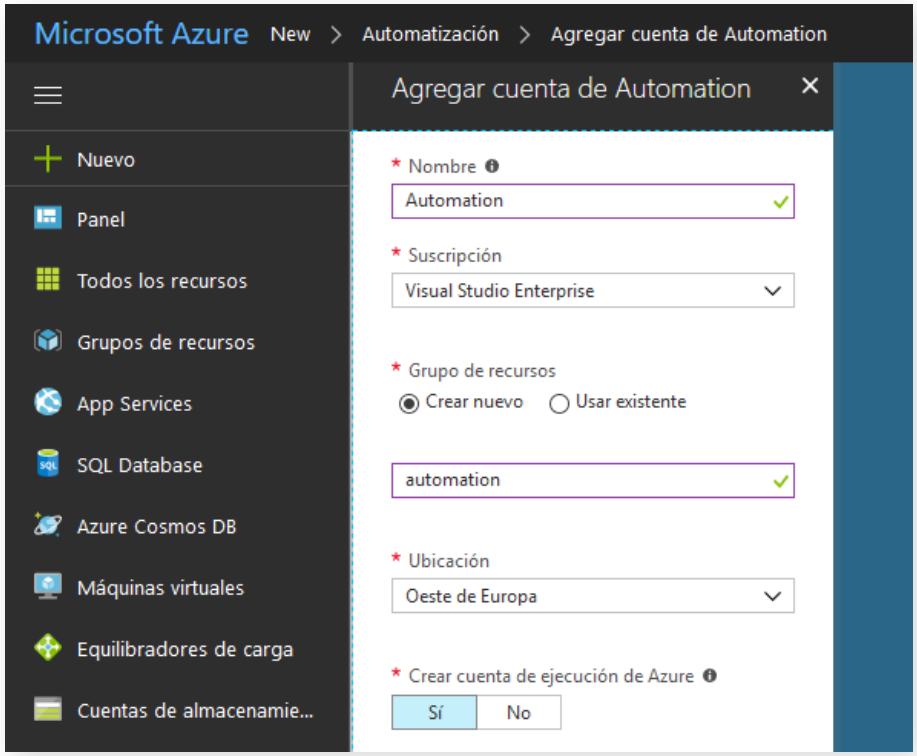
Gracias a **Let's Encrypt** podemos tener todos los certificados SSL que necesitemos, gratis y de por vida. La única pega es que caducan cada 3 meses, y eso fácilmente nos puede tirar para atrás... Por suerte, gracias a la magia de **PowerShell** y **Azure Automation** podemos configurar la renovación periódica y nos podremos olvidar de esta tarea. Y lo mejor de todo es que es completamente **compatible con cualquier tipo de Azure Web Apps**!

En primer lugar, necesitamos tener una cuenta de **Azure Automation** en nuestra suscripción de Azure. Si ya la tenemos, nos podemos saltar el siguiente paso.

1. Agregar una cuenta de Azure Automation

Como comento en el párrafo anterior, este paso lo podemos omitir si ya contamos con una cuenta de Azure Automation en nuestra suscripción. De lo contrario, adelante con estos sencillos pasos:

1. Iniciamos sesión en el portal de Azure.
2. Podemos utilizar el buscador para encontrar "Cuentas de Automation".
3. Incluimos un nombre, suscripción, grupo de recursos y ubicación. En mi caso he utilizado "automation" tanto como nombre como grupo de recursos.

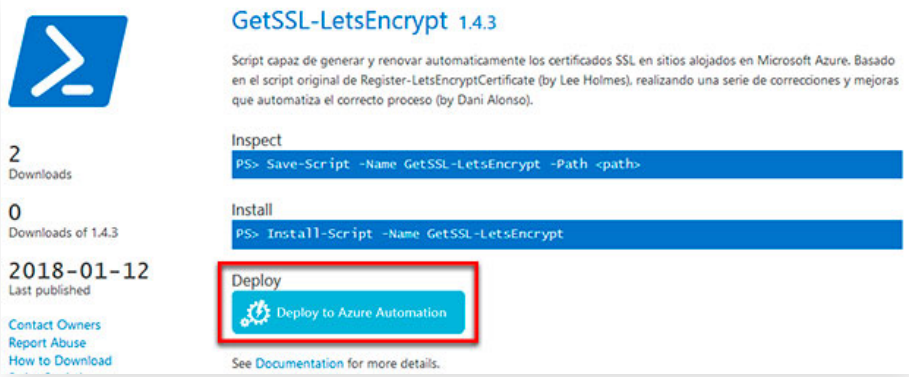


Esperamos a que se completen las implementaciones que hemos iniciado, y con esto ya habremos creado una cuenta de Azure Automation y podremos seguir adelante.

2. Desplegar GetSSL-LetsEncrypt en Azure

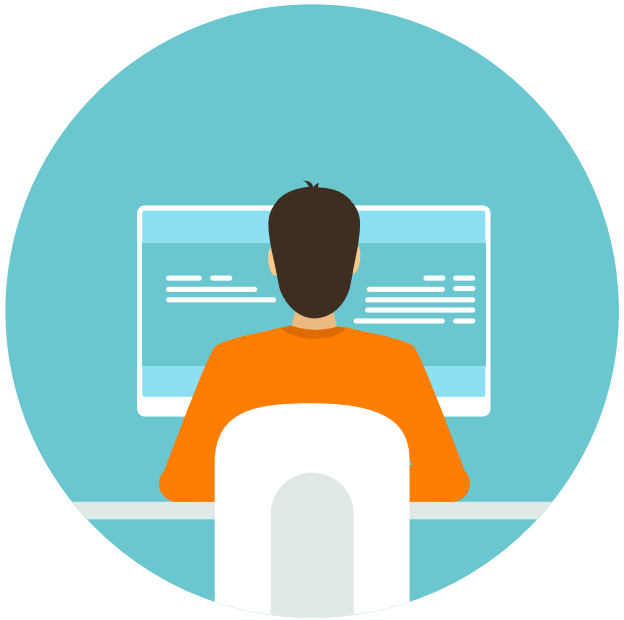
Este proceso también es muy sencillo. Para instalar el script en Azure Automation, debemos ir al siguiente enlace de la **PowerShell Gallery**:

https://www.powershellgallery.com/packages/GetSSL-LetsEncrypt



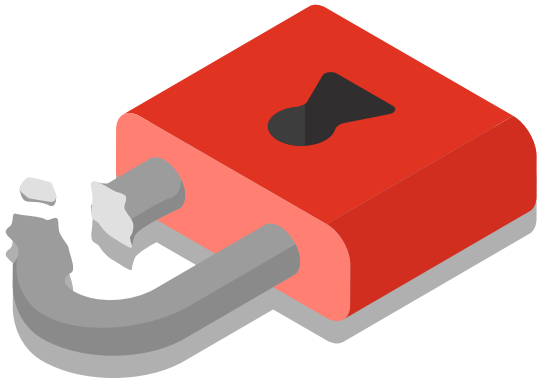
Asegurémonos de desplegar la versión más reciente! Pulsamos sobre el botón "**Deploy to Azure Automation**", y automáticamente se nos abrirá el importado de Runbooks en Azure. Aquí seleccionamos nuestra cuenta de Automation y aceptamos.

En el momento que se inicie la implementación, comenzará la instalación de los módulos que GetSSL-LetsEncrypt necesita para funcionar. Si no contábamos con los módulos requeridos, esta implementación puede llegar a tardar unos 5 minutos en completarse. Si ya teníamos instalados los módulos, el proceso es instantáneo. En cualquier caso, se realizará de manera automática y desatendida.

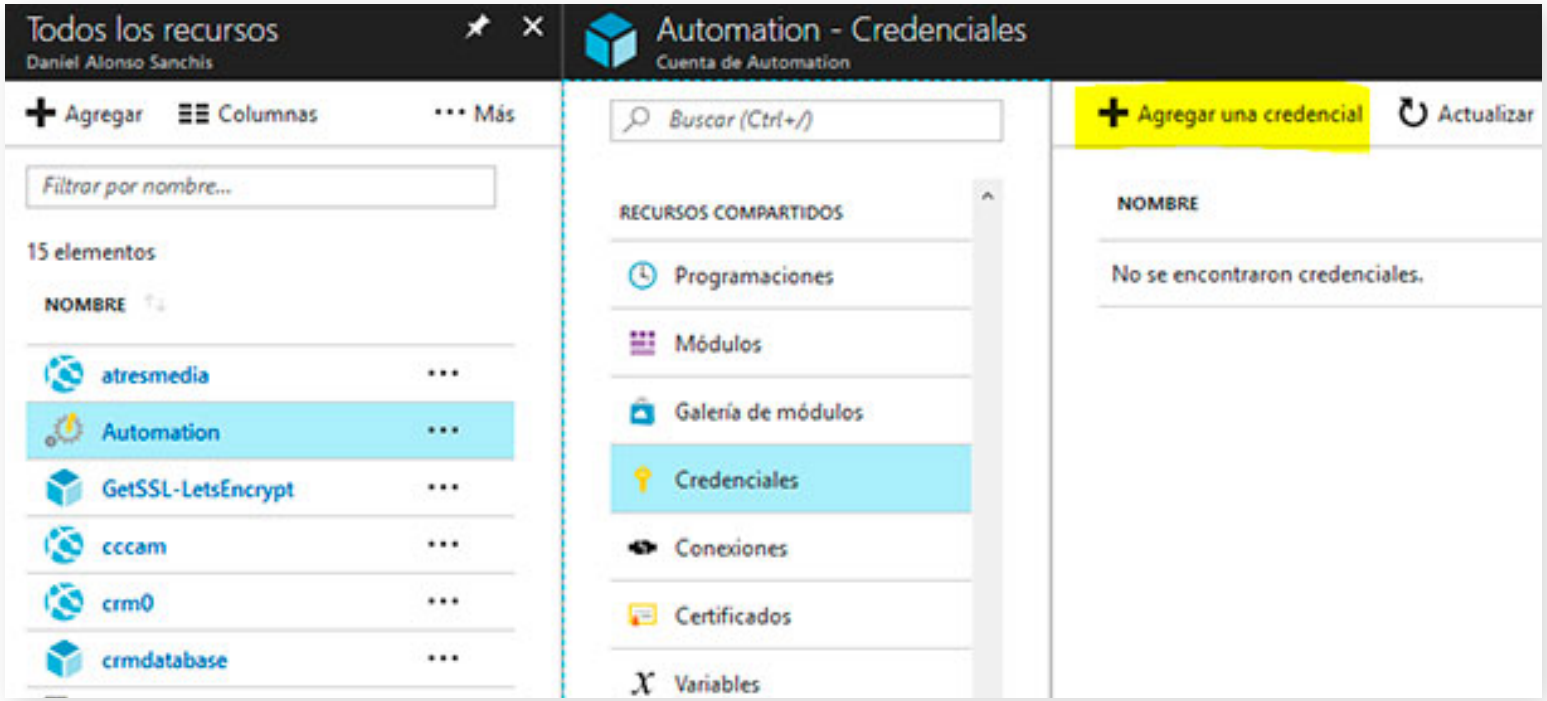


3. Puesta en marcha de GetSSL Let's Encrypt

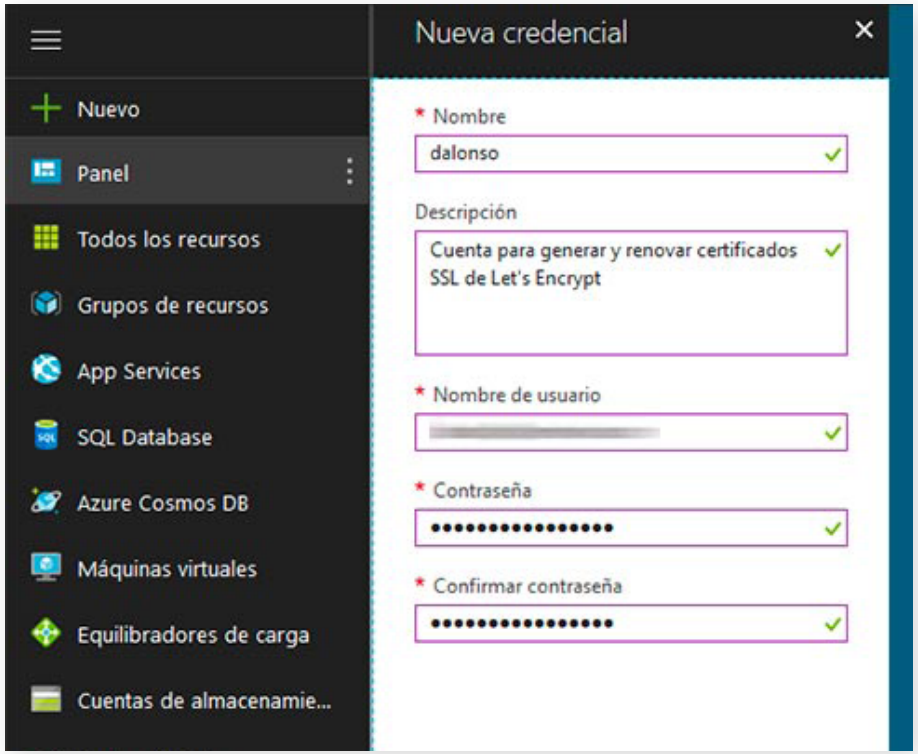
Cuando se complete el despliegue de GetSSL-LetsEncrypt, vamos a configurar un credencial para automatizar los procesos.



1. Nos vamos a Cuenta de Automation > Recursos Compartidos > Credenciales. Y hacemos clic en "+ Agregar una credencial"



2. Creamos la cuenta especificando la cuenta de usuario y contraseña que utilizamos para acceder al Portal de Azure. Para el ejemplo he utilizado "dalonso".

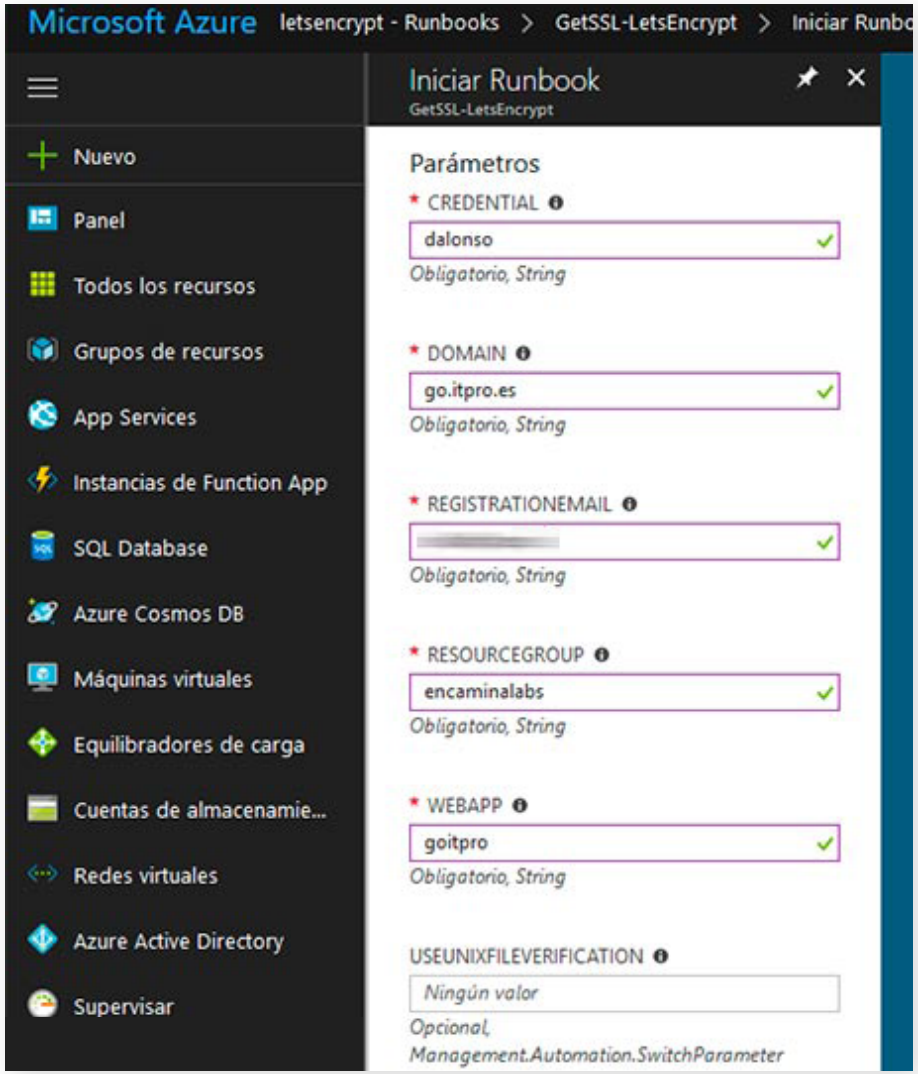


3. Ahora vamos a **Automatización de Procesos** > **Runbooks**. Ahí veremos el Runbook de GetSSL-LetsEncrypt. Pulsamos en él.

4. En la parte superior, veremos varios botones. Pulsamos en Editar, y en la siguiente página le damos directamente a **Publicar**, respondiendo **SÍ** a la pregunta.

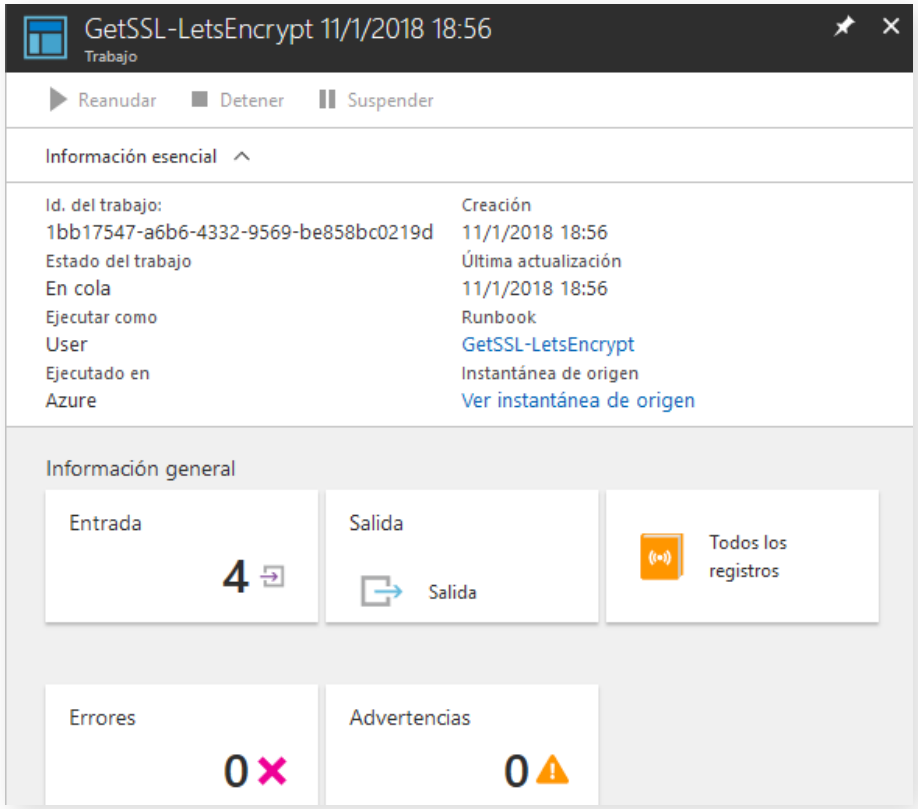
Antes de programar la tarea, es interesante probar que todo funciona bien, así que pulsamos sobre el botón **Iniciar**, y rellenamos los parámetros requeridos:

> **Credential**: Especificaremos la cuenta de credencial que hemos creado. En mi caso es dalonso.
> **Domain**: El dominio que queramos añadir el certificado.
> **Registrationemail**: El email donde recibiremos notificaciones de LetsEncrypt, como por ejemplo avisos de caducidad.
> **Resourcesgroup**: Grupo de recursos.
> **Webapp**: Nombre de la instancia web.
> **UneUnixFileVerification**: Este es un valor opcional, comúnmente innecesario.



Cuando lo completemos, pulsamos el botón **Aceptar**.

Una vez haya finalizado, comprobaremos que no se haya producido errores. Si no se han producido errores, nos vamos al navegador y cargamos el sitio web que estamos instalando el certificado SSL...

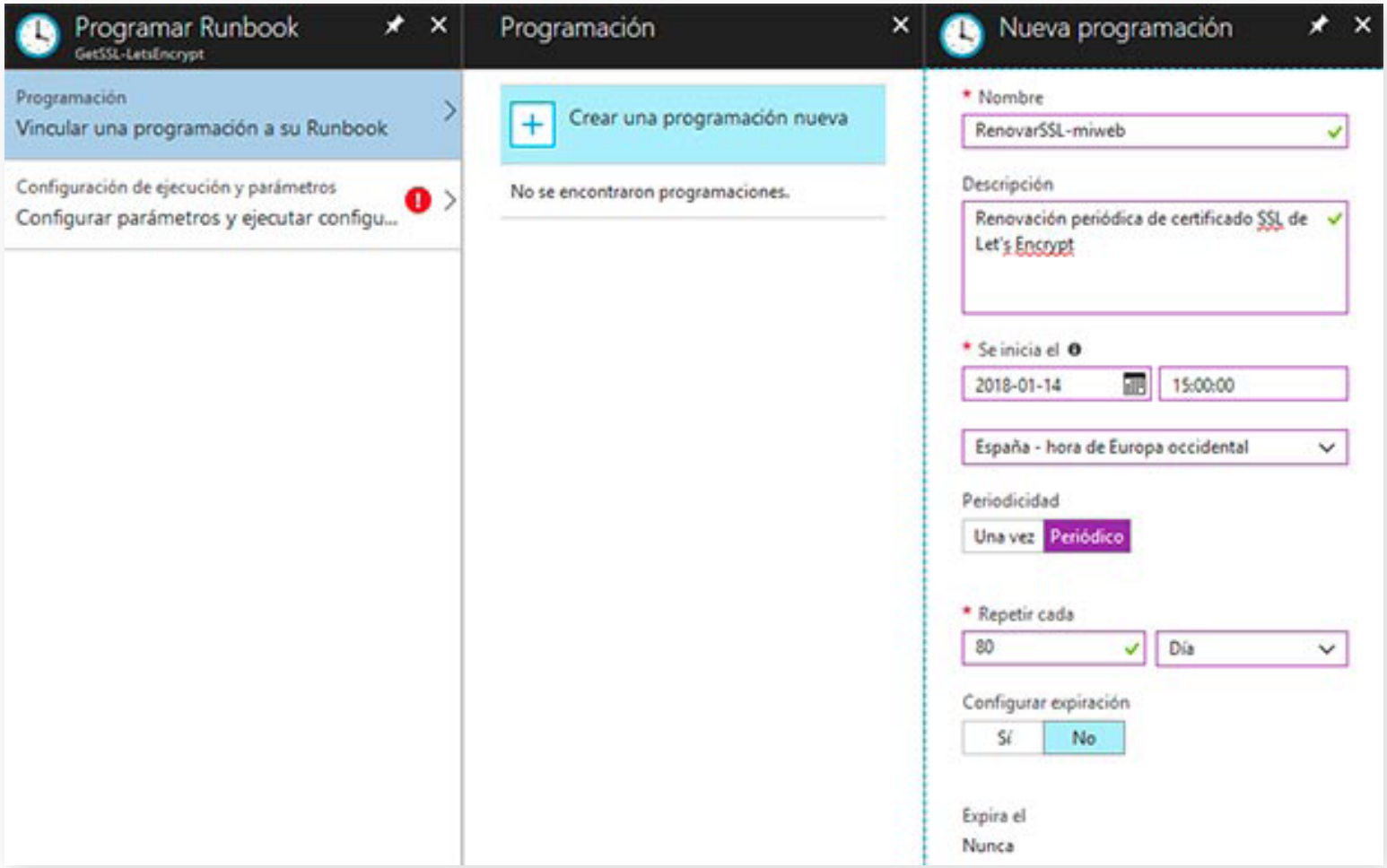


Ou yeah! **Ya tenemos nuestro sitio web funcionando con SSL**! Ahora vamos a programar la renovación periódica.

4. Programar la renovación automática

Ahora sí! Para poder olvidarnos de tener que estar renovando el certificado cada tres meses, podemos crear una tarea programada que ejecute el script cada cierto tiempo.

1. Nos vamos al Runbook de GetSSL-LetsEncrypt, y pulsamos sobre el botón **Programar**.
2. Hacemos clic en **Programación** > **Crear una programación nueva**.
3. Completamos los datos de la programación, incluimos un nombre que sea lo más descriptivo posible, una breve descripción, fecha de inicio, etc. Debemos tener en cuenta que la duración de los certificados es de 3 meses, así que programar **una periodicidad de 80 días estaría bien**. Cuando lo tengamos, pulsamos en crear.



Ahora añadimos los parámetros del mismo modo que hicimos en el apartado de puesta en marcha. Cuando lo tengamos, aceptamos.

Y ya está, hemos programado la renovación automática de nuestros certificados SSL!

Algunas consideraciones importantes

LIMITACIONES:

Si estamos realizando pruebas o si tenemos muchos dominios/subdominios que deseemos registrar. Debemos tener en cuenta las limitaciones establecidas por Let's Encrypt:

> 20 dominios distintos (inclusive subdominios) por semana.
> Certificados duplicados, 5 por semana.
> Se pueden crear un máximo de 10 cuentas por dirección IP en 3 horas.

INCOMPATIBLE CON MICROSOFT ACCOUNT (LIVEID):

Debemos tener en cuenta que **sólo funciona con cuentas de empresa o educación** (OrgID), no cuentas personales (LiveID). Esto se debe a que las cuentas Microsoft Account son ajenas a Azure, y el proceso de inicio de sesión necesita una redirección a través de live.com para recuperar un token, algo que no es posible hacer de forma no-interactiva. Pero no os preocupéis, tiene fácil **SOLUCIÓN** y no nos llevará más de 5 minutos:

1. Si no tenemos un tenant de AzureAD, lo creamos.
2. Creamos un usuario de Azure AD con rol de usuario.
3. Nos vamos al **grupo de recursos** del sitio web que queramos añadir SSL, y en control de acceso (IAM), agregamos el usuario que hemos creado en AzureAD asignándole el rol de **Colaborador**.
4. Por último, configuramos los credenciales de la cuenta AzureAD en Azure Automation, como vimos en el paso 3.2.

Daniel Alonso Sanchis
Cloud Solutions Principal Advisor

AIP Scanner: la madurez de Azure Information Protection

Azure Information Protection avanza de nivel con un escáner que rastrea sistemas locales para aplicar etiqueta y protección a contenido en reposo.

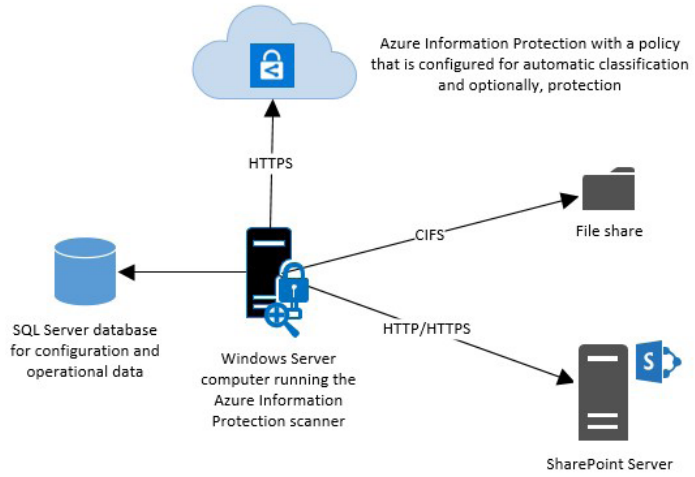
¿Os he dicho ya que **me encanta** Azure Information Protection?

Como os contaba en artículos anteriores, Azure Information Protection (AIP) es un servicio que permite **crear directivas para etiquetar y proteger documentos**, tanto de forma manual como automática si se cumplen ciertas condiciones. Esos documentos protegidos se pueden compartir libremente y **el acceso se controla a través de la autenticación en Azure AD**.

Esto funciona muy bien para nuevos documentos, pero ¿qué pasa con todos **los documentos que ya tenemos** en nuestros sistemas? ¿hay que abrirlos uno a uno para **aplicar la protección** adecuada? Pues no. Para dar respuesta a esas preguntas está **AIP Scanner**, un servicio que corre sobre Windows Server y utiliza la aplicación cliente de Azure Information Protection para **descubrir, etiquetar y proteger los archivos existentes en sistemas locales**, según las directivas definidas en Azure.

El concepto es simple: **le dices a AIP Scanner qué localizaciones escanear**. El escáner rastreará esas localizaciones constantemente y **donde encuentre una coincidencia** con las condiciones de una directiva AIP, **aplicará la etiqueta** correspondiente.

Las **localizaciones** que pueden ser escaneadas por AIP Scanner son **sistemas de archivos** CIFS y bibliotecas de **SharePoint Server** 2013/2016.



Requisitos

Microsoft recomienda instalar el escáner en un servidor independiente con 4 cores y 4 GB RAM, que ejecute al menos Windows Server 2012 R2, instancia SQL y conexión con el servicio RMS y **api.informationprotection.azure.com**.

Además, se debe **aprovisionar una cuenta de servicio** sincronizada con Azure AD, con permisos de lectura-escritura en las ubicaciones a escanear, y configurada como "**super user**" si se van a utilizar etiquetas que anulen o cambien la protección.

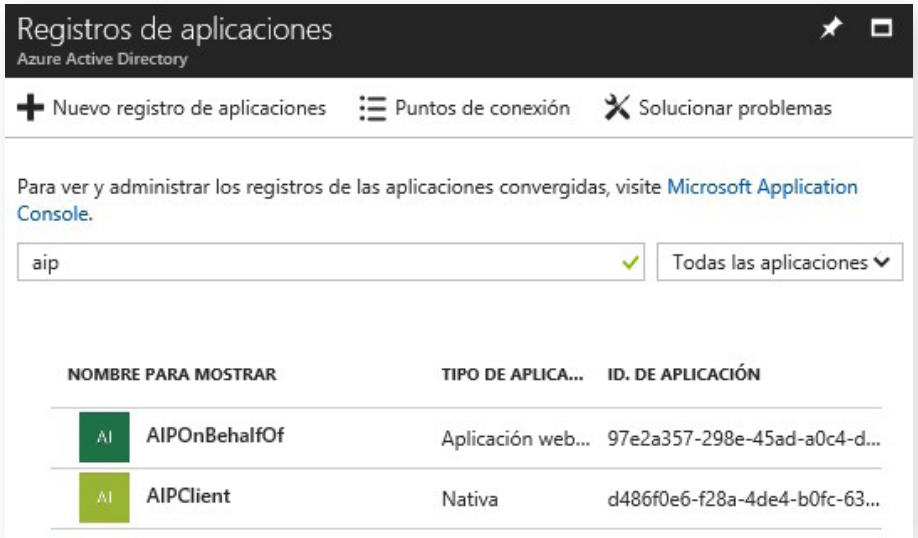
Instalación

De momento, la instalación y configuración del servicio se realiza completamente con Powershell, aunque es posible que en el futuro exista una **interfaz gráfica para la administración**.

Lo primero es instalar el cliente de AIP para poder disponer del módulo Powershell que incluye los cmdlets de AIPScanner.

A continuación instalamos el escáner indicando la instancia de SQL Server: Install-AIPScanner -SqlServerInstance <database name>

Por defecto, los comandos de Powershell de AIP se ejecutan en el contexto del usuario, pero **AIP Scanner requiere la ejecución desatendida**. Para ello se deben registrar dos aplicaciones en Azure AD y luego ejecutar el comando Set-AIPAuthentication con los parámetros de dichas aplicaciones. Esto **permite al Scanner utilizar un token para autenticarse en Azure AD**, en lugar de utilizar una cuenta de usuario.



Configuración

Para **indicar ubicaciones** a escanear utilizamos Add-AIPScannerRepository -Path <ruta>, indicando una ruta de archivos o **URL de SharePoint Server**. Con el verbo Get obtenemos una lista de todas las ubicaciones que se están escaneando, y con Remove podemos quitar una ubicación del escaneo.

Con Set-AIPScannerConfiguration definimos **cómo se aplica la clasificación y la protección**, según los siguientes parámetros:

parámetro	Valor	Descripción
-ScanMode	{**Enforce** | Discover}	***Discover*** rastrea las ubicaciones en modo "whatif", creando reports sin etiquetar ni proteger. ***Enforce*** rastrea las ubicaciones y aplica etiquetas y protección según las directivas AIP. Se recomienda comenzar por ***Discover*** para evaluar los resultados y luego pasar a ***Enforce***
-Schedule	{OneTime | **Continuous** | Never}	***OneTime*** para un único escaneo. ***Continuous*** para escaneo continuo.
-OverrideLabel	{Off | **AppliedByScanner** | On}	Define si AIP Scanner puede cambiar la clasificación. Por defecto solo puede cambiar clasificaciones aplicadas por el propio Scanner.
-JustificationMessage	*Texto libre*	Justificación para cambiar etiqueta.
-ReportLevel	{Off | Debug | **Info** | Error}	Nivel de registro..
-PreserveFileDetails	**On** Off	***On*** para preservar los atributos del archivo.
-DefaultOwner	*Owner's e-mail*	Cambia el owner del archivo.

En la ubicación **%localappdata%\Microsoft\MSIP\scanner\Reports** podemos encontrar todos los registros de actividad del Scanner.

Licencias

A nivel de **licenciamiento**, se necesita una licencia **AIP Premium P2** por cada usuario con permisos de escritura en las localizaciones escaneadas.

Demo

En el siguiente vídeo puedes ver el *Scanner* en acción.

¿Y en Office 365?

Yo también me he hecho esa pregunta. Estaría genial tener algo similar a este escáner que rastree **todas las ubicaciones de Office 365**: SharePoint online, Exchange online, OneDrive for Business, etc.

¡Pero si eso ya existe!

¿Cómo?

Claro, las **etiquetas de clasificación en el Centro de Seguridad y Cumplimiento de Office 365 (CSC)** hacen justamente eso: creas tus etiquetas y las condiciones para que se apliquen automáticamente en cualquier ubicación de Office 365.

Ya, pero no protegen.

Es verdad, ¡pero por poco tiempo! De aquí a nada, **las etiquetas de AIP aparecerán en el área de Clasificación del CSC**, y viceversa, y se podrá editar la protección tanto en un lado como en el otro. Puedes ver el anuncio y la demo en esta sesión del Ignite, donde además desgranan el roadmap del ecosistema **Microsoft Information Protection**.

Conclusión

Ya sea por motivos de **auditoría**, para cumplir con los **requerimientos de la GDPR**, o simplemente por retomar el control del contenido empresarial, **AIP Scanner se convertirá en un gran aliado** de la seguridad y la protección de los datos.

Pablo Ortiz Baiardo
Former employee of ENCAMINA

Azure Information Protection: Acceso Condicional a documentos

La combinación de **Azure AD Premium** y **Azure Information Protection** abre un sinfín de posibilidades de protección de contenido basado en condiciones. Hoy te contamos las claves.

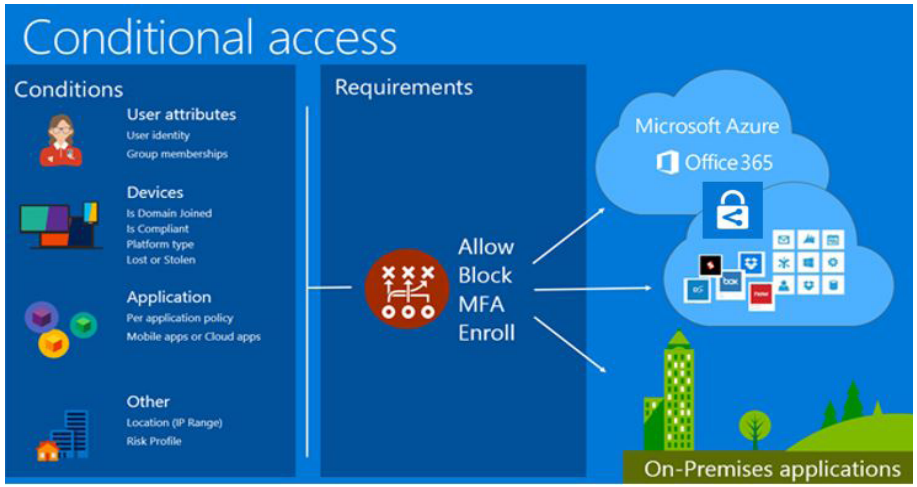
Ahh, me encanta el Acceso Condicional de Azure AD Premium.

Defines políticas para **controlar el acceso a aplicaciones** protegidas basándote en diferentes condiciones, como la **identidad del usuario**, el tipo de **dispositivo** que se utiliza para acceder a la aplicación, el estado del dispositivo, la **ubicación de acceso** (red interna vs internet), e incluso **factores de riesgo** (login desde dispositivos en riesgo, salto imposible, etc.). Luego combinas esas **condiciones** para controlar, no sólo el **acceso**

a una aplicación específica, sino también si se aplican controles adicionales durante el inicio de sesión, como **MFA** o exigir que el dispositivo esté **unido a dominio**. ¡Y todo en dos clics!

Azure Information Protection (AIP) es otro gran servicio del que me declaro fan incondicional (nunca mejor dicho). Ya he escrito algunos artículos explicando su uso, tanto en la revista CompartiMOSS como en este mismo blog, por lo que no voy a entrar en detalles técnicos. La idea es que defines **directivas AIP para etiquetar y proteger documentos**. Esos documentos protegidos los puedes compartir, pero el acceso se controla a través de la **autenticación en Azure AD**.

Pues bien, ahora el Acceso Condicional de **Azure AD se combina con AIP** para ofrecer una nueva capa de protección a los contenidos corporativos. Dependiendo de las condiciones de acceso al documento etiquetado por AIP, se puede **bloquear el acceso**, o bien permitir, si se cumplen ciertos requisitos.

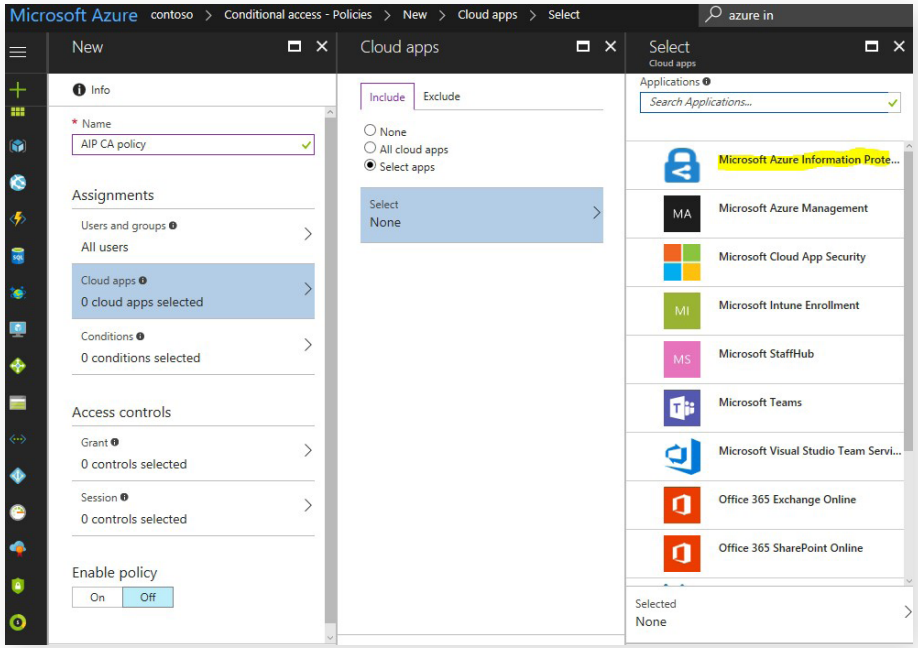


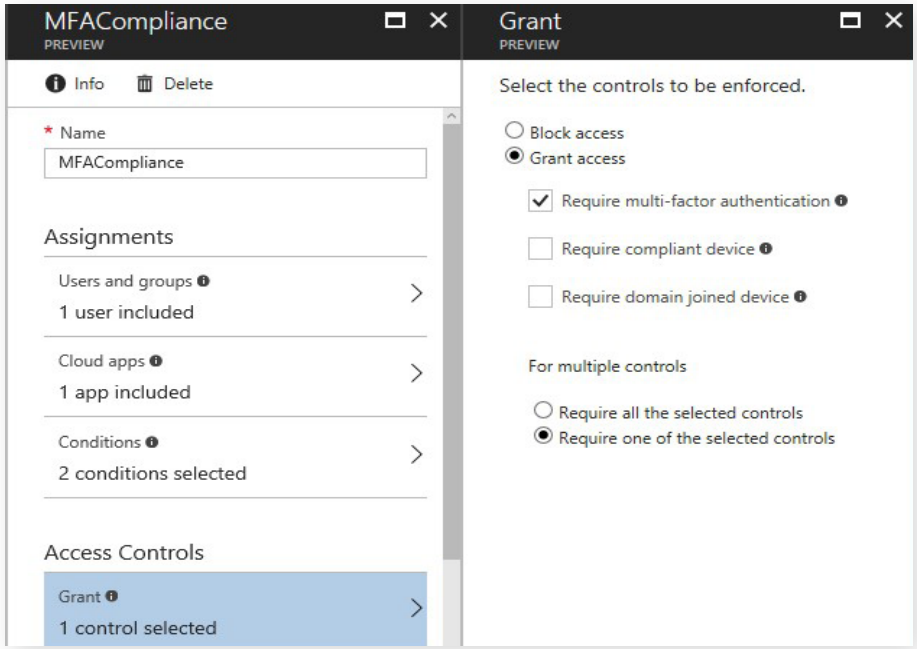
¿Cómo funciona?

En el momento de definir una **política de Acceso Condicional**, optamos porque dicha política **aplique a Azure Information Protection**.

Además, **seleccionamos los usuarios** a los cuales va a aplicar la política, definimos **condiciones adicionales**, como localizaciones o dispositivos de acceso, y aplicamos el control de acceso.

Por ejemplo, podemos **requerir MFA** como condición para poder acceder a **documentos confidenciales** abiertos por miembros del departamento Legal, desde dispositivos móviles.





Estos son algunos de los escenarios más comunes para políticas de Acceso Condicional aplicadas a contenido protegido por AIP:

- **Requerir autenticación multifactor**: forzar MFA para acceder a documentos protegidos, lo cual ayuda a la protección contra credenciales robadas o comprometidas.
- **Dispositivo controlado o unido a dominio**: permitir el acceso sólo si el dispositivo del usuario está unido a dominio o cumple con las directivas MDM/MAM (Intune).

- **Inicio de sesión de riesgo**: bloquear el acceso cuando el inicio de sesión del usuario está definido como “de riesgo” (p.e. saltos imposibles, inicio de sesión desde dispositivo de otro usuario, etc)
- **Red de confianza**: bloquear el acceso cuando el usuario no está en las oficinas de la empresa, de manera que sólo se podrá acceder a contenido sensible desde una red de confianza.

Como podéis imaginar, esto abre un **enorme abanico de posibilidades** de protección granular, que en combinación con otras características de **Azure AD Premium** (por ejemplo los grupos dinámicos), convierte la protección del contenido corporativo en una actividad sumamente fácil, flexible, y dirigida.

Demo

En el siguiente vídeo podéis ver cómo llevamos todo esto a la práctica:

Pablo Ortiz Baiardo
Former employee of ENCAMINA

Azure Advanced Threat Protection

Advanced Threat Analytics (ATA), la herramienta de instalación local que protege contra ataques de intrusión. Ahora **Microsoft la ha llevado a la nube con Azure Advanced Threat Protection** (AATP).

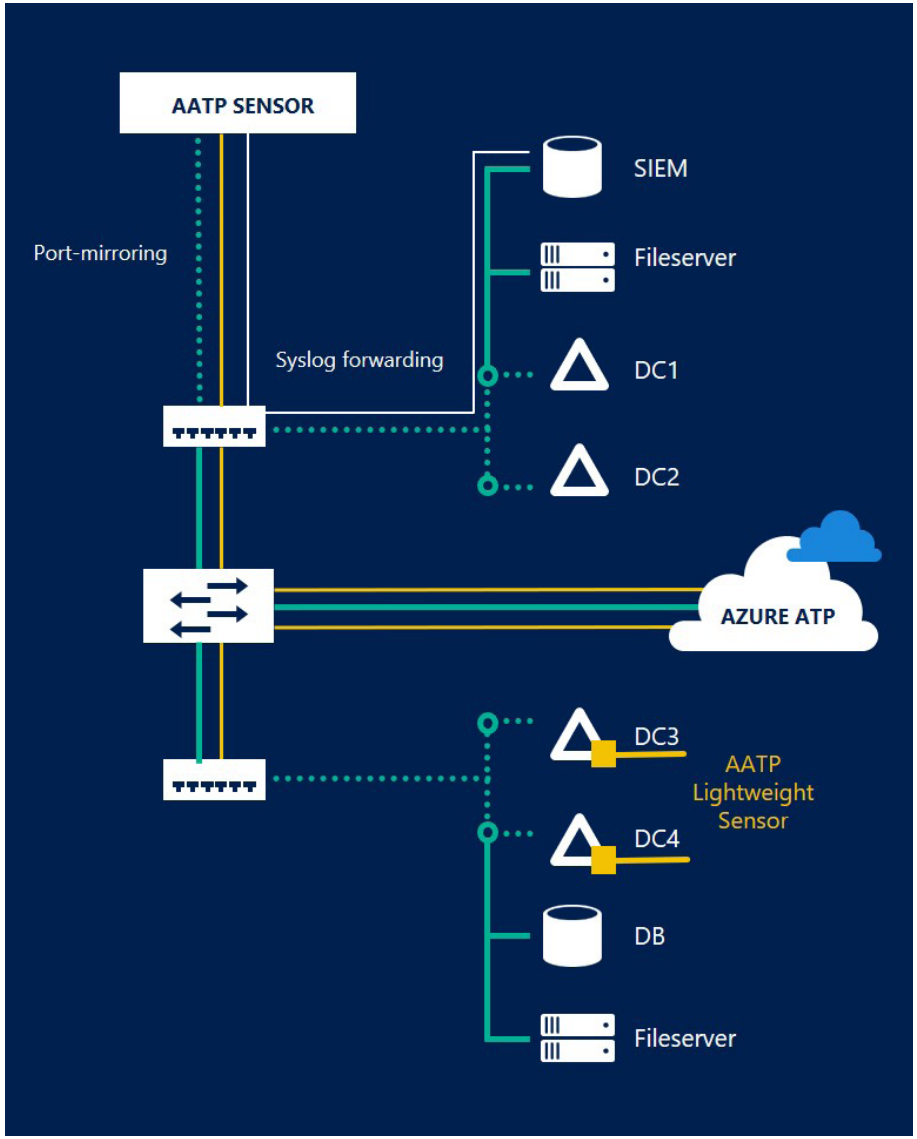
El funcionamiento de **Azure Advanced Threat Protection** (AATP) es igual al de ATA: recoge información de tráfico de los controladores de dominio para **crear perfiles de comportamiento y detectar amenazas**.

Arquitectura

La diferencia más evidente de AATP con respecto a ATA a nivel de arquitectura, es que el **ATA Center se va a la nube**.

Para los que no estéis familiarizados con la terminología ATA, el **ATA Center** es un servidor independiente **encargado de recibir los datos de tráfico de los controladores de dominio** (DC) del bosque de directorio activo (AD), a través de Gateways o Puertas de enlace. Este servidor tiene unos **requerimientos mínimos** que, por ejemplo, en el caso de la memoria RAM parten de **32GB para tráfico muy bajo**, que puede irse **fácilmente a 48GB** para una empresa de 40-60 usuarios activos. Si el tráfico aumenta y no escalamos el hardware, se incrementarán los tiempos de detección de amenazas.

Pues bien, **AATP lleva la potencia del ATA Center a la nube, como servicio**. Es decir, nos despreocupamos de los recursos del servidor, de su mantenimiento y del escalado. Los tiempos de detección son siempre óptimos. Y el software estará **siempre actualizado** a la última versión.

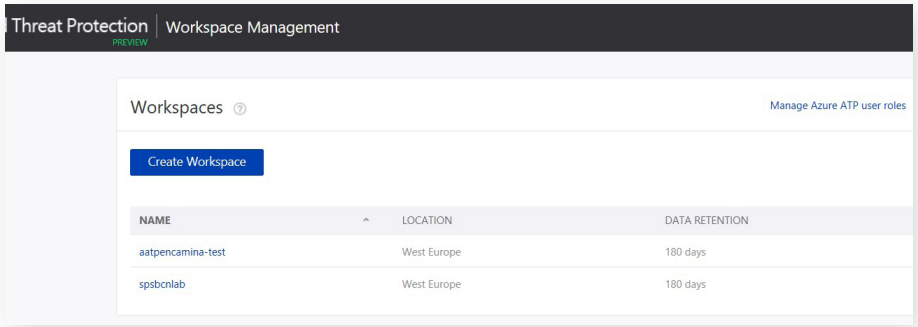


Las Gateways de ATA ahora son **Sensores**. Su funcionamiento es similar, capturando el tráfico de paquetes en los DC y enviándolo a Azure. Pero los requerimientos de hardware son más ajustados que en el caso de las Gateways.

Despliegue

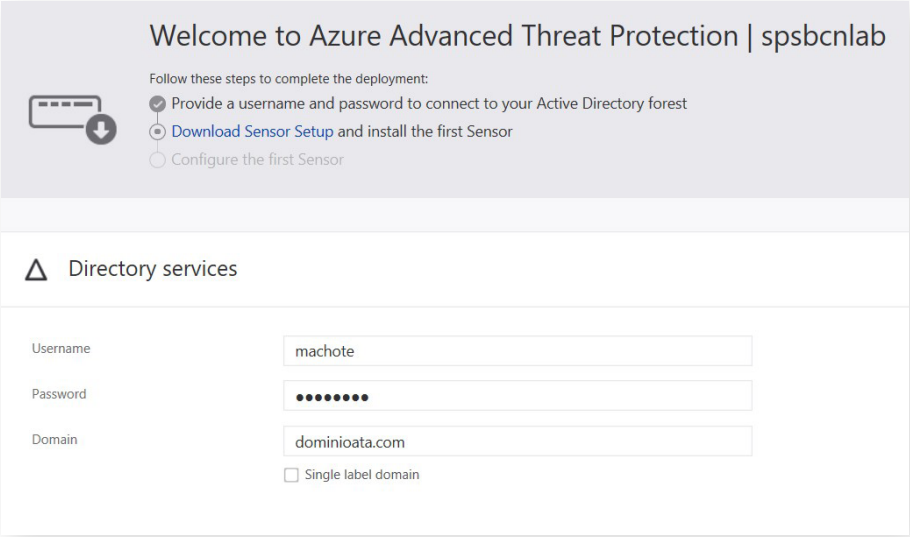
Una vez habilitado el servicio, veremos una **nueva entrada en los Centros de administración de Office 365, "Azure ATP"**, que nos lleva a la consola de administración, accesible también en la dirección https://portal.atp.azure.com.

Lo primero que debemos hacer es crear un nuevo **Workspace**.



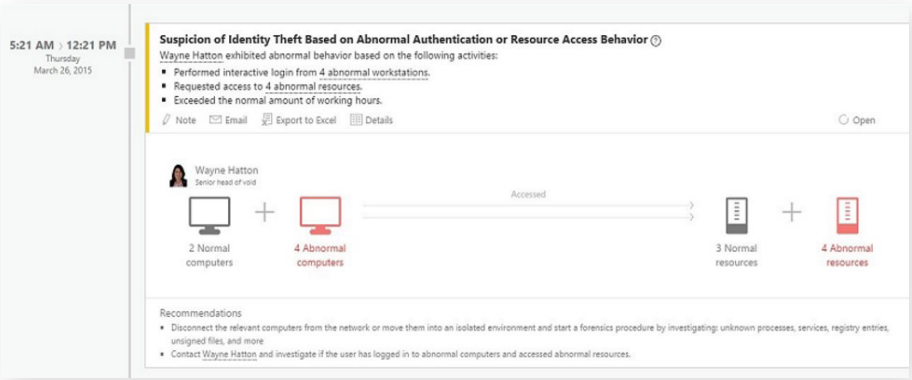
Cada Workspace es un **despliegue de AATP independiente**. Se pueden configurar diferentes Workspaces para producción, desarrollo, lab, etc., y se necesita **un Workspace por cada bosque de AD**.

Una vez creado el Workspace, lo siguiente es **configurar la conexión** con el bosque de AD, ingresando las credenciales de un usuario con permisos de lectura del bosque de AD, para luego **descargar, instalar y configurar el sensor en el controlador de dominio**. Los requisitos de esta instalación son tener instalado .Net framework 4.7 y abrir puerto 443 a *.atp.azure.com.



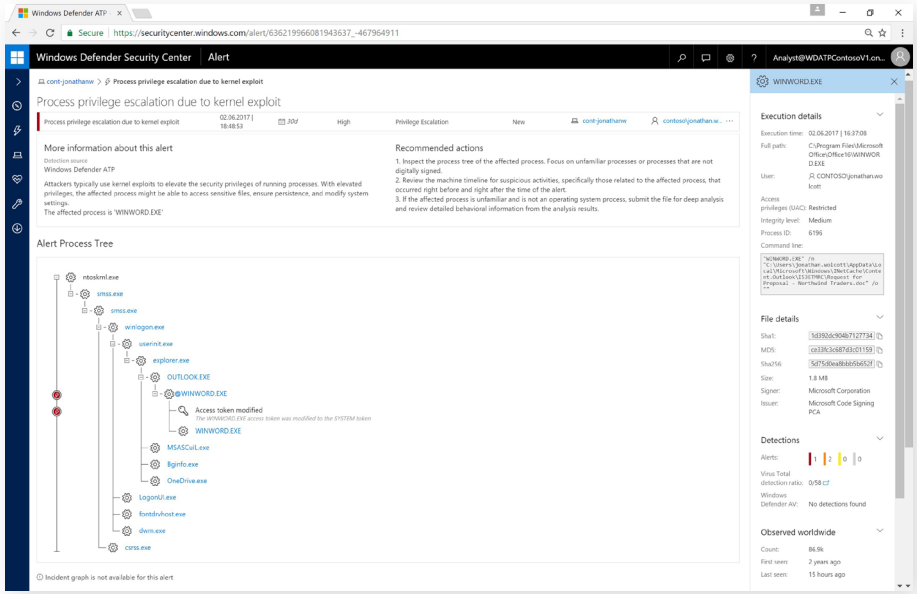
Funcionamiento

Una vez configurado el servicio y desplegado **el primer Workspace, el funcionamiento de AATP** es similar al de ATA, utilizando algoritmos de **Machine Learning** y el Microsoft Intelligent Security Graph para **detectar cualquier tipo de amenaza** antes de que pueda causar daños.

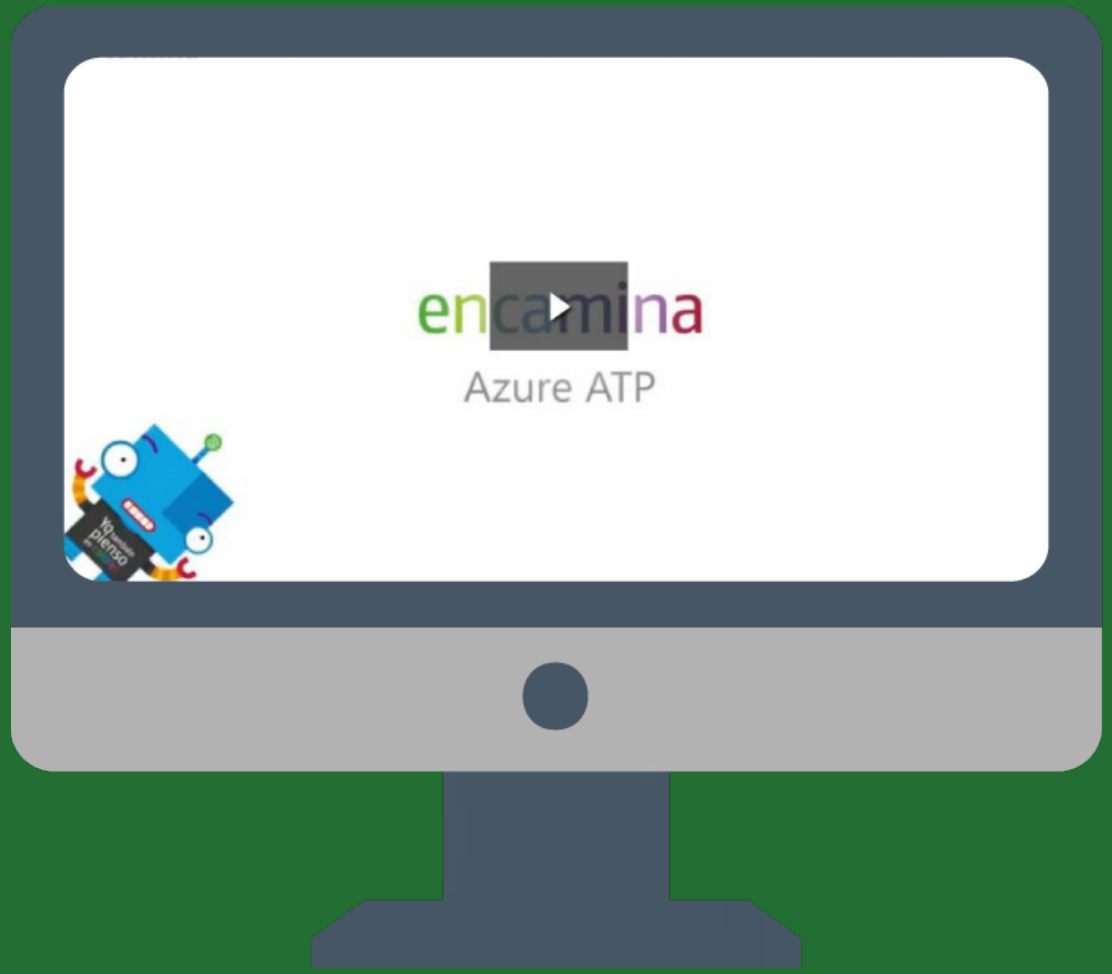


Las detecciones se muestran en una **línea de tiempo contextual**, donde cada alerta incluye una descripción de la actividad que la desencadenó, y los **pasos necesarios para solucionar el problema**.

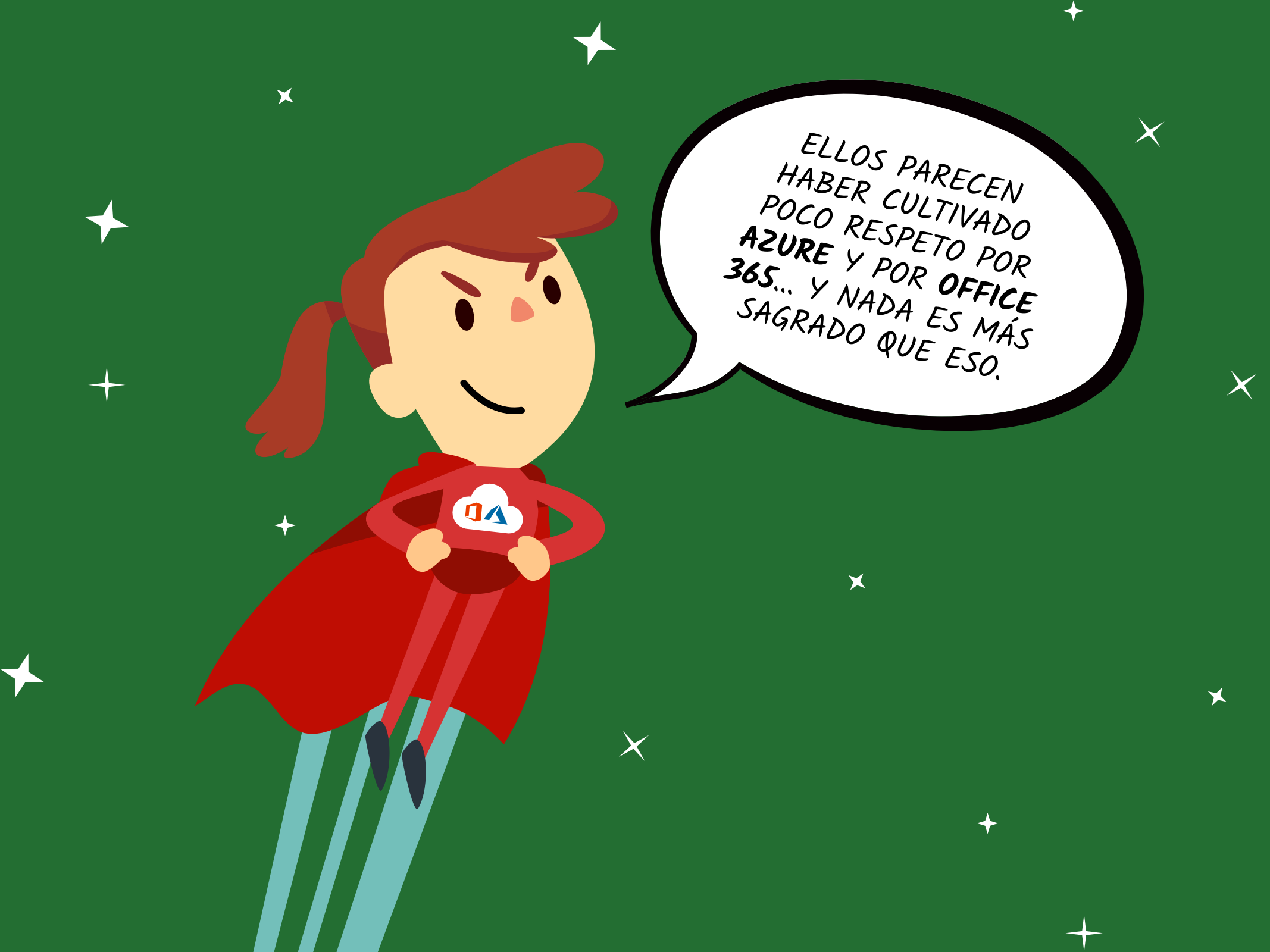
Además, para **profundizar en la investigación** de las alertas Windows Defender Advanced Threat Protection proporciona el contexto de las operaciones que se han realizado en las ubicaciones afectadas.



En el siguiente vídeo te mostramos cómo instalar, configurar, y empezar a usar AATP en unos pocos pasos:



Pablo Ortiz Baiardo
Former employee of ENCAMINA


ELLOS PARECEN HABER CULTIVADO POCO RESPETO POR **AZURE** Y POR **OFFICE 365**... Y NADA ES MÁS SAGRADO QUE ESO.

Cómo erradicar la sesión activa de un usuario en Office 365

Si detectamos un **uso anómalo y/o malintencionado en Office 365**, muchos podemos pensar que bloquear, eliminar la licencia, o eliminar al usuario en cuestión erradicaría el problema. Lo cierto es que no es así, ya que, si por ejemplo ha iniciado sesión en SharePoint Online, ésta permanecerá activa durante 4 horas hasta que expire la sesión.

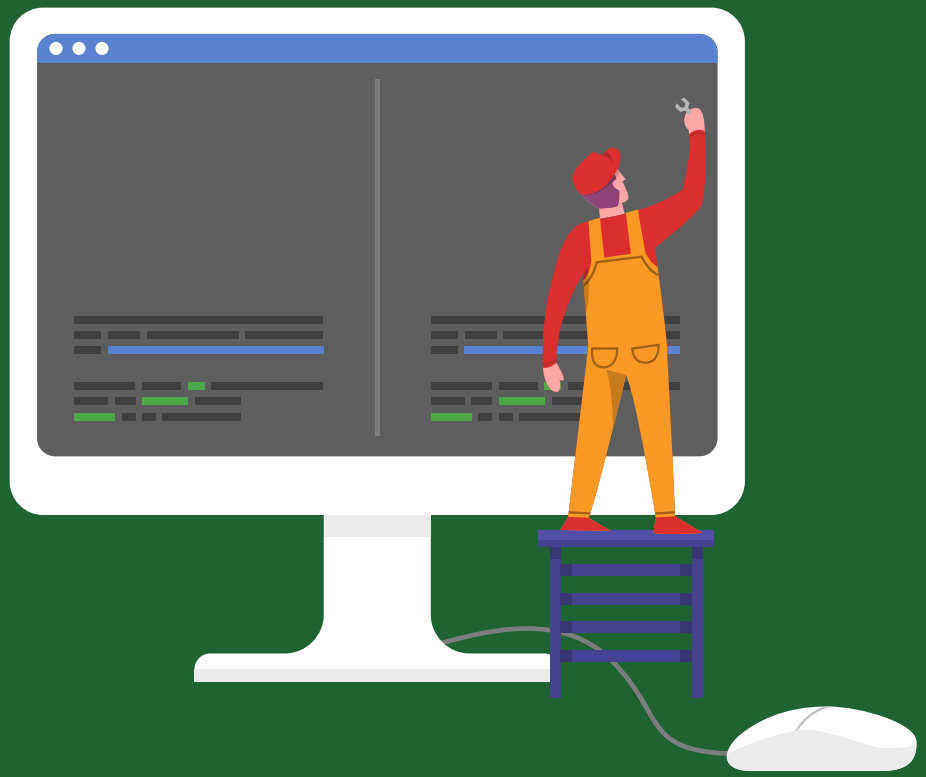
Cuatro horas son una eternidad cuando hablamos de un acceso no autorizado o amenaza, tiempo más que suficiente para hacerse con cualquier información sensible de la empresa, y nosotros sin poder hacer nada… ¿o tal vez sí?

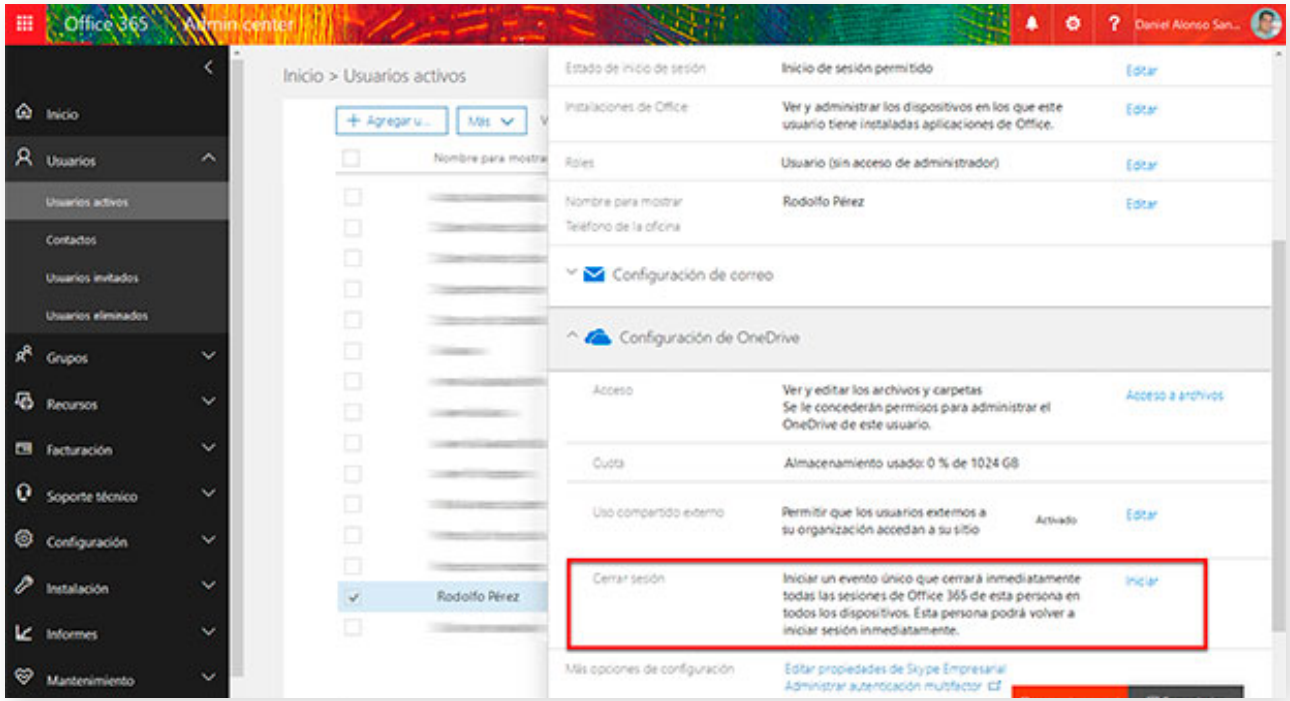
Por suerte, para estas situaciones tan comprometidas existen **tres opciones posibles** para revocar o erradicar la sesión activa del usuario.

Opción 1: Desde el panel de administrador

Si te sientes más cómodo con el **Admin Center de Office 365**, no hay ningún problema, sólo tienes que:

1. Iniciar sesión como administrador en Office 365 > Usuarios > Usuarios Activos.
2. Hacemos clic al usuario que queramos eliminar la sesión activa y pulsamos sobre **Configuración de OneDrive**.
3. Aquí encontraremos la opción de **cerrar sesión**. Al pulsar en **Iniciar**, se iniciará un evento único que cerrará inmediatamente todas las sesiones de Office 365 de este usuario en todos los dispositivos. Si el usuario está descargando algo, también se cortará la descarga.





Al instante se le cerrará la sesión al usuario, indicándole que **por motivos de seguridad, esta aplicación requiere que inicie sesión de nuevo**.

Aunque esto lo hemos hecho en un apartado llamado “Configuración de OneDrive”, se hace efectivo en todas las sesiones activas de Office 365, incluido SharePoint Online o Exchange Online.

Opción 2: Revocar sesiones con PowerShell

Esta segunda opción nos permite erradicar la sesión activa de un usuario de Office 365 utilizando **PowerShell**. Para ello vamos a utilizar el cmdlet de Revoke-SPOUserSession, disponible desde el módulo de SharePoint Online.

```
Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\dalonso> Connect-SPOService -URL https://alonsosanchis-admin.sharepoint.com -Credential $credential
PS C:\Users\dalonso> revoke-SPOUserSession -User rodolfo@alonsosanchis.onmicrosoft.com -Confirm:$false
We successfully signed out rodolfo@alonsosanchis.onmicrosoft.com from all devices.
PS C:\Users\dalonso>
```

Con este comando obtendremos el mismo resultado que si utilizamos el Admin Center, explicado en la primera opción. Sin embargo, este método es muy útil **si deseamos automatizar flujos de respuesta a incidentes de seguridad**, o si necesitamos revocar las sesiones activas de múltiples usuarios.

Opción 3: Revocar sesiones activas en cualquier aplicación AzureAD

Si además de acabar con la sesión activa de Office 365, deseamos hacerlo con CRM Online, Dynamics 365, Azure, etc, esta es la mejor opción. Para ello debemos utilizar el cmdlet Revoke-AzureADUserAllRefreshToken, disponible en el módulo Azure AD V2.

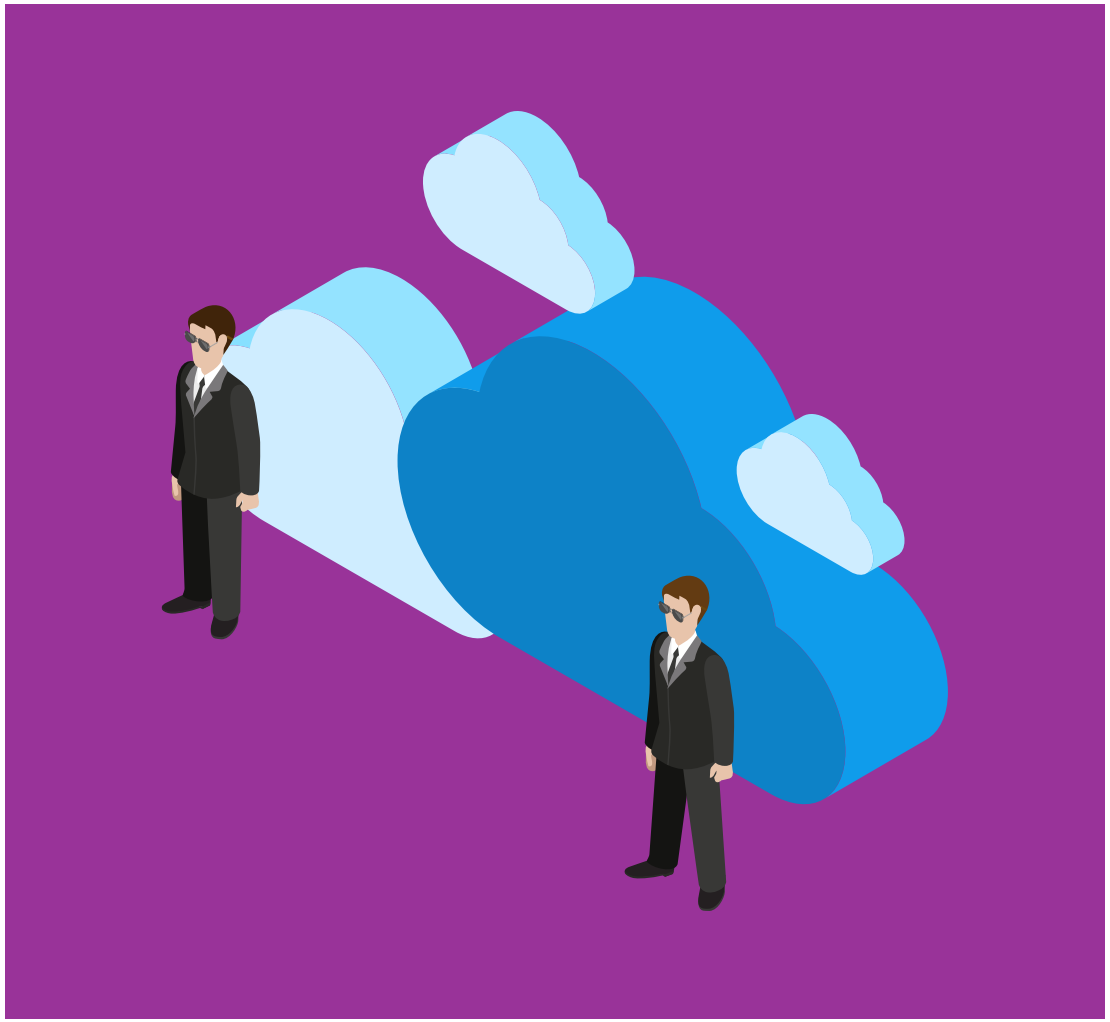
```
Windows PowerShell
PS C:\> Connect-AzureAD -Credential $credential

Account                             Environment TenantId                             TenantDomain AccountType
-------                             ----------- --------                             ------------ -----------
daniel@alonsosanchis.onmicrosoft.com AzureCloud  574a8271-f624-4e0f-8a55-4433c7c125a0 itpros.es    User


PS C:\> get-AzureADUser -SearchString rodolfo@alonsosanchis.onmicrosoft.com | Revoke-AzureADUserAllRefreshToken
PS C:\>
```

Con estas cualquiera de estas opciones, habremos logrado revocar la sesión activa al instante. Pero para estar seguros de que la información sensible de nuestra organización está a bien protegida, os recomiendo Azure RMS y AIP.

¿Quieres ver cómo se materializa todo esto? Pues no te pierdas el vídeo donde te lo explico todo, paso a paso, en 5 minutos ;)

Daniel Alonso Sanchis
Cloud Solutions Principal Advisor

Algunos elementos de seguridad en Azure



Microsoft está construyendo su plataforma de nube pública, Azure, **garantizando la seguridad de los datos de sus clientes**. En **Azure** se protege la privacidad de los datos y los clientes mantienen, en todo momento, la propiedad y el control de los mismos, asegurando que sólo son usados de una manera consistente con las expectativas de sus clientes.

Azure es el proveedor de cloud con más certificaciones, hecho que garantiza que la ejecución de los servicios esté construida con la calidad de **seguridad y privacidad** necesarias.

ISO/IEC CSA/CCM ITAR CJIS HIPAA IRS 1075

En el centro de confianza de Microsoft Azure, https://azure.microsoft.com/en-us/support/trust-center/, se puede entrar en más en detalle en estas certificaciones.

Con respecto al ámbito europeo, Microsoft mantiene las siguientes certificaciones:

> BIR 2012
> EN 301 549
> ENISA IAF
> EU Model Clauses
> EU-US Privacy Shield
> FACT
> IT Grundschutz Compliance Workbook
> NEN 7510:2011
> NHS IG Toolkit
> Spain ENS
> UK G-Cloud

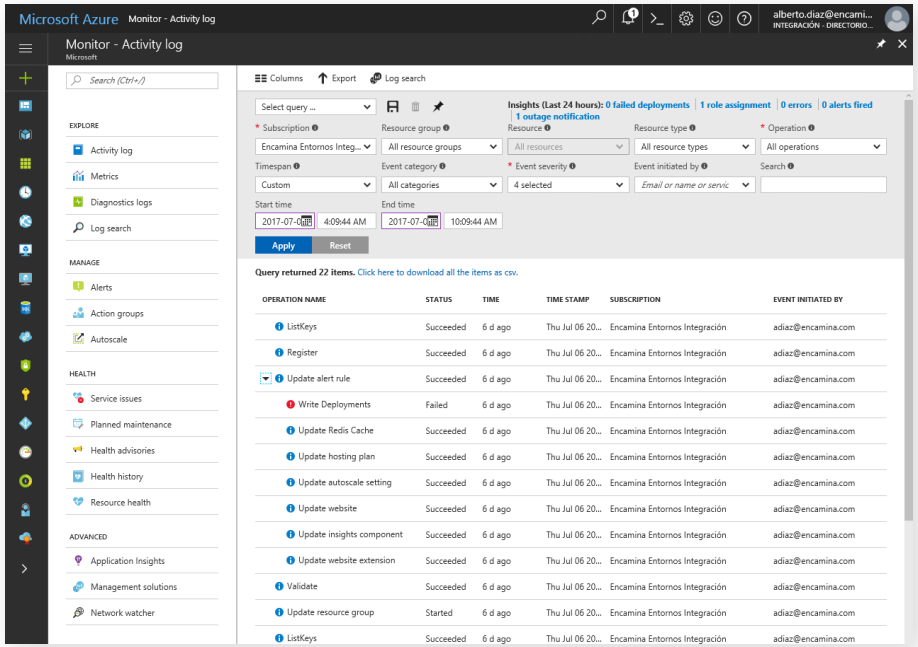
A nivel nacional, la Agencia Española de Protección de Datos (AEPD) ha reconocido la solvencia y garantía de los servicios de Microsoft Azure en lo relativo a **transferencias internacionales de datos**, lo que nos ofrece la posibilidad de exportar datos personales a Microsoft Corp. bajo el amparo de la Ley Orgánica de Protección de Datos (LOPD). En el siguiente enlace se puede descargar la resolución de la AEPD

Con respecto a la nueva GDPR, la ley de privacidad europea que entrará en vigor en mayo de 2018, Microsoft garantiza ya en sus contratos de Azure que sus clientes podrán cumplir con esta nueva ley en los siguientes puntos:

> Responder correctamente a las peticiones de modificación o borrado de datos personales
> Detectar y reportar brechas de seguridad sobre los datos personales
> Demostrar el cumplimiento con GDPR

Log de registro de cambios

Además, **Azure nos provee de un log de actividades** para registrar qué operaciones se realizan sobre los recursos, quién realiza las operaciones, cuando se realizan, el estado de las mismas y las propiedades y valores de los cambios realizados, de los últimos 90 días.



En la imagen podemos ver las operaciones que se han realizado en una suscripción de Azure, entre las que podemos destacar las siguientes:

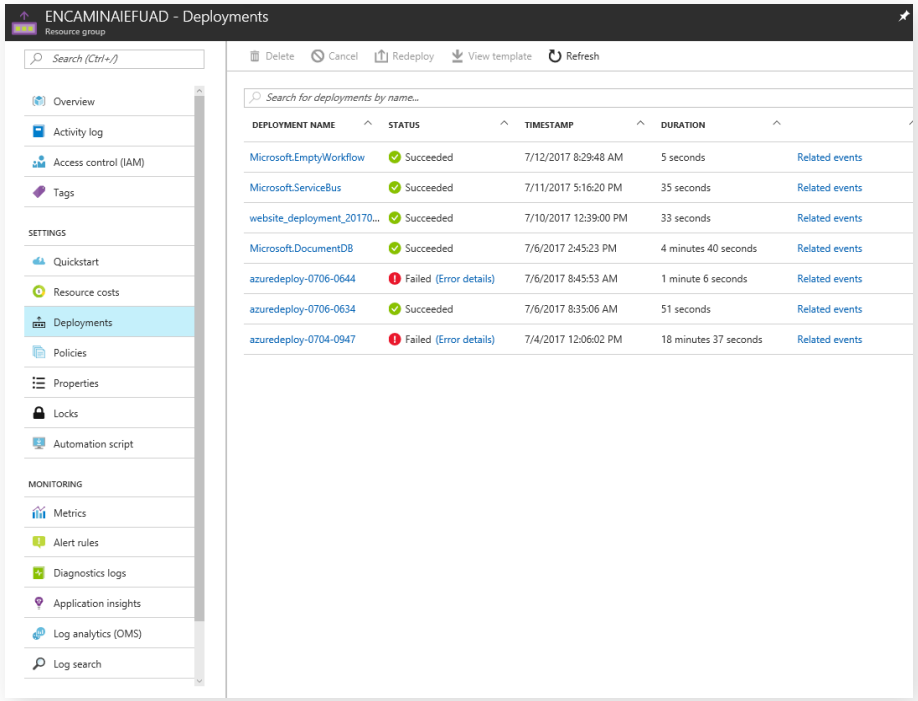
> Listado de claves de acceso.
> Actualizaciones de recursos (Redis Cache, website, hosting plan, ...).
> Actualización de grupo de recursos.

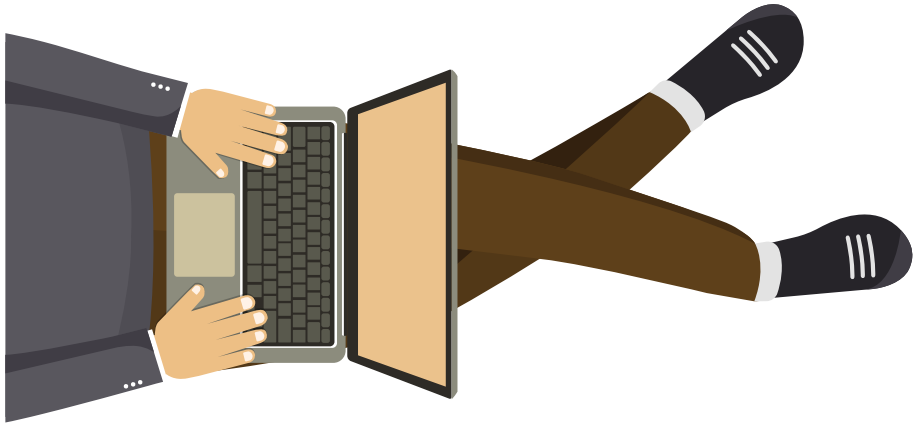
En las distintas suscripciones de un servicio, se agrupan de forma lógica **los recursos de Azure**.

Estos grupos de recursos nos permiten gestionar distintos factores como las operaciones de despliegue.

Este log nos provee de una vista de las operaciones que se realizan en los servicios de los grupos de recursos. Por una parte, **asegura que no se producen cambios no esperados**, y por otra, permite realizar un **diagnóstico detallado de**

los errores de despliegue como herramienta de resolución de problemas.





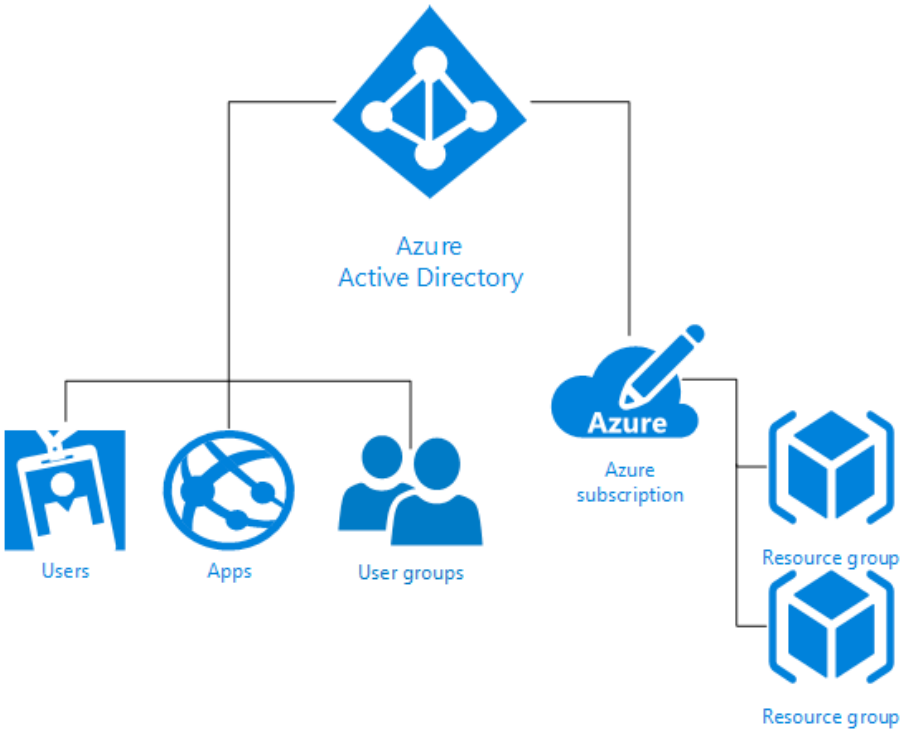
Control de acceso a los recursos basada en roles

Azure nos permite establecer control de acceso granular a los recursos de la suscripción utilizando el **Role-Based Access Control (RBAC)**.

Con RBAC asignamos sólo los permisos necesarios para que los usuarios puedan realizar su trabajo. Por ejemplo, podemos dar permisos a un usuario para visualizar los informes de Application Insight pero que no tenga permisos para modificar la configuración de este servicio.

Cada suscripción está asociada a un **Azure Active Directory** que RBAC usa para gestionar los usuarios, grupos y aplicaciones. Por defecto, RBAC usa los roles de Owner, Contributor y Reader, pero si fuera necesario, se pueden crear roles personalizados con los permisos necesarios.

El control de acceso se puede aplicar a nivel de Suscripción, grupo de recursos o recurso, con lo que garantizamos la simplicidad de la administración y la granularidad necesaria para dar los permisos adecuados a cada usuario.



Encriptado de la información sensible

Azure nos ofrece diversos mecanismos para mantener información sensible, por ejemplo, datos personales, encriptada en transporte y en almacenamiento.

- **Transport Layer Security / Secure Sockets Layer**, que nos permite cifrar simétricamente las comunicaciones, por ejemplo, de los sitios web.
- **Microsoft Azure Storage Service Encryption** para cifrar la información almacenada en Blob Storage.
- **Transparent Data Encryption**, tecnología que permite encriptar la información de las bases de datos de Azure SQL de forma transparente a las aplicaciones que tienen que hacer uso de estos.
- **Azure Key Vault**, servicio que ofrece la capacidad de administrar las claves de encriptación y/o de almacenar de forma segura y encriptar los valores de configuración de las aplicaciones web, usando una versión cloud de HSM (Hardware Security Module).

Seguridad en las comunicaciones

Azure App Service, el servicio PaaS de aplicaciones de Azure, administra la seguridad a nivel de infraestructura y plataforma, en los siguientes puntos básicos:

> Las aplicaciones se ejecutan en un entorno aislado seguro.
> Las comunicaciones entre recursos de Azure se ejecutan en la red segura de Azure y no cruzan redes públicas, además de ser comunicaciones encriptadas.
> La protección de recursos ante amenazas del tipo malware, DDoS, Man-in-the-middle y otras amenazas está activa las 24 horas del día.
> Las actualizaciones del sistema operativo son gestionados por el equipo de operaciones de Azure.

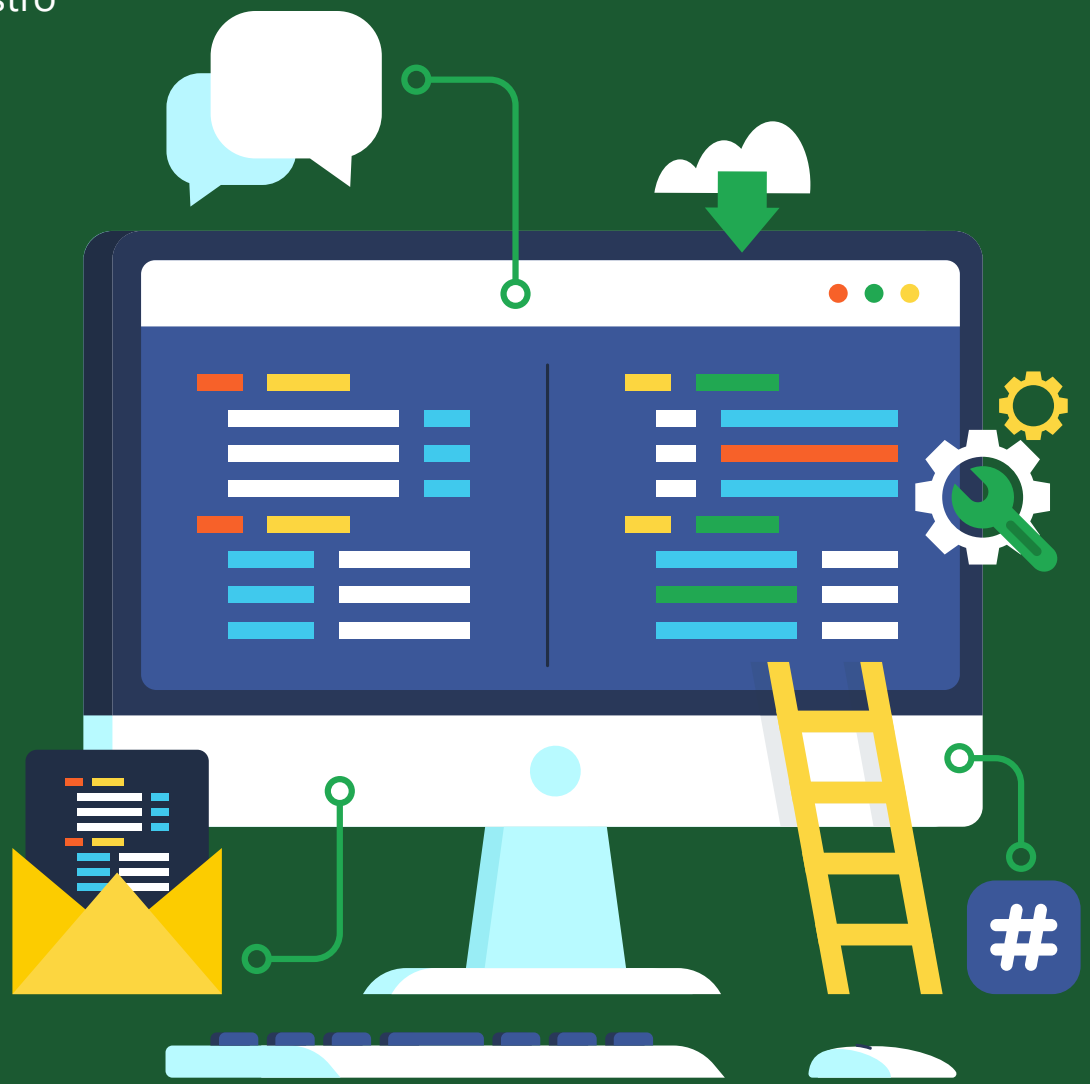
Si fuera necesario, podemos aumentar el nivel de seguridad que nos ofrece por defecto Azure, utilizando **Azure Application Gateway** configurado como **Web Application Firewall (WAF)** que nos ofrece una protección centralizada contra las vulnerabilidades de seguridad más comunes:

> SQL injection.
> Cross site scripting.
> Ataques web comunes (Command injection, HTTP request smuggling, HTTP response splitting, remote file inclusion).
> HTTP protocol violations.
> HTTP protocol anomalies (missing host user-agent, ...).
> Bot, crawlers and scanners

Todas estas reglas, configurables, están basadas en el conjunto de reglas OWASP (Open Web Application Security Project).

Algún elemento más de seguridad se me queda en el tintero, pero seguro que en este blog iremos

hablando sobre ellos. De momento, quedaos con la **gran ventaja que nos ofrece Microsoft en Azure para estar al día**, sin tener grandes problemas de seguridad y con poco esfuerzo, en comparación a lo que nos costaría tener este nivel en nuestro propio Datacenter.



Alberto Díaz Martín
CTIO

Protege tus reuniones de Skype Empresarial

Cuando implementamos **Skype Empresarial** como solución de comunicaciones unificadas para nuestras reuniones, nos damos cuenta de que gracias a ser una herramienta tan intuitiva, todos los usuarios se adaptan rápidamente a ella. Sin embargo, existen ciertas buenas prácticas que muchos ignoran, incluso tras llevar muchos años utilizando Skype Empresarial.

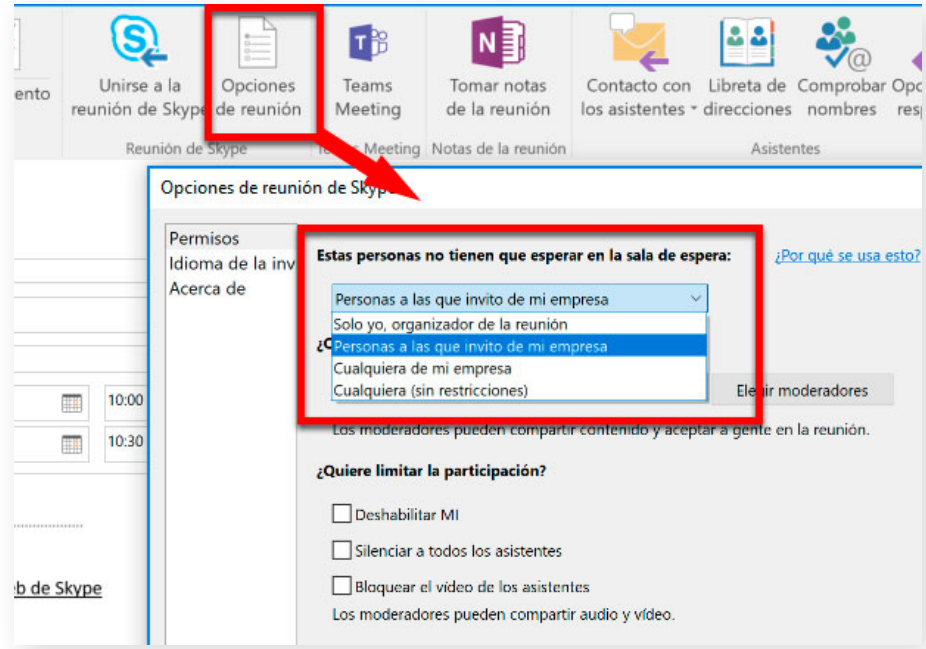
Si eres de los que habitualmente realiza o asiste a reuniones con Skype Empresarial, te habrás dado cuenta de que cuando el organizador crea una reunión inmediatamente después de terminar otra, los usuarios más puntuales de la segunda pueden

unirse a la reunión anterior, y si permanecen en silencio, podrían incluso estar escuchando todo… y nosotros sin enterarnos que están ahí :(

Para entender mejor la gravedad del asunto, vamos a exponer un buen ejemplo:

Imagina que organizas una reunión con la gerencia para discutir el futuro de un empleado, y dejas unos 15 minutos de espacio entre esa reunión y otra que tendrás con el empleado en cuestión, pero la reunión con gerencia se extiende varios minutos. Entonces el empleado se conecta temprano esperando en silencio, y te oye hablar de cómo despedirlo. Menuda situación, ¿no?

En Skype Empresarial existen varias opciones para organizar reuniones en línea, pero siempre solemos optar por la configuración predeterminada, que crea la reunión sin restricciones. Para proteger nuestras reuniones, sólo debemos irnos a las **Opciones de reunión** y hacer uso de la **sala de espera**.



En "**Estas personas no tienen que esperar en la sala de espera**", debemos cambiar la opción a cualquiera de las dos primeras. Las opciones están ordenadas de más restrictiva a menos.

A mi personalmente me gusta más la segunda opción, la que dice "**Personas a las que invito de mi empresa**", de este modo la sesión reconocerá a los miembros de mi empresa que he invitado a la reunión, tanto requeridos como opcionales, y a estos les permitirá acceder a la reunión sin tener que pasar por la sala de espera. Todos los

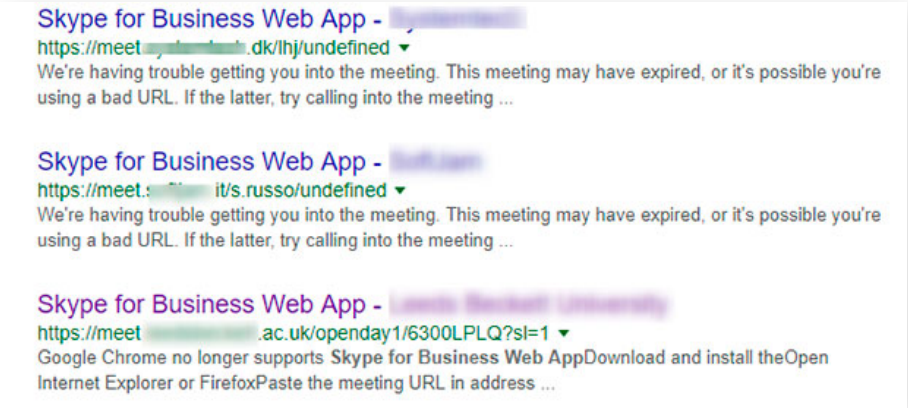
demás miembros (internos o externos), irán a la sala de espera hasta que les autoricemos a entrar en la reunión. Si pulsamos sobre "**recordar configuración**", ésta opción se establecerá como predeterminada para todas las reuniones que organicemos en el futuro.

¡Vayamos más allá!

¿Sabías que es relativamente fácil encontrar una sesión de reuniones en Internet? Incluso sin conocer la URL de la reunión dedicada. ¡Veámoslo!

Buscamos en Google "Skype for Business Web App", y nos vamos a la página 3 en adelante (aunque desde la primera página sería suficiente), allí veremos algunos resultados con URL tipo:

> https://join.domain.com/meet/user.name/meetid
> https://meet.domain.com/user.name/meetid



Si hacemos clic en alguno de los resultados, probablemente podremos permanecer de oyentes de una importante reunión privada, y si han agregado archivos adjuntos a la sesión, también conseguiremos acceder a ellos. Además, podemos unirnos a la reunión de manera completamente anónima desde la aplicación web de Skype for Business. ¡Así de sencillo! Escalofriante, ¿verdad?

Eso se agrava todavía más si el usuario organizador de la reunión tiene habilitada la licencia/característica de Conferencias RTC con un proveedor ACP, o directamente PSTN Conferencing, de modo que podríamos llamar a quien quisiéramos de manera gratuita.

¿Qué podemos hacer para evitarlo?

Como vimos antes, con hacer uso de las salas de espera lograremos proteger enormemente nuestras reuniones, pero desde el lado del administrador de sistemas también necesitamos tomar medidas para evitar la indexación, así como el empleo de políticas adecuadas para evitar el fraude o el espionaje.

Para ello debemos seguir las siguientes recomendaciones:

1) Aplicar directivas de conferencia:

Por PowerShell debemos aplicar una serie de políticas, con el cmdlet Set-CsConferencingPolicy. Con ellas lograremos:

> No permitir marcado a usuarios anónimos.
> Evitar que usuarios externos puedan guardar contenido.
> No permitir a usuarios externos registrar reuniones.
> Forzar el uso de la sala de espera a usuarios externos.

2) Es probable que necesitemos otras configuraciones de refuerzo. En este enlace encontraremos la configuración completa con muchos ejemplos:

https://technet.microsoft.com/es-es/library/gg425788.aspx

3) Evitar indexación en buscadores:

Si trabajamos con Skype for Business Online de Office 365, no será necesario. Pero si trabajamos con un escenario híbrido o 100% on-premises, debemos asegurarnos de evitar que los motores de búsqueda indexen las URLs de nuestras reuniones. Para ello tenemos dos métodos:

Método 1, utilizar un archivo robots.txt:

1. Nos vamos a la raíz del sitio web externo de Skype for Business, y creamos un archivo llamado **robots.txt**.
2. Añadimos el siguiente código y lo guardamos.

   *User-agent: **

   Disallow: /

Método 2, utilizar HTTP Response Header.

1. Abrimos el administrador de IIS, y hacemos clic en el nombre del servidor.
2. Abrimos **HTTP Response Headers**, y añadimos un nuevo registro.
   1. En el campo Nombre: **X-Robots-Tag**.
   2. En el campo Valor: **noindex**.

También podemos implementar el **módulo de SEO** desde IIS Web Gallery, y controlar las indexaciones a través de una interfaz de usuario más amigable. Aquí podremos encontrar más información:

https://docs.microsoft.com/en-us/iis/extensions/iis-search-engine-optimization-toolkit/managing-robotstxt-and-sitemap-files

¿Qué hacemos si nuestras reuniones ya están indexadas?

Además de todas las recomendaciones anteriores, si encontramos que nuestras reuniones han sido indexadas en los motores de búsqueda, lo recomendable es que inmediatamente volvamos a generar nuevas ID de conferencia, de modo que anularemos los enlaces existentes y dejarán de estar disponibles para unirse.

Además, desde las herramientas de Webmaster de los principales buscadores, podemos solicitar la eliminación de esos enlaces.

> Google: https://www.google.com/webmasters/tools/removals?pli=1

> Bing: https://www.bing.com/webmaster/tools/content-removal?rflid=1

Esperamos que con éstos consejos puedas disfrutar todavía más de tus reuniones de Skype Empresarial
;)

Daniel Alonso Sanchis
Cloud Solutions Principal Advisor

Nuestros autores:

Alberto Díaz Martín
CTIO

Con más de 15 años de experiencia en tecnologías Microsoft, actualmente es parte del equipo de Dirección de ENCAMINA. Organiza y participa en las conferencias más relevantes del mundo Microsoft en España. Autor de diversos libros, en 2013 entró a formar parte de la Dirección de CompartiMOSS, una revista digital sobre tecnologías Microsoft. Desde 2011 es Microsoft MVP en la categoría de Azure. Es fundador de TenerifeDev y coordinador de SUGES.

Daniel Alonso Sanchis
Cloud Solutions Principal Advisor

Apasionado de todas las tecnologías y plataformas, experto en ciberseguridad y soluciones cloud. Cuenta con más de 17 años de experiencia en ciberseguridad y arquitectura IT y desde 2011 forma parte del equipo de MVPs de Microsoft. Actualmente es Cloud Solutions Principal Advisor en ENCAMINA, puesto desde el cual se encarga de seguir impulsando nuestro liderazgo en soluciones Cloud y Office 365.

Pablo Ortiz Baiardo
Former employee of ENCAMINA

Especializado en seguridad e infraestructuras. Está certificado en MCSE Cloud Platform & Infrastructure, MCSE SharePoint, MCSE Productivity, MCSA Windows Server 2012. Es un apasionado de la tecnología Microsoft y disfruta con los proyectos de arquitectura y seguridad de Microsoft cloud. Actualmente es *Infrastructure & Cloud Consultant* en TOKIOTA.

encamina

PIENSA EN COLORES