UNIVERSIDAD DE CASTILLA-LA MANCHA

ESCUELA SUPERIOR DE INGENIERÍA INFORMÁTICA

MÁSTER EN CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

TRABAJO FIN DE MÁSTER

MITRE ATT&CK aplicado a la relación con los controles de seguridad en entornos Cloud

Silvia Cristina Gutiérrez Puertas

Septiembre, 2020

UNIVERSIDAD DE CASTILLA-LA MANCHA

ESCUELA SUPERIOR DE INGENIERÍA INFORMÁTICA

MÁSTER EN CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

TRABAJO FIN DE MÁSTER

MITRE ATT&CK aplicado a la relación con los controles de seguridad en entornos Cloud

Autor: Silvia Cristina Gutiérrez Puertas

Director: Pablo González

Septiembre, 2020

Resumen

En este documento se presenta la memoria de un Trabajo de Fin de Máster correspondiente al "Máster en Ciberseguridad y Seguridad de la Información", que explica la base de conocimiento MITRE ATT&CK relacionandolo con los controles de seguridad y buenas prácticas en entornos Cloud, con un enfoque en Azure.

Este documento respondera a preguntas tales como, por qué es fundamental, ahora más qué nunca, securizar entornos cloud, qué indicadores permiten detectar un ciberataque, que son TTPs y por que son tan importantes, cuales son las fases del ciclo de vida durante un ataque, que es MITRE ATT&CK y para qué se utiliza, qué controles de seguridad se recomienda implementar en entornos cloud, asi como buenas practicas que se pueden aplicar para una defensa en profundidad, con un enfoque en entornos Azure, y justificando qué acciones maliciosas mitigan, aplicando su relacion con MITRE ATT&CK.

Agradecimientos

A Pablo por su orientación durante el desarrollo de este trabajo.

A Jose Luís por su apoyo y por hacer posible este extraordinario Máster.

A todos los profesores por lo mucho que he aprendido gracias a ellos.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1. INTRODUCCIÓN

En este primer capítulo se explican la motivación que me ha llevado a la realización de este TFM, los objetivos y la planificación para la realización de éste. Finalmente, se concluye el capítulo, con una explicación de la estructura de la memoria, con el objetivo de que el lector pueda seguir este documento fácilmente.

1.1 MOTIVACIÓN

La elección de este proyecto está relacionada con la enorme aceleración que se ha producido recientemente en nuestra sociedad, donde muchas organizaciones se han tenido que transformar digitalmente, de una manera rápida inesperada, debido a la pandemia del COVID-19, usando tecnología en la nube para poder ofrecer sus servicios y permitir el teletrabajo a sus empleados. Esto unido al crecimiento de los ciberataques, que aprovechan esta excepcional situación que estamos viviendo, han motivado este trabajo sobre MITRE ATT&CK y la seguridad en Cloud.

1.2 OBJETIVOS

El objetivo principal de este Trabajo de Fin de Máster es desarrollar una guía de MITRE ATT&CK aplicando la relación con los controles de seguridad y buenas prácticas en entornos Cloud, con un enfoque en Azure.

Entre los objetivos secundarios se encuentran: ampliar mis conocimientos de seguridad en entornos Cloud, particularmente Azure, y sobre MITRE ATT&CK.

1.3 PLANIFICACIÓN

A continuación, se muestra un diagrama Gantt con la planificación de este TFM, donde se muestra las actividades realizadas, la ejecución en el tiempo y las horas aproximadas de dedicación por cada actividad.

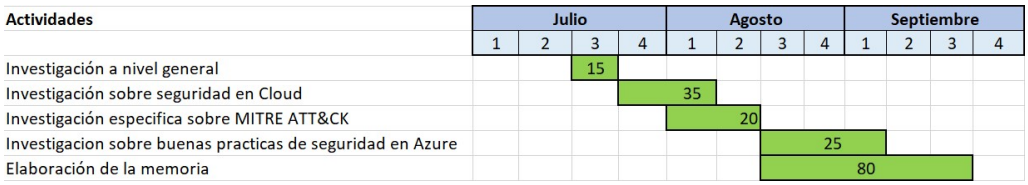

Figura 1. Diagrama Gantt con la planificación del TFM.

En la siguiente tabla se muestra el detalle de las actividades, así como las horas de dedicación, incluyendo el total.

Actividades	Horas dedicación aprox.
Investigación a nivel general	15
Investigación sobre seguridad en Cloud: lectura de libros, consultas en Internet (articulos, videos de conferencias, etc)	35
Investigación especifica sobre MITRE ATT&CK: consultas en Internet relacionadas con ATT&CK, Piramide del Dolor, Kill Chain, etc	20
Investigacion sobre buenas practicas de seguridad en Azure: lectura de guias, consultas en Internet	25
Elaboración de la memoria: creacion, revisiones, incorporación de comentarios del tutor, etc.	80
	Total: 175

Tabla 1. Detalle de las actividades del TFM.

1.4 ESTRUCTURA DE LA MEMORIA

En el capítulo segundo se presenta el estado del arte para proporcionar información contexto sobre la situación actual de entornos Cloud y de ciberataques.

A continuación, en el capítulo tercero se explican los indicadores de un ataque, y en el capítulo cuarto se presenta la Pirámide del Dolor, detallando los diferentes indicadores, especificando cuales son los más relevantes.

Seguidamente, en el capítulo quinto se explica el ciclo de vida de un ciberataque a través de la *Kill-Chain*.

En el capítulo sexto se explica con detalle que es MITRE ATT&CK, sus casos de uso, los componentes que forman el modelo ATT&CK, la matriz de Cloud, la de Azure. A continuación, se detallan los controles de seguridad y buenas prácticas para entornos Cloud, relacionando estos con las tácticas, técnicas y subtecnicas de ATT&CK. Cabe comentar que se ha usado la versión 7 de MITRE ATT&CK publicada en julio de este año.

Finalmente, en el capítulo séptimo se exponen las conclusiones del TFM, así como propuestas para trabajos futuros.

CAPÍTULO 2. Estado del Arte

A consecuencia de la pandemia de COVID-19, muchas organizaciones han trasladado la mayor parte de su actividad al mundo digital, adoptando de una manera rápida e inesperada el teletrabajo, lo que incluye el acceso remoto a sistemas e información que pueden ser de importancia crítica para sus negocios. El despliegue y uso de la tecnología en la nube está aumentando muy rápidamente para responder a la necesidad de digitalización de muchas organizaciones, y para hacer posible un masivo trabajo en remoto.

Se prevé que aumenten considerablemente los ciberataques, debido al contexto de escasez de tiempo y de recursos para esta transformación digital en muchas organizaciones, lo que aumenta sus riesgos de seguridad.

El trabajo desde casa es un concepto nuevo para muchas organizaciones, y los ciberdelincuentes se están aprovechando de la situación de incertidumbre como la que estamos viendo, ya que los empleados que no estén familiarizados con el trabajo en remoto y estén sometidos a una situación de estrés ocasionada por la pandemia pueden ser objetivos fáciles de ataques de phishing y de ingeniería social.

Cabe comentar que los ciberataques no van destinados exclusivamente a organizaciones, sino también a usuarios finales. Situaciones de confinamiento y una disminución de relaciones sociales y comerciales cara a cara han hecho que la actividad online personal se haya incrementado enormemente: videollamadas, compras y gestiones por internet son algunos de los ejemplos. Muchos usuarios han tenido que aprender y adaptarse rápidamente a entornos digitales completamente nuevos para ellos. Si esto lo unimos a una concienciación no suficientemente adecuada sobre riesgos de seguridad, vulnerabilidades en aplicaciones y sistemas, y una situación actual de incertidumbre, se forma con una combinación perfecta para muchos ciberataques.

Según datos de IBM[1] durante el primer trimestre de 2020, los ciberataques aumentaron un 40% a nivel mundial y un 125% en zona de Europa, Oriente Próximo y África, comparado con el mismo período del año pasado. Desde marzo se ha producido un incremento de más del 5.000% en el spam vinculado con el COVID-19.

Esta situación está acelerando que muchas organizaciones se conciencien de la importancia del papel que juega la ciberseguridad, particularmente, la respuesta ante incidencias y caza de amenazas ("*Threat Hunting*"). Esto último es "el proceso de búsqueda iterativa y proactiva a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes."[2], y como indica su definición, es la proactividad su principal característica, a diferencia de otras herramientas de seguridad como por ejemplo sistemas de gestión de información y eventos de seguridad (*SIEM, Security Information and Event Management*), sistemas de detección de intrusiones (*IDS, Intrusion Detection System*) y firewalls.

[1] Ciberseguridad en tiempos de la COVID-19: IBM alerta de un incremento de los ciberataques durante el primer trimestre de 2020, IBM https://es.newsroom.ibm.com/announcements?item=122574

[2] Cyber threat hunting, Wikipedia https://en.wikipedia.org/wiki/Cyber_threat_hunting

CAPÍTULO 3. Indicadores de Compromiso y de Ataque

En estos campos de la ciberseguridad, el uso de indicadores es crucial. Primeramente, vamos a explicar dos tipos de indicadores que existen: los indicadores de compromiso y los indicadores de ataque.

- **Indicadores de Compromiso (IOC)**: son un indicador que identifican un ataque en un sistema informático, evidenciando, con una alta probabilidad, que se haya producido una brecha de seguridad, es decir, que la seguridad ha sido comprometida.

  Un IOC es, por ejemplo, un hash de un archivo con malware, una IP o un dominio malicioso, un clave del registro, etc. Todos ellos han sido previamente clasificados como maliciosos. Es importante destacar que los IOCs ofrecen generalmente un método para reaccionar ante un ataque.

- **Indicadores de Ataque (IOA)**: indican que un ataque se está realizando, o todavía antes de que se convierta en una amenaza real. Se centran en detectar un intento de ataque sin considerar el malware o exploit usado. Indican, dentro de un determinado contexto, comportamientos anómalos que pueden ser una amenaza.

  Los IOAs, a diferencia de los IOCs, son un método proactivo.

Figura 2. Comparación entre IOCs y IOAs [6]

CAPÍTULO 4. La Pirámide del Dolor

La finalidad de estos indicadores es primeramente detectarlos, a continuación, responderlos lo más rápido posible, para finalmente bloquear al adversario que continúe utilizando esos indicadores. Sin embargo, no todos los indicadores son iguales, ya que algunos de ellos son más relevantes que otros.

Para ilustrar esta idea, el profesional de seguridad, David Bianco, publico en 2013 el concepto de "La Pirámide del Dolor" (*The Pyramid of Pain*). En esta pirámide se indica, por cada nivel, la relación entre los diferentes tipos de indicadores que se pueden utilizar para detectar las actividades de un adversario y cuánto dolor le causará cuando se pueda bloquear esos indicadores. Por tanto, la pirámide del dolor determina que indicadores son los más efectivos para detectar ataques.

En la siguiente figura se muestra un diagrama de la Pirámide del Dolor, cuyos niveles se describen a continuación.

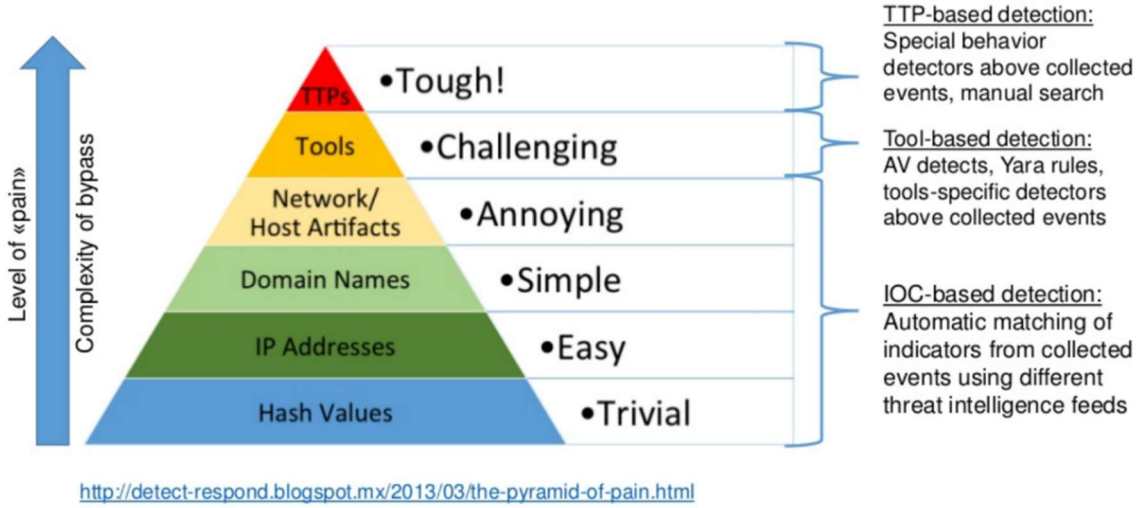

Figura 3. La Pirámide del Dolor de David Bianco.[13]

Valores Hash: los valores hash (SHA256, MD5, entre otros) sirven para identificar archivos maliciosos o sospechosos. En este nivel encontraríamos, por ejemplo, las muestras de malware.

Es muy fácil modificar el hash de un archivo, ya que cualquier cambio, por mínimo que sea, tendrá un hash diferente.

Direcciones IP: un atacante puede cambiar las direcciones IP fácilmente (VPNs, Tor, proxies, etc.).

Nombres de dominio: un atacante puede usar dominios, por ejemplo "evil.net" (o también subdominios). Estos son un poco más difíciles de cambiar, ya que deben estar registrados y los dominios nuevos podrían tardar un par de días en ser visibles en Internet.

Artefactos de red y de sistema operativo: los artefactos son causas observables de actividades maliciosas. Los artefactos de red son observables relacionados con el contenido de diferentes protocolos de tráfico, entre los cuales patrones URI, información C2 integrada en protocolos de red, valores diferenciadores de HTTP User-Agent, emails empleados en sus dominios (valores de SMTP Mailer) o certificados. Artefactos de sistema operativo serian, entre otros, claves de registro, nombres de mutex o servicios maliciosos.

A este nivel, si se detecta y se responde a estos indicadores, el atacante tendría que dedicar tiempo y esfuerzo para solucionar ese obstáculo, ya que tendría que analizar cómo fue detectado y probablemente adaptar sus herramientas.

Herramientas: son las herramientas o software que el atacante usa, por ejemplo, mimikatz, Windows Task Scheduler, GCC, Powershell, DLLs o ejecutables específicos, troyanos, etc.

Es muy frecuente que los atacantes usen las mismas herramientas que conocen y a las que están acostumbrados. Si podemos detectarlas y bloquearlas se rompe el flujo de trabajo del atacante, ya que tendría que buscar otras herramientas y aprender a usarlas, o crear herramientas nuevas.

Tácticas, Técnicas y Procedimientos (TTP): son los pasos que el adversario realiza durante el ataque. Algunos ejemplos serian, ataques "Pass-the-Hash", y *Spearphising* con un PDF adjunto que contiene un troyano.

Si se responde a este nivel, se actúa directamente contra el comportamiento y los hábitos del atacante (no contra sus herramientas), por lo tanto, se le obliga a modificar su modus operandi, que es lo que más "dolor" le puede causar, ya que le supone aprender nuevos comportamientos, para lo que necesitaría emplear mucho tiempo y esfuerzo, por lo que o bien se daría por vencido, o tendría que reinventarse.

Cada nivel de la pirámide constituye una oportunidad de detectar y prevenir ataques. Sin embargo, casi todos los indicadores que hemos visto tienen un valor que no es permanente, es decir, va cambiando con el paso del tiempo, ya que los atacantes evolucionan y se adaptan a nuevas herramientas y servicios.

Las Tácticas, Técnicas y Procedimientos (TTP) constituyen los indicadores más valiosos y efectivos para detectar ataques, ya que reflejan el comportamiento de un atacante y ayudan a comprender la forma en la que realiza sus ataques. Detectar y prevenir estos indicadores implica hacer más "doloroso", y, por tanto, más costoso para el atacante conseguir su objetivo.

CAPÍTULO 5. Cyber Kill-Chain

Cyber Kill Chain es un framework que fue desarrollado como un método avanzado para prevenir y detectar un ciberataque. Fue publicado en 2011 por la organización Lockheed Martin.

Este framework muestra el ciclo de vida de un ciberataque, es decir, las fases que un adversario realiza durante un ciberataque, especificadas en siete pasos:

1. **Reconocimiento** (*Reconnaissance*): Selección del objetivo, obtención de la mayor información que sea posible, intentando identificar las vulnerabilidades.

2. **Armamento** (*Weaponization*): Basado en la información adquirida durante la etapa de reconocimiento, el adversario elige las herramientas más apropiadas para realizar el ataque (ej. un malware).

3. **Entrega** (*Delivery*): El adversario lanza el "arma" contra el objetivo, por ejemplo, mediante un correo adjunto, un sitio web o un disco USB.

4. **Explotación** (*Exploitation*): explota la vulnerabilidad al ejecutar el código en el sistema de la víctima.

5. **Instalación** (*Instalación*): también es conocida como la fase de Ejecución. Instala una "Puerta trasera" (backdoor) para ser usada por el adversario.

6. **Comando y Control** (*Command and Control, C&C*): establece un canal de comando que hace que el adversario pueda manipular remotamente el sistema de la víctima.

7. **Acciones sobre Objetivos** (*Actions on Objective*): lleva a cabo la acción para lograr sus objetivos, la más común es Exfiltración, pero también puede ser destrucción o encriptación de datos.

Las tácticas de MITRE ATT&CK corresponden con las últimas etapas de *la Cyber Kill Chain* como se muestra en la siguiente figura. Estas proporcionan un mayor nivel de granularidad para describir que es lo que ocurre durante una intrusión.

MITRE PRE-ATT&CK contiene las tácticas y técnicas relacionadas con lo que los adversarios hacen antes de intentar explotar una red o sistema, por lo tanto, se centra en las etapas de Reconocimiento, Armamento y Entrega de la *Cyber Kill Chain*.

En la siguiente figura se muestra las siete etapas de la Cyber Kill Chain, con la relación con PRE-ATT&CK y ATT&CK.

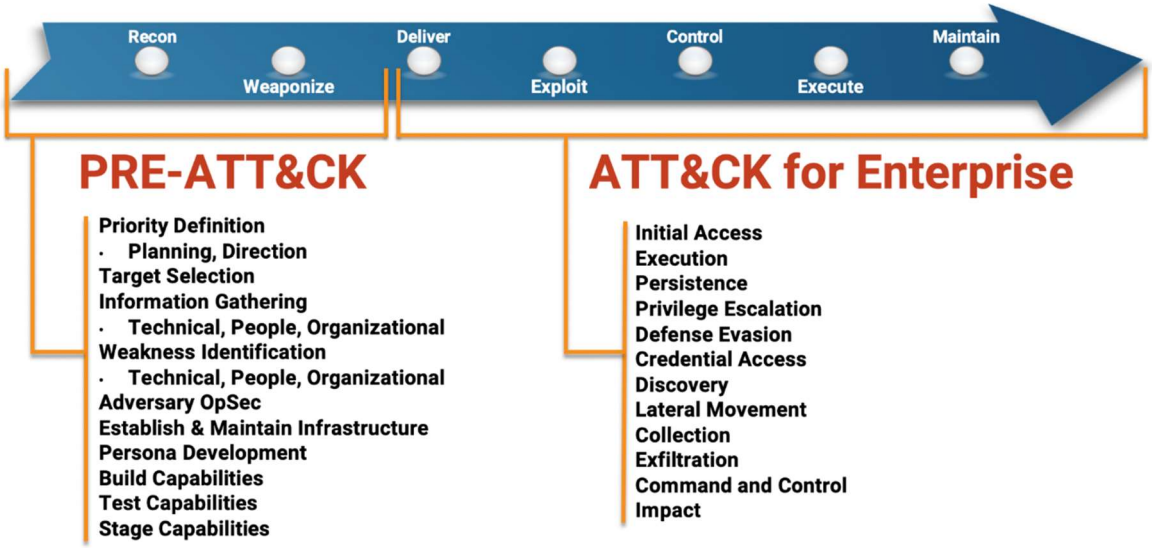

Figura 4. Diagrama de Cyber Kill Chain con la relación PRE-ATT&CK y ATT&CK [19]

CAPÍTULO 6. MITRE ATT&CK

6.1 INTRODUCCIÓN

ATT&CK se creo en 2013, y estaba enfocado a entornos Windows. MITRE lo define como "una base de conocimiento accesible globalmente de tácticas y técnicas adversarias basadas en observaciones del mundo real."[3].

En ATT&CK se modela el comportamiento de adversarios, considerando las diferentes fases del ciclo de vida de un ataque, centrándose en cómo los adversarios comprometen e interactúan con los sistemas y redes durante un ataque.

Esta base de conocimiento se utiliza como fundamento para el desarrollo de modelos y metodologías de amenazas específicas, tanto por organizaciones privadas como por gobiernos, así como por el sector de productos y servicios de ciberseguridad.

ATT&CK es gratuito, abierto, e impulsado por la comunidad.

6.2 CASOS DE USO DE ATT&CK

Emulación de Adversarios

Permite diseñar escenarios que imitan ataques de adversarios aplicando inteligencia de ciber amenazas, esto es, usando la información contenida en ATT&CK para entender cómo específicos grupos de adversarios realizan los ataques.

[3] MITRE ATT&CK https://attack.mitre.org/

El objetivo principal de la emulación de adversarios es verificar la eficiencia de controles preventivos, las capacidades de detección y de respuesta frente a las "técnicas" usadas en esos ataques.

Algunas herramientas para automatizar la emulación de adversarios son *CALDERA*, que realiza comportamientos adversarios post-compromiso dentro de redes Windows [62]; *Infection Monkey*, que simulador de brechas y ataques [63] y *ATTPwn*, enfocado para entornos Windows a través del uso de Powershell [64].

La siguiente figura un diagrama a alto nivel de la estructura general del plan de emulación del grupo FIN6, donde se aprecia las diferentes fases.

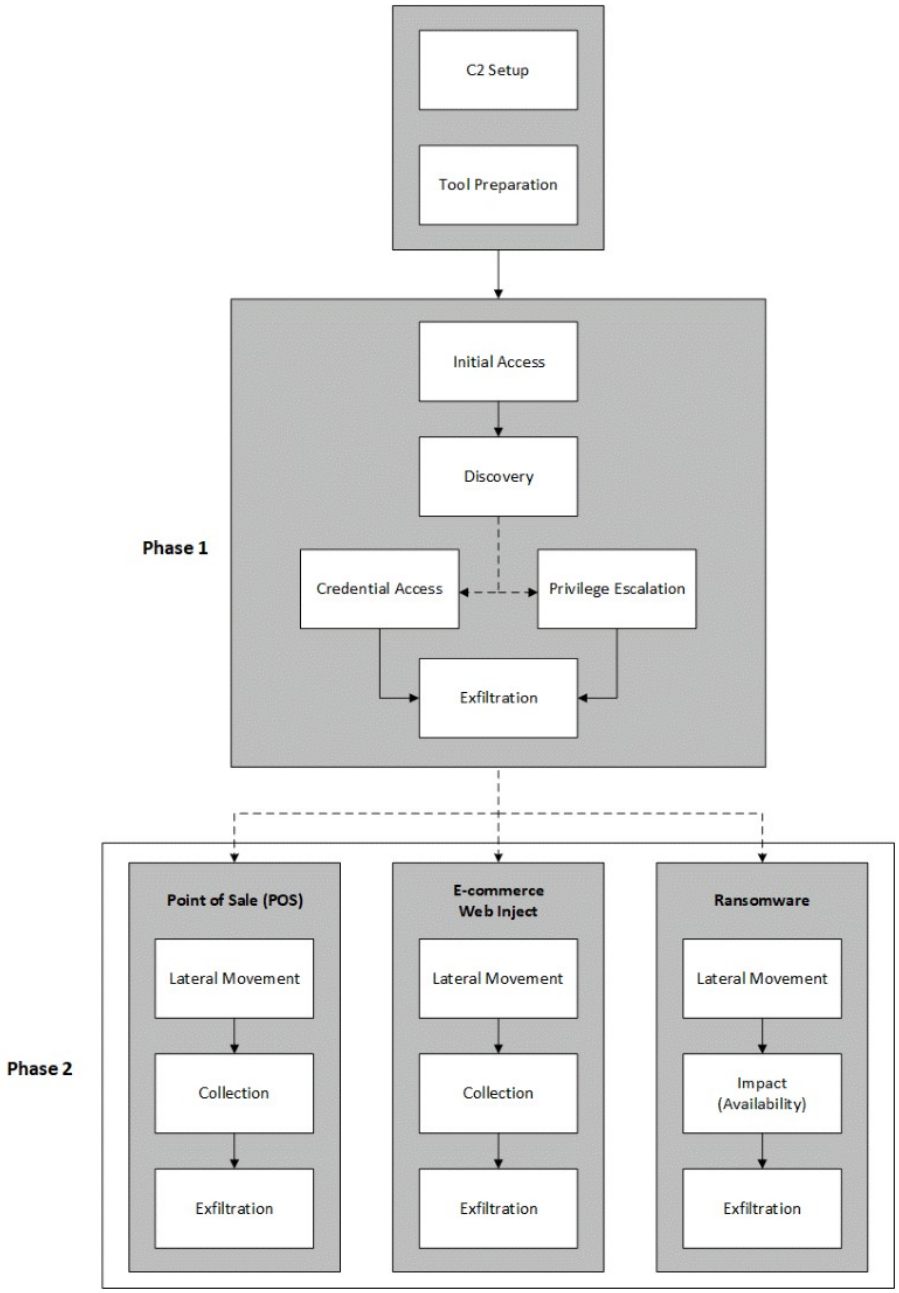

Figura 5. Diagrama de la estructura general del plan de emulación del grupo FIN6.[18]

Red Teaming

ATT&CK puede servir para diseñar ejercicios de red team para evitar determinados controles de seguridad implementados dentro de la red. Un ejercicio de red team implica la emulación de una amenaza realista, usando TTPs. El objetivo es no ser detectado para evaluar el nivel de prevención y detección.

Desarrollo de Análisis de Comportamiento

Se puede utilizar analítica de detección de comportamiento para reconocer actividad maliciosa.

Se puede usar ATT&CK para diseñar y probar analíticas de comportamiento para detectar ataques basándose en como los adversarios interactúan con el sistema o red indistintamente de las herramientas que pudieran usar, indicadores de compromiso (IoCs) o hashes.

Evaluación de Brechas Defensivas

Una evaluación de brechas de defensa tiene el objetivo de identificar los puntos que carecen del suficiente nivel de defensa.

Se puede usar ATT&CK para evaluar las áreas de la infraestructura de una organización que carecen de controles de seguridad y/o visibilidad. Estas áreas son potenciales vectores de "entrada" por los que un atacante (o adversario) podría acceder sin que fuera detectado, o sin que el ataque fuera mitigado.

ATT&CK se puede utilizar para valorar y comparar herramientas de ciberseguridad, así como el nivel de monitorización y defensa de una infraestructura.

Evaluación del nivel de madurez de Centros de Operaciones de Seguridad

El nivel de madurez o desarrollo de un Centro de Operaciones de Seguridad (SOC en inglés) puede medirse con ATT&CK, ya que permite evaluar la eficiencia en los procesos para monitorizar, detectar y actuar ante ciberataques.

Enriquecimiento de Inteligencia de Ciberamenazas

La inteligencia de ciberamenazas abarca el conocimiento de los grupos de adversarios que realizan ciberataques, sus TTPs (Tácticas, Técnicas y Procedimientos), herramientas que utilizan, malware, su comportamiento, etc.

Es importante conocer estos grupos desde el punto de vista de cómo actúan normalmente, independientemente de las herramientas que pudieran utilizar. El conocimiento de estos grupos desde una perspectiva de su comportamiento se puede entender con ATT&CK.

Entre mejor se entienda a los grupos de adversarios más eficiente puede ser la defensa frente a ellos. En consecuencia, analistas de seguridad pueden priorizar defensas enfocadas contra determinados grupos de adversarios, o focalizar defensas en técnicas usadas por múltiples grupos, según sea lo más conveniente en cada caso.

6.3 COBERTURA DE ATT&CK, VISIBILIDAD Y ATRIBUCION

ATT&CK es un modelo, y como todos los modelos, son aproximaciones a la realidad, por lo que tienen sus limitaciones. Es fundamental destacar que es poco realista la detección de cada técnica definida en ATT&CK, por lo tanto, no es posible una cobertura del 100%. Además, las técnicas pueden tener muchos procedimientos, es decir, como un adversario implementa una técnica. Algunas pueden no estar documentadas en ATT&CK, esto unido a que los adversarios están continuamente cambiando y evolucionado, imposibilita conocer todos los procedimientos con antelación.

Por otro lado, no todas las técnicas deberían generar una alerta. Existen acciones que pueden ocurrir normalmente en cualquier ambiente, por ejemplo, el uso de ipconfig.exe o Powershell, sin la necesidad de ser de naturaleza maliciosa. Es decir, hay un importante solapamiento entre técnicas de un atacante, funcionalidad del sistema operativo y operaciones normales de TI. Por ello se debería analizar cuestiones tales como, la frecuencia de que eso ocurra en el entono, si es posible asociarlo con un proceso legítimo, o cómo de normal es que esa acción la realice el usuario o servidor especifico. Por lo tanto, es el contexto de estas acciones lo que podría indicar si una acción es maliciosa o no.

Visibilidad es un concepto clave a la hora de trabajar con ATT&CK. Esto está relacionado con poder recopilar la información necesaria en los sistemas para que se pueda prevenir, detectar y responder ante amenazas. ATT&CK puede ayudar a identificar los vacíos en visibilidad.

Otro aspecto que destacar es la atribución. ATT&CK contiene información sobre los adversarios conocidos y grupos que han utilizado determinadas técnicas en el pasado. “Multitud de grupos dentro de ATT&CK usan las mismas técnicas. Por esta razón, no es recomendable atribuir la actividad únicamente basándose en las técnicas de ATT&CK usadas. La Atribución a un grupo es un proceso complejo que no implica únicamente el uso de TTPs por parte del adversario” [MIT20].

6.4 MODELO ATT&CK

El fundamento de ATT&CK es un conjunto de técnicas y subtecnicas que representan acciones que adversarios pueden realizar para lograr sus objetivos.

6.4.1 La Matriz ATT&CK

La Matriz ATT&CK es la representación visual de las relaciones entre tácticas, técnicas y sus técnicas.

MITRE tiene definidos tres dominios tecnológicos: Enterprise (representa las redes empresariales tradicionales y tecnologías en la nube), Mobile (para dispositivos móviles) y ICS (para Sistemas de Control Industrial), con las correspondientes matrices:

- Enterprise
  - Windows
  - macOS
  - Linux
  - Cloud: incluye las matrices para AWS, GCP, Azure, Office 365, Azure AD y SaaS.
- Mobile: incluye las matrices para Android y iOS.
- ICS (Industrial Control Systems)

También se encuentra definida la matriz PRE-ATT&CK.

A continuación, se muestra las tácticas y subtecnicas para la Matriz ATT&CK para Enterprise.

Figura 6. Matriz ATT&CK para Enterprise [MIT20].

6.4.2 Tácticas

Las tácticas representan el objetivo táctico de un adversario, es decir, la razón por la que realiza una acción. Por ejemplo: escalada de privilegios o exfiltración.

6.4.3 Técnicas y Subtecnicas

Las técnicas representan la manera en la que un adversario realiza una táctica. También representa lo que el adversario obtiene cuando realiza una acción. Existen muchas técnicas dentro de una táctica, ya que existen muchas maneras diferentes de alcanzar un objetivo táctico. Ejemplos de técnicas son fuerza bruta o manipulación de cuentas.

Algunas técnicas pueden dividirse en sub-tecnicas en las que se describe con más detalle las acciones realizadas por un adversario.

6.4.4 Procedimientos

Los procedimientos son las implementaciones especificas (como por ejemplo herramientas) que los adversarios usan para las técnicas y subtecnicas.

En la siguiente figura se representa la matriz ATT&CK con los diferentes componentes de esta: tácticas y técnicas, con el detalle de procedimientos para la técnica *Spearphising Attachment*.

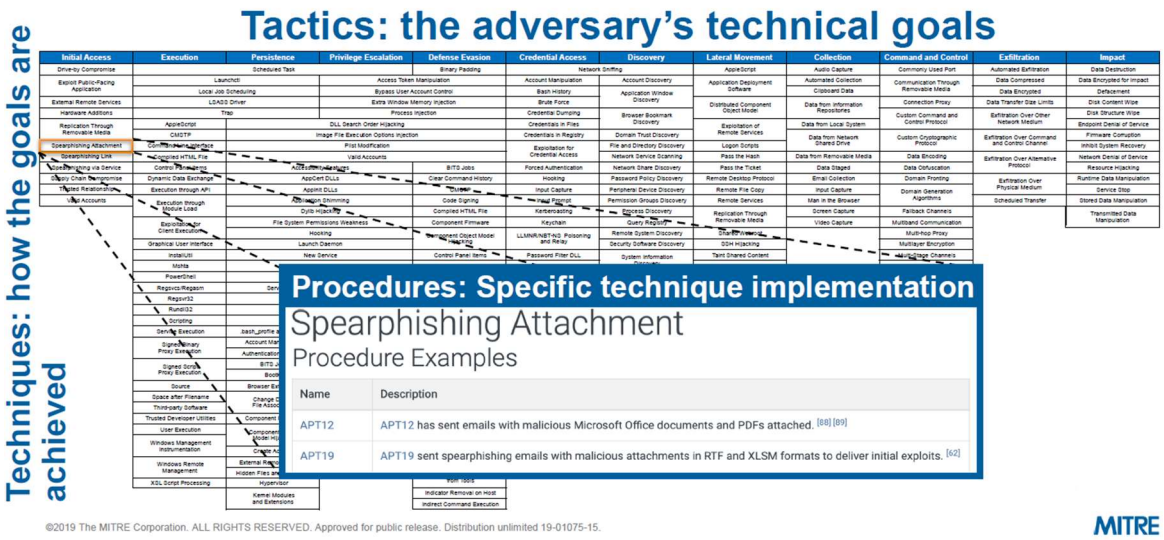

Figura 7. Desglose Modelo ATT&CK. Fuente: MITRE.

6.4.5 Grupos

Son los adversarios conocidos, monitorizados por organizaciones y que aparecen en informes de inteligencia de amenazas. Ejemplos: APT12, APT29 y FIN6.

6.4.6 Software

Los adversarios normalmente utilizan diferente software durante las intrusiones. El software se divide en herramientas y malware.

6.4.7 Mitigaciones

Representan los controles de seguridad que se pueden usar para evitar que un atacante lleve a cabo una tecnica o subtecnica con exito.

6.5 TÁCTICAS EN CLOUD

MITRE ATT&CK define las siguientes tácticas para Cloud.

Nombre	Descripción
Acceso Inicial	El atacante está intentando acceder a la red.
Persistencia	El atacante está intentando mantener el acceso.
Escalada de Privilegios	El atacante está intentando obtener un nivel de permisos más alto.
Evasión de medidas de defensa	El atacante está intentando que no sea detectado.
Acceso a Credenciales	El atacante está intentando robar credenciales.
Descubrimiento	El atacante está intentando entender el entorno.
Movimiento Lateral	El atacante está intentando moverse por el entorno.
Recopilación	El atacante está intentando recopilar información de interés para su objetivo.
Exfiltración	El atacante está intentando robar datos.
Impacto	El atacante está intentando manipular, interrumpir o destruir sistemas y datos.

Tabla 2. Tácticas para Cloud de MITRE ATT&CK

Acceso Inicial

El atacante está intentando acceder a la red.

La táctica de "Acceso Inicial" consta de técnicas para conseguir acceder a una red por primera vez. Una técnica dentro de esta táctica es el uso de contraseñas robadas de un usuario o servicio para ganar el acceso inicial, esto sería la técnica 'Valid Accounts'. Otro ejemplo es explotar vulnerabilidades en servidores web públicos.

Persistencia

El atacante está intentando mantener el acceso.

La Persistencia es una táctica que engloba técnicas que permiten al atacante continuar teniendo acceso una vez que lo ha conseguido, incluso en situaciones en las que se pudiera cortar su acceso como el caso de reinicios de sistemas, cambios de credenciales y otras interrupciones. Técnicas usadas de persistencia son cualquier acceso, acción o cambios en configuración que permita al atacante mantener el acceso.

Escalada de Privilegios

El atacante está intentando obtener un nivel de permisos más alto.

Esta táctica tiene como finalidad obtener un nivel más alto de privilegios en un sistema o red. Normalmente el atacante puede acceder y explorar una red con un acceso no privilegiado, sin embargo, necesita permisos elevados para llegar a lograr sus objetivos.

Esta táctica únicamente contiene una técnica para Cloud, "Valid Accounts": el atacante ya ha accedido, y utiliza una cuenta comprometida para explorar el sistema o red buscando vulnerabilidades tales como cuentas de usuario con permiso de administrador (o con acceso a un sistema especifico o bien con permisos para llevar a cabo alguna función determinada) o configuraciones erróneas.

Evasión de medidas de defensa

El atacante está intentando que no sea detectado.

Esta táctica consiste en técnicas que el atacante usa para no ser detectado. Hay muchas maneras que puede utilizar para lograr evadirse de medidas de defensa, por ejemplo, desinstalando o deshabilitando software de seguridad, ofuscando o encriptando datos o scripts, aprovecharse de procesos de confianza para ocultar malware. Un ejemplo de una técnica seria la ya menciona en anteriormente, “Valid Account”.

Acceso a Credenciales

El atacante está intentando robar credenciales.

Acceso a Credenciales es la táctica en la que el atacante está intentando obtener nombres de cuentas y contraseñas. Algunas técnicas para lograr esto es recolectar la información que un usuario teclea (keylogging) o extraer credenciales de la memoria, uso de fuerza bruta (intento masivo de probar usuarios y contraseñas). Si el atacante puede usar credenciales legitimas entonces puede acceder a sistemas, se dificulta que sea detectado, y tiene la posibilidad de crear más cuentas que le ayudan a conseguir sus objetivos.

Descubrimiento

El atacante está intentando entender el entorno.

Aquí se incluyen las técnicas que el atacante usa para obtener más información sobre el sistema o red, y que le ayudan a explorar, orientarse en el entorno y decidir más adecuadamente como seguir actuando.

Movimiento Lateral

El atacante está intentando moverse por el entorno.

El Movimiento Lateral comprende técnicas que usa el atacante para acceder y controlar otros sistemas en la red, moviéndose o privotando a través de diferentes sistemas. Puede instalar sus propias herramientas para el acceso remoto o usar credenciales legitimas usando herramientas nativas de red y del sistema operativo.

Recopilación

El atacante está intentando recopilar información de interés para su objetivo.

Esta táctica consiste en técnicas relacionadas con la recopilación de datos e información, que posteriormente el atacante puede robar (exfiltrar). Las fuentes de datos que normalmente son objetivo son unidades de almacenamiento, navegadores, video, audio y email. Entre los métodos más comunes de recopilación se encuentran capturas de pantalla y la entrada del teclado.

Exfiltración

El atacante está intentando robar datos.

La exfiltración es la técnica que agrupa técnicas en las que el adversario usa para robar datos fuera de la red. Es frecuente la compresión y encriptación de los datos para que la exfiltración pase desapercibida.

Impacto

El atacante está intentando manipular, interrumpir o destruir sistemas y datos.

Esta técnica consiste en técnicas para afectar la disponibilidad de sistemas, o destruir o alterar datos. El adversario puede usar estas técnicas para lograr alcanzar su objetivo.

A continuación, se muestra las tácticas y técnicas que representan la matriz ATT&CK para Cloud. Esta matriz contiene información de las plataformas: AWS, GCP, Azure, Azure AD, Office 365 y SaaS.

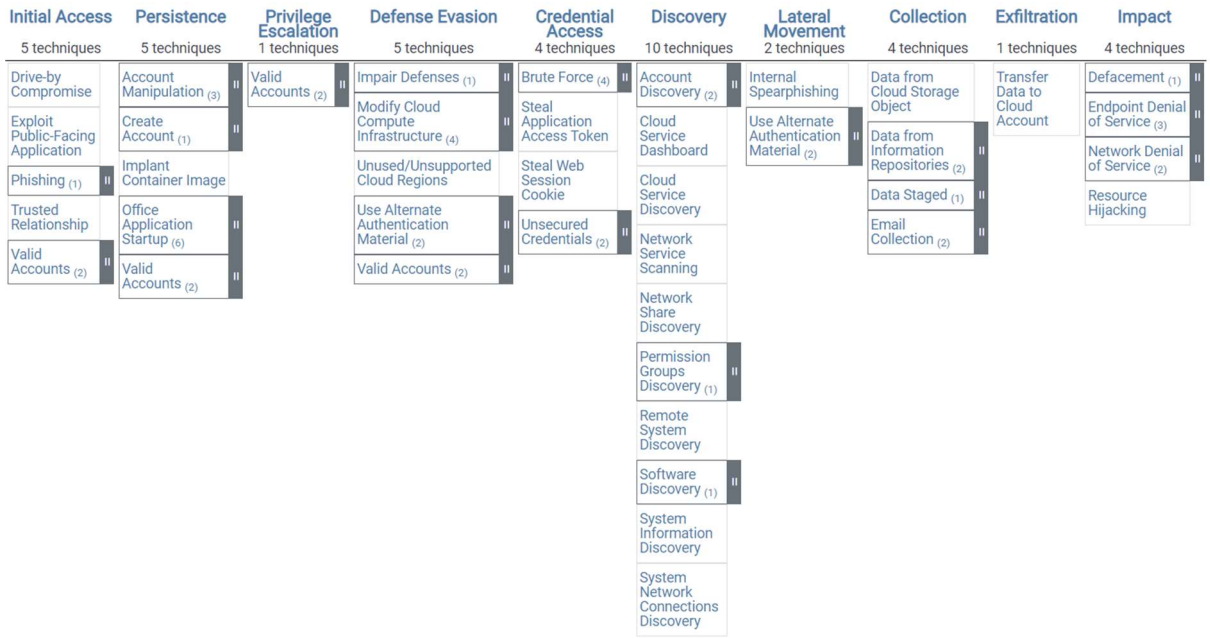

Figura 8. Matriz de MITRE ATT&CK para Cloud. Fuente: MITRE.

Las técnicas no son exclusivas de una determinada táctica, ya que una determinada técnica puede estar contenida en diferentes tácticas.

En la matriz para Cloud no existe la táctica de Ejecución, ni la de Comando y Control que se definen para la versión de la matriz para Enterprise.

6.6 MATRIZ ATT&CK DE CLOUD: AZURE

A continuación, se muestra las tácticas y técnicas que representan la matriz ATT&CK para Cloud

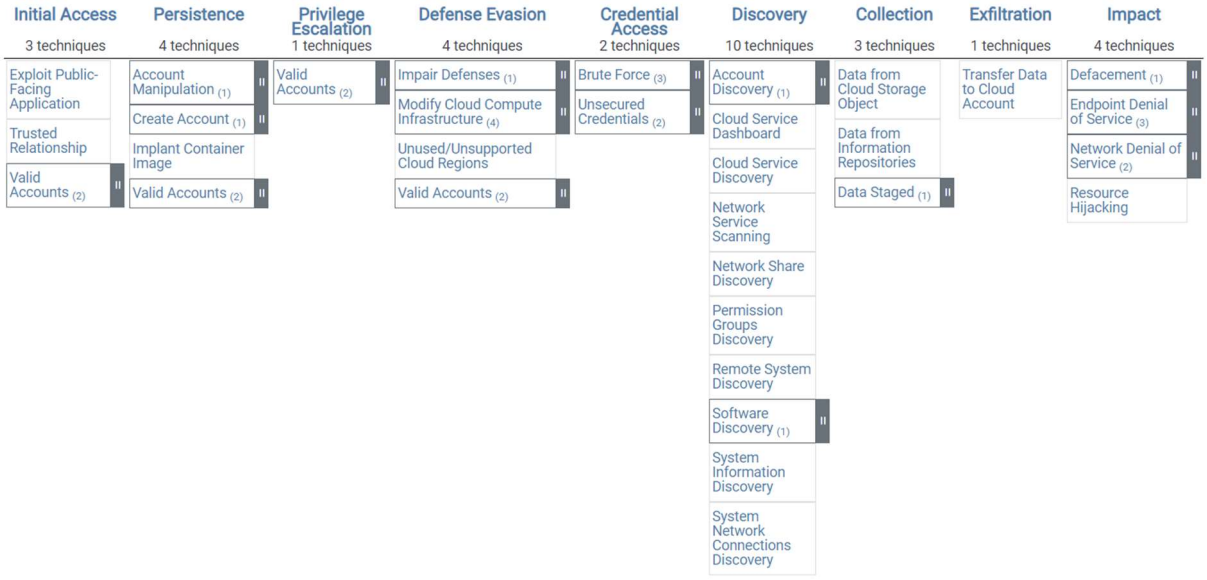

Figura 9. Matriz de MITRE ATT&CK para Cloud: Azure. Fuente: MITRE.

6.7 CONTROLES DE SEGURIDAD Y BUENAS PRACTICAS

6.7.1 Autenticación Multifactor

La autenticación multifactor (MFA) es un método de control de acceso en el que un usuario, para acceder a un sistema, debe presentar dos o más pruebas diferentes de que es quien dice ser.

Estas pruebas se denominan factores de autenticación. Los diferentes factores son normalmente:

1. Algo que el usuario conoce, como una contraseña o un pin
2. Algo que el usuario tiene, una notificación que recibe en el móvil o un código de seguridad.
3. Alguna característica biométrica del usuario, como su huella dactilar o el reconocimiento facial.

La autenticación multifactor es un control de seguridad, que añade una capa extra para la protección de las identidades.

Este tipo de autenticación mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Persistencia**	**Acceso a Credenciales**	**Recopilación**
TÉCNICA	*Account Manipulation*	*Brute Force*	*Data from Cloud Storage Object*
	Account Manipulation: Additional Azure Service Principal Credentials	*Brute Force: Password Guessing*	
	Create Account	*Brute Force: Password Spraying*	
	Create Account: Cloud Account	*Brute Force: Credential Stuffing*	

Tabla 3. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Autenticación Multifactor

En la táctica de **Persistencia** encontramos las siguientes técnicas para intentar mantener el acceso a sistemas:

- *Account Manipulation*: un atacante puede alterar cuentas, por ejemplo, modificar credenciales o los grupos de permiso de la cuenta comprometida.
  - *Additional Azure Service Principal Credentials*: es una subtecnica de *Account Manipulation*. "Una entidad de servicio de Azure es una identidad creada para su uso con aplicaciones, servicios hospedados y herramientas automatizadas que acceden a los recursos de Azure."[24]
  Las entidades de servicio soportan dos tipos de autenticación: autenticación basada en contraseña y autenticación basada en certificado.
  Un atacante puede añadir credenciales para entidades de servicio de Azure además de las credenciales legitimas existentes.

- *Create Account*: un atacante puede crear una cuenta local, en un dominio o en un inquilino en la nube (*cloud tenant*) para establecer unas credenciales de acceso complementarias.

  - *Cloud Account*: es una subtecnica de *Create Account*. Un atacante puede crear una cuenta de Cloud, que puede tener acceso limitado a determinados servicios de Cloud con el objetivo de reducir las posibilidades de detección.

Para mitigar estas técnicas ser recomienda usar autenticación multifactor para las cuentas de usuario y para las cuentas privilegiadas.

En la táctica de **Acceso a Credenciales** encontramos las siguientes técnicas para intentar robar credenciales:

- *Bruce Force*: un atacante puede servirse de técnicas de fuerza bruta cuando desconoce la contraseña de cuenta o conjunto de cuentas.
  - *Password Guessing*: un atacante puede adivinar la contraseña de una cuenta utilizando listas de contraseñas comunes.
  - *Password Spraying*: uso de listas de contraseñas comunes contra diferentes cuentas. Con esta técnica se evita bloqueos de las cuentas, lo que normalmente sucede cuando se usa fuerza bruta para una única cuenta intentando muchas contraseñas.
  - *Credential Stuffing*: un adversario puede usar credenciales de cuentas no relacionadas que se hayan comprometido en otras brechas, ya que podría aprovechar de que los usuarios tienen la tendencia de usar la misma contraseña en cuentas corporativas y personales.

Para mitigar estas técnicas ser recomienda usar autenticación multifactor, y si es posible también en servicios expuestos externamente.

En la táctica de **Recopilación** se encuentra la técnica *Data from Cloud Storage Object*, en la que un atacante puede acceder a objetos de datos en un almacén de datos en la nube si no se encuentra apropiadamente securizado.

Existen soluciones para almacenamiento de datos, dependiendo del proveedor se servicios en la nube, Amazon S3, Azure Storage, Google Cloud Storage, etc. Estos disponen de APIs para recuperar los datos.

"La plataforma de Azure Storage es la solución de almacenamiento en la nube de Microsoft. Los servicios principales de almacenamiento ofrecen un almacén de objetos escalable de forma masiva para objetos de datos, un almacenamiento en disco para máquinas virtuales (VM) de Azure, un servicio de sistema de archivos para la nube, un almacén de mensajes para mensajería confiable y un almacén NoSQL." [26]

Para mitigar la tecnica *Data from Cloud Storage Object* se recomienda usar autenticación multifactor para restringir el acceso a recursos y APIs de almacenamiento en la nube.

Según estudios de Microsoft una cuenta es más del 99.9% menos probable de ser comprometida si se usa autenticación multifactor (MFA).[61]

Microsoft dispone de *Azure Multi-Factor Authentication* (*Azure MFA*) (Figura 10), que permite configurar métodos de autenticación adicionales. Se necesita indicar el método que van a utilizar los usuarios para registrarse.

A continuation se indican los métodos de autenticación existentes:

- Notificación a través de aplicación móvil.
- Código de verificación de aplicación móvil o token de hardware.
- Mensaje de texto al teléfono.
- Llamada al teléfono.

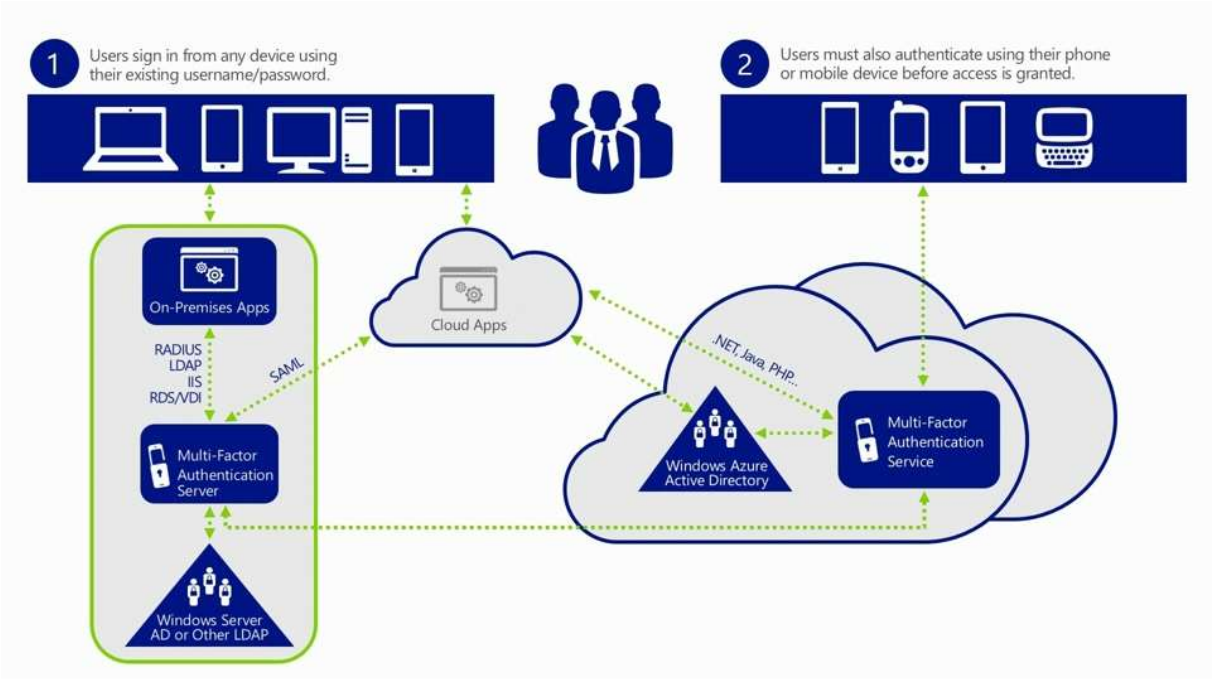

Figura 10. Grafico funcionamiento a alto nivel de Windows Azure Multi-Factor Authentication [60]

Microsoft recomienda, en su guía de buenas prácticas de seguridad para soluciones Azure, imponer autenticación multifactor para todos los usuarios (incluidos administradores).

Existen diferentes opciones para habilitar la verificación en dos pasos:

1. Habilitar autenticación multifactor para todos los usuarios y métodos de inicio de sesión con los valores predeterminados de seguridad de Azure AD.
2. Habilitar autenticación multifactor mediante cambio de estado del usuario. Esta opción exige que los usuarios realicen la verificación en dos pasos cada vez que inicien sesión, e invalida las directivas de acceso condicional.

3. Habilitar autenticación multifactor con la directiva de acceso condicional. La verificación en dos pasos únicamente se solicitará cuando se cumplen unas condiciones específicas, como, por ejemplo, sesión desde distintas localizaciones, dispositivos en los que no se confía, o aplicaciones de riego.
4. Habilitar autenticación multifactor con directivas de acceso condicional mediante la evaluación de directivas de acceso condicional basadas en riesgos.
   Esta opción utiliza la evaluación de riesgos de Azure AD Identity Protection para establecer la verificación en dos pasos dependiendo de los riesgos del usuario y el inicio de sesión para todas las aplicaciones en la nube.

6.7.2 Protección contra Exploits

Existen soluciones que permiten detectar y bloquear situaciones en la que un atacante pudiera estar intentando una explotación de software.

Este tipo de protección mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Acceso Inicial**
TÉCNICA	*Exploit Public-Facing Application*

Tabla 4. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Protección contra Exploits

En la táctica de **Acceso Inicial** encontramos la siguiente técnica para intentar acceder a la red.

- *Exploit Public-Facing Application*: un adversario puede intentar beneficiarse de vulnerabilidades en un ordenador o una aplicación accesibles desde internet usando software, datos o comandos. Sitios web son un ejemplo común de estas aplicaciones, sin embargo, también encontramos servidores web, bases de datos y servicios estándar (como SSH) accesibles desde Internet.

En entornos Cloud, un atacante mediante la explotación de una aplicación podría comprometer la instancia de base, pudiendo acceder a las APIs, o aprovecharse de políticas inseguras de administración de identidades y acceso.

OWASP Top 10 y CWE Top 25 describen las vulnerabilidades web más comunes.

Un **Firewall de Aplicaciones Web (*WAF*)** protege a las aplicaciones contra explotaciones y vulnerabilidades comunes, como por ejemplo ataques de inyección SQL o cross site scripting (XSS).

En la siguiente figura se muestra diagrama de WAF de Azure.

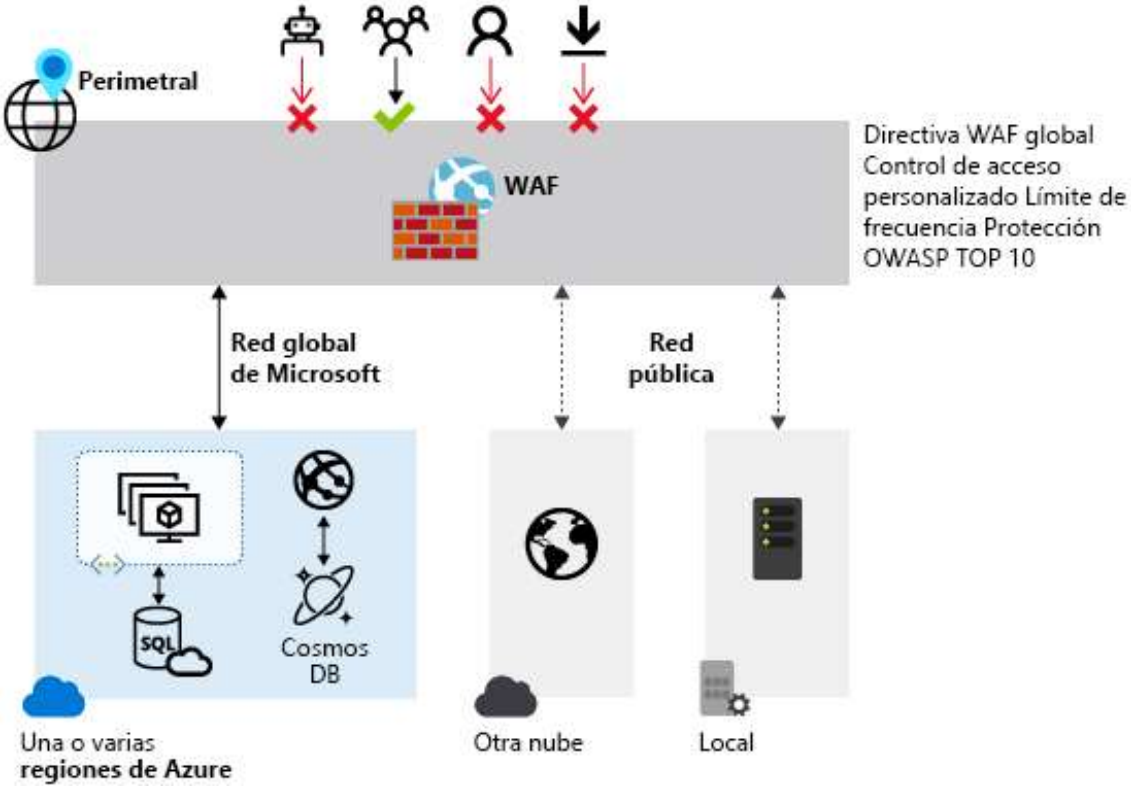

Figura 11. WAF de Azure [32]

Abordar vulnerabilidades en el código o a nivel de diseño de una aplicación puede resultar complejo, ya que puede requerir mantenimiento, actualización y monitorización de muchas capas en la aplicación.

Un firewall de aplicaciones web puede ser una solución centralizada, ya que se puede responder más rápido ante una vulnerabilidad conocida aplicando parches específicos sin tener que abordar esa vulnerabilidad en cada una de las aplicaciones web que pudieran verse afectadas.

El firewall de aplicaciones web se puede implementar con *Azure Application Gateway*, *Azure Front Door* y el servicio *Azure Content Delivery Network (CDN)* de Microsoft. WAF en Azure CDN se encuentra actualmente en versión preliminar pública (en el momento de la escritura de este documento).

WAF con *Application Gateway* esta basado en Core Rule Set (CRS) 3.1, 3.0, or 2.2.9 de OWASP (*Open Web Application Security Project*).

El WAF protege contra las siguientes vulnerabilidades web:

- Ataques de inyección SQL.
- Ataques *Cross-site scripting* (XSS).
- Otros ataques comunes, como la inyección de comandos, el contrabando de solicitudes HTTP (*HTTP request smuggling*), la división de respuestas HTTP (*HTTP response splitting*) y la inclusión de archivos remotos (*remote file inclusion*).
- Infracciones del protocolo HTTP.
- Anomalías del protocolo HTTP, como la falta de agentes de usuario de host (*user-agent*) y encabezados (*headers*) de aceptación.
- Bots, rastreadores (*crawlers*) y escáneres.
- Errores de configuración comunes de las aplicaciones, como Apache y IIS.

6.7.3 Administración de Cuentas con Privilegios

La administración de cuentas con privilegios se encarga de la creación, modificación y uso de cuentas privilegiadas (incluidas Administrador, SYSTEM y root, en función del sistema operativo). También se encarga de la gestión de los permisos asociados a dichas cuentas.

Una administración segura de cuentas con privilegios mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	Acceso Inicial	Persistencia	Escalada de Privilegios	Evasión de Defensa	Acceso a Credenciales
TÉCNICA	*Exploit Public-Facing Application*	*Account Manipulation*	*Valid Accounts*	*Valid Accounts*	*Unsecured Credentials*
	Valid Accounts	*Account Manipulation: Additional Azure Service Principal Credentials*	*Valid Accounts: Cloud Accounts*	*Valid Accounts: Cloud Accounts*	
	Valid Accounts: Cloud Accounts	*Create Account*			
		Create Account: Cloud Account			
		Implant Container Image			
		Valid Accounts			
		Valid Accounts: Cloud Accounts			

Tabla 5. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Administración de Cuentas con Privilegios

En la táctica **Acceso Inicial**, con la técnica *Exploit Public-Facing Application*, anteriormente explicada, un adversario intentar beneficiarse de vulnerabilidades en un ordenador o una aplicación accesibles desde internet para intentar acceder a la red.

Para mitigar esta técnica se recomienda que las cuentas de servicio (*service accounts*) usen el mínimo privilegio posible, ya que esto limitara los permisos que el proceso comprometido tenga en el resto del sistema.

Con la técnica *Valid Accounts*, un adversario puede conseguir cuentas existentes y servirse de ellas para obtener acceso inicial, persistencia, realizar escalada de privilegios y/o evadir medidas de defensa.

Las cuentas objetivo de un atacante son cuentas privilegiadas de dominio que tengan privilegios como administrador en muchos equipos y en Active Directory, y que pueden ser utilizadas para propagar el ataque y para manipular otras cuentas o los datos a los que estas pueden acceder. Las cuentas de dominio VIP ("*Very Important Person*"), es decir, ejecutivos, y otras personas (como personal de Soporte técnico) también son valiosas, ya que tienen acceso a la información que el atacante tiene como objetivo, o bien cuentas que pueden ser usadas para conceder acceso a esa información.

Dentro de la tecnica *Valid Account* se encuentra la subtecnica *Cloud Accounts*, en la que una atacante compromete cuentas en la nube. Las cuentas en la nube pueden tener diferente finalidad: pueden ser usadas por usuarios, para soporte remoto, servicios o administración de recursos dentro del proveedor de servicios en la nube. Un atacante puede valerse de estas cuentas para obtener acceso inicial, persistencia, realizar escalada de privilegios y/o evadir medidas de defensa, de manera similar que con cuentas de dominio (gestionadas por *Active Directory Domain Services*, *AD DS*).

Se recomienda auditar cuentas (locales, dominio y Cloud) y sus permisos.
Situaciones en las que cuentas por defecto han sido habilitadas, o cuentas locales han sido creadas sin autorización, deberían ser incluidas en la auditoria. Es importante limitar el uso de cuentas privilegiadas.

En la táctica de **Persistencia** encontramos las siguientes técnicas con el objetivo de mantener el acceso a sistemas:

- *Account Manipulation*: un atacante puede alterar cuentas.
    - *Additional Azure Service Principal Credentials*: es una subtecnica de *Account Manipulation* que consiste en añadir credenciales para entidades de servicio de Azure.

- *Create Account:* un atacante puede crear una cuenta local, en un dominio o en un inquilino en la nube (*cloud tenant*) para establecer unas credenciales de acceso complementarias.
    - *Cloud Account:* es una subtecnica de *Create Account*. Un atacante puede crear una cuenta de Cloud.
- *Implant Container Image:* esta técnica se basa en implantar una imagen de contenedor, como ejemplo una imagen Docker, con código malicioso para mantener el acceso.

Para mitigar las técnicas de creación y manipulación de cuentas, se recomienda no usar cuentas de administrador de dominio en operaciones cotidianas.
Relativo a imágenes de contenedor, la recomendación es limitar al máximo posible los permisos relacionados con la creación de imágenes o contenedores.

La técnica *Unsecured Credentials*, asociada a la táctica **Acceso a Credenciales**, consiste en buscar en los sistemas y conseguir credenciales que se encuentran almacenadas de una forma insegura. Estas credenciales pueden estar en múltiples ubicaciones, por ejemplo, en ficheros de texto plano (ej. histórico de comandos Bash), repositorios del sistema operativo o de aplicaciones (ej, credenciales en el registro de Windows), o en otros ficheros, tales como ficheros de certificados claves privadas.

Si un software necesita almacenar credenciales en el registro se debería asegurar que las cuentas asociadas tienen los mínimos permisos.

Uno de los principios fundamentales en seguridad es el principio de privilegio mínimo. Este principio especifica que a un usuario, sistema o aplicación se le debe conceder la mínima cantidad de permisos absolutamente necesarios para realizar su función.

Adicionalmente, es importante minimizar el número de cuentas con privilegios, cuentas que administran los sistemas informáticos, dado que son las cuentas que buscan los atacantes, puesto que les facilitan el acceso a datos y a los sistemas. También se reduce el riesgo de que un usuario autorizado, por error, dañe datos confidenciales o sistemas.

Es recomendable identificar y monitorizar las cuentas privilegiadas.

Es fundamental revisar periódicamente si alguna cuenta ya no necesita estar en roles privilegiados. Además de desaprovisionar (borrar o desactivar) cuentas de administrador cuando empleados abandonen la organización.

Las cuentas privilegiadas no deberían usarse para ninguna actividad fuera de su finalidad, como por ejemplo para leer emails o navegar por Internet, para evitar ataques como el *phishing.*

Es importante la concienciación de los usuarios en el uso apropiado de estas cuentas.

En Azure, se pueden controlar y monitorizar las cuentas privilegiadas *con Azure AD Privileged Identity Management* activado, para recibir emails notificando cambios en el rol de acceso con privilegios. También se puede habilitar *Azure AD Identity Protection*, como mínimo, en cuentas como administradores globales, y de usuarios que gestionen información sensible a nivel corporativo.

Se puede implementar el acceso "*Just-In-Time (JIT)*" para disminuir el tiempo de exposición de privilegios. *Azure AD Privileged Identity Management* permite limitar a los usuarios a aceptar solo sus privilegios JIT, y también, asignar roles de una duración determinada.

Se recomienda que todas las cuentas de administrador críticas no tengan contraseña (opción preferida) o requieran el uso de autenticación multifactor. Se puede utilizar la app *Microsoft Authenticator* para iniciar sesión en cualquier cuenta de Azure AD sin utilizar una contraseña.

6.7.4 Administración de Cuentas de Usuarios

La administración de cuentas de usuarios: creación, modificación y uso. También se encarga de la gestión de los permisos asociados a dichas cuentas.

Una administración segura de cuentas de usuarios mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	Evasión de Defensa	Acceso a Credenciales	Descubrimiento	Recopilación	Exfiltración
TÉCNICA	*Impair Defenses*	*Brute Force*	*Cloud Service Dashboard*	*Data from Cloud Storage Object*	*Transfer Data to Cloud Account*
	Impair Defenses: Disable or Modify Cloud Firewall	*Brute Force: Credential Stuffing*		*Data from Information Repositories*	
	Modify Cloud Compute Infrastructure				
	Modify Cloud Compute Infrastructure: Create Snapshot				
	Modify Cloud Compute Infrastructure: Create Cloud Instance				
	Modify Cloud Compute Infrastructure: Delete Cloud Instance				

Tabla 6. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Administración de Cuentas de Usuarios

En la táctica de **Evasión de Medidas de Defensa** encontramos las siguientes técnicas con el objetivo de que el atacante no sea detectado:

- *Impair Defenses*: esta técnica consiste en alterar componentes en los sistemas para dificultar o desactivar mecanismos de defensa, como firewalls o antivirus. También se incluiría la manipulación o eliminación de elementos para auditar actividad maliciosa.
    - *Disable or Modify Cloud Firewall*: un atacante puede desactivar o modificar un firewall dentro de un entorno Cloud, como ejemplo añadir nuevas reglas, para eludir controles que limitan el acceso a recursos en la nube.

- *Modify Cloud Compute Infrastructure:* un adversario puede intentar modificar una infraestructura de servicio informático de una cuenta en la nube, como, por ejemplo, crear, modificar o eliminar instancias, máquinas virtuales o instantáneas. Esto le podría servir a un atacante para eludir medidas de defensa y eliminar evidencias de su presencia.
    - *Create Snapshot:* esta subtécnica consiste en crear una instantánea (*snapshot*) o respaldo de datos dentro de una cuenta en la nube para evadir restricciones que impidan el acceso a una infraestructura de servicio existente. Una instantánea es una copia en un momento especifico de un componente existente en la nube como una máquina virtual, un disco duro virtual o un volumen. las instancias que residen dentro de una cuenta.
    - *Create Cloud Instance:* un atacante puede crear una nueva instancia o máquina virtual dentro del servicio de computación de una cuenta de Cloud, permitiéndole evadir reglas del firewall y permisos que existen en las instancias que residen dentro de una cuenta.
    - *Delete Cloud Instance:* un atacante puede borrar una instancia de Cloud después de realizar actividades maliciosas con el objetivo de evitar su detección y eliminar evidencias.

En la táctica de **Acceso a Credenciales** encontramos las siguientes técnicas para intentar robar credenciales:

- *Bruce Force*: un atacante puede servirse de técnicas de fuerza bruta cuando desconoce la contraseña de cuenta o conjunto de cuentas.

- *Credential Stuffing*: un adversario puede usar credenciales de cuentas no relacionadas que se hayan comprometido en otras brechas, ya que podría aprovechar de que los usuarios tienen la tendencia de usar la misma contraseña en cuentas corporativas y personales.

Con la técnica *Cloud Service Dashboard*, asociada a la táctica **Descubrimiento**, un atacante puede usar un panel (*dashboard*) en la interfaz gráfica de usuario de un servicio Cloud para obtener información útil sobre el entorno (servicios, recursos y características).

En la táctica de **Recopilación** encontramos las siguientes técnicas para intentar recopilar información de interés.

- *Data from Cloud Storage Object*: un atacante puede acceder a objetos de datos en un almacén de datos en la nube si no se encuentra apropiadamente securizado.
- *Data from Information Repositories*: Un atacante puede extraer información valiosa de repositorios de información, o repositorios de almacenamiento ubicados en una infraestructura Cloud. Repositorios de información son herramientas que almacenan información, normalmente compartida entre usuarios, y que facilita la colaboración, como Sharepoint o bases de datos como SQL Server. Algunos ejemplos de información almacenada en estos repositorios son: diagramas de red y/o arquitectura, documentación técnica de sistemas, procedimientos, directivas de seguridad, planificación de proyectos, credenciales de entornos de desarrollo o pruebas, código fuente, etc.

Con la técnica *Transfer Data to Cloud Account*, asociada a la táctica **Exfiltración**, un atacante puede exfiltrar datos (incluyendo copias de respaldo de entornos Cloud, como instancias) a otras cuentas de Cloud en el mismo proveedor Cloud para evitar la detección por exfiltración por la típica transferencia o descarga de ficheros en la red, via canales de comando y control. Estas transferencias de datos pueden hacerse utilizando APIs del proveedor de Cloud y direcciones internas del proveedor para mezclarse con trafico normal o evitar transferencias sobre interfaces de red externos.

A continuación, se indican buenas prácticas para la Administración de Cuentas de Usuarios:

- Se recomienda verificar que los permisos de usuarios son los adecuados para evitar que un atacante pueda desactivar controles de seguridad, de registro y auditoria.

.

- Limitar permisos para la creación de instantáneas y copias de respaldo, crear y eliminar instancias en Cloud.

- Limitar las cuentas de usuario y las directivas de seguridad de la Administración de Identidad y Acceso (*Identity and Access Management*, *IAM*) aplicando el principio del privilegio mínimo.
- Limitar el número de usuarios con un rol de Administración de Identidad y Acceso que tenga privilegios administrativos.
- Esforzarse por reducir asignaciones permanentes a roles privilegiados. Se recomienda considerar el uso de credenciales temporales para cuentas que son únicamente validas por un periodo de tiempo determinado.
- Revisar periódicamente directivas de seguridad, roles y usuarios en la Administración de Identidad y Acceso.
- Restablecer inmediatamente las cuentas de las que se conoce que han sido afectadas por una brecha de credenciales, o después de detectar ataques de fuerza bruta.
- Verificar que se aplica el principio de privilegio mínimo para que solo se puedan visualizar los recursos estrictamente necesarios en paneles del interfaz grafico de usuario de un servicio Cloud.
- Se recomienda configurar grupos de permisos de usuario y roles para el acceso a almacenamiento Cloud.
- Se recomienda implementar mecanismos de control de acceso tanto para autenticación como para autorización en repositorios de información.

6.7.5 Directivas de Seguridad del Uso de Cuentas

Configurar características relacionada con el uso de cuentas como bloqueos de intentos de acceso, específicos tiempos de acceso, etc.

Unas buenas directivas de seguridad del uso de cuentas mitigan el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Acceso a Credenciales**
TECNICA	*Brute Force*
	Brute Force: Password Guessing
	Brute Force: Password Spraying
	Brute Force: Credential Stuffing

Tabla 7. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Directivas de Seguridad del Uso de Cuentas

En la táctica de **Acceso a Credenciales** encontramos las siguientes técnicas para intentar robar credenciales:

- *Bruce Force*: un atacante puede servirse de técnicas de fuerza bruta cuando desconoce la contraseña de cuenta o conjunto de cuentas.
    - *Password Guessing*: un atacante puede adivinar la contraseña de una cuenta utilizando listas de contraseñas comunes.
    - *Password Spraying*: uso de listas de contraseñas comunes contra diferentes cuentas. Con esta técnica se evita bloqueos de las cuentas, lo que normalmente sucede cuando se usa fuerza bruta para una única cuenta intentando muchas contraseñas.
    - *Credential Stuffing*: un adversario puede usar credenciales de cuentas no relacionadas que se hayan comprometido en otras brechas, ya que podría aprovechar de que los usuarios tienen la tendencia de usar la misma contraseña en cuentas corporativas y personales.

Como buena practica de Directivas de Seguridad del Uso de Cuentas se recomienda bloquear una cuenta después de un cierto número de intentos fallidos de acceso. Se debería valorar no aplicar una política demasiado restrictiva ya que podría producir una denegación de servicio.

6.7.6 Directivas de Seguridad de Contraseñas

Directivas de seguridad para contraseñas seguras de cuentas.

Unas buenas directivas de seguridad referentes a contraseñas seguras para las cuentas mitigan el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Acceso Inicial / Persistencia / Escalada de Privilegios / Evasión de Defensa**	**Acceso a Credenciales**	**Exfiltración**
TÉCNICA	*Valid Accounts*	*Brute Force*	*Transfer Data to Cloud Account*
	Valid Accounts: Default Accounts	*Brute Force: Password Guessing*	
	Valid Accounts: Cloud Accounts	*Brute Force: Password Spraying*	
		Brute Force: Credential Stuffing	
		Unsecured Credentials	
		Unsecured Credentials: Credentials In Files	

Tabla 8. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Directivas de Seguridad de Contraseñas

En las tácticas de **Acceso Inicial**, **Persistencia**, **Escalada de Privilegios** y **Evasión de Defensa** se encuentra la técnica:

- *Valid Accounts*: un adversario puede conseguir cuentas existentes y servirse de ellas para obtener acceso inicial, persistencia, realizar escalada de privilegios y/o evadir medidas de defensa.
    - *Default Accounts*: con esta subtecnica un atacante compromete cuentas preestablecidas que incorporan sistemas, herramientas o dispositivos. Estas cuentas por defecto suponen una importante amenaza debido a que son un objetivo fácil para atacantes.
    - *Cloud Accounts*: con esta subtecnica un atacante compromete cuentas en la nube.

En la táctica de **Acceso a Credenciales** encontramos las siguientes técnicas para intentar robar credenciales:

- *Bruce Force:* un atacante puede servirse de técnicas de fuerza bruta cuando desconoce la contraseña de cuenta o conjunto de cuentas.
    - *Password Guessing*: un atacante puede adivinar la contraseña de una cuenta utilizando listas de contraseñas comunes.
    - *Password Spraying*: uso de listas de contraseñas comunes contra diferentes cuentas. Con esta técnica se evita bloqueos de las cuentas, lo que normalmente sucede cuando se usa fuerza bruta para una única cuenta intentando muchas contraseñas.
    - *Credential Stuffing*: un adversario puede usar credenciales de cuentas no relacionadas que se hayan comprometido en otras brechas, ya que podría aprovechar de que los usuarios tienen la tendencia de usar la misma contraseña en cuentas corporativas y personales.

- *Unsecured Credentials:* un atacante puede buscar y obtener credenciales que se encuentran almacenadas de una forma insegura en los sistemas comprometidos. Estas credenciales pueden estar en múltiples ubicaciones, por ejemplo, en ficheros de texto plano (ej. histórico de comandos Bash), repositorios del sistema operativo o de aplicaciones (ej, credenciales en el registro de Windows), o en otros ficheros, tales como ficheros de certificados claves privadas.
    - *Credentials In Files*: esta subtecnica consiste en localizar credenciales almacenadas en ficheros, que han podido ser creados por usuarios para

almacenar sus propias credenciales, o compartirlas con otros usuarios. Credenciales pueden estar contenidas dentro de código fuente o binarios, en ficheros de configuración de sistemas o servicios, etc.

En Cloud, es habitual que credenciales de usuarios autenticados estén almacenadas en ficheros locales de configuración o ficheros de credenciales.

Con la técnica *Transfer Data to Cloud Account*, asociada a la táctica **Exfiltración**, un atacante puede exfiltrar datos (incluyendo copias de respaldo de entornos Cloud, como instancias) a otras cuentas de Cloud en el mismo proveedor Cloud para evitar que sea detectado.

A continuación, se indican buenas prácticas para las Directivas de Seguridad de Contraseñas:

- Se recomienda cambiar de inmediato el usuario y la contraseña por defecto de las aplicaciones y dispositivos que utilicen cuentas preestablecidas.
- En entornos Cloud, se recomienda que las cuentas tengan contraseñas complejas y únicas en todos los sistemas de la red.
- Se recomienda consultar directivas de NIST (*NIST Special Publication 800-63B Digital Identity Guidelines [39]*) cuando se creen directivas de seguridad de contraseñas.
- Se recomienda usar contraseñas robustas para claves privadas.
- No almacenar credenciales en ficheros ni en el registro.
- Se recomienda tener en cuenta la rotación periódica de claves de acceso para reducir la posibilidad del uso de credenciales robadas.

6.7.7 Control de Cuentas de Usuario

Una adecuada configuración del Control de Cuentas de Usuario de Windows (*User Account Control, UAC*) disminuye el riesgo de que un atacante consiga acceso a un proceso con permisos elevados.

Esto mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Acceso Inicial**
TÉCNICA	*Trusted Relationship*

Tabla 9. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con el Control de Cuentas de Usuario

En la táctica de **Acceso Inicial** encontramos la siguiente técnica *Trusted Relationship* para intentar acceder a la red:

- *Trusted Relationship*: un atacante puede valerse de terceros que tienen acceso al entorno de la víctima, y en los que esta tiene una relación de confianza. Algunos ejemplos pueden ser proveedores externos, como proveedores de servicios de IT, de seguridad o de infraestructura. Estos pueden tener accesos elevados para el mantenimiento de sistemas o entornos Cloud.

Como buena práctica, se recomienda gestionar adecuadamente las cuentas y los permisos de grupos de terceros en los que existe una relación de confianza para minimizar un mal uso por parte de estos grupos o si un atacante compromete cuentas existentes de estos.

6.7.8 Filtrado de Tráfico de Red

Uso de dispositivos de red para filtrar el tráfico de salida o entrada y realizar filtrados basados en el protocolo.

Un filtrado adecuado del tráfico de red mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Acceso a Credenciales**	**Recopilación**	**Exfiltración**	**Impacto**
TÉCNICA	*Unsecured Credentials*	*Data from Cloud Storage Object*	*Transfer Data to Cloud Account*	*Endpoint Denial of Service*
	Unsecured Credentials: Cloud Instance Metadata API			*Endpoint Denial of Service: Service Exhaustion Flood*
				Endpoint Denial of Service: Application Exhaustion Flood
				Endpoint Denial of Service: Application or System Exploitation

				Network Denial of Service
				Network Denial of Service: Direct Network Flood
				Network Denial of Service: Reflection Amplification

Tabla 10. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con el Filtrado de Trafico de Red.

En la táctica de **Acceso a Credenciales** encontramos las siguientes técnicas con el objetivo de robar credenciales:

- Unsecured Credentials: un atacante busca en los sistemas para conseguir credenciales que se encuentran almacenadas de una forma insegura.
  - *Cloud Instance Metadata API:* Un atacante puede intentar obtener credenciales y otros datos sensibles a través de la API de Metadatos de Instancias en la nube, soportado por la mayoría de los proveedores de servicios en la nube. Esta API es un servicio en las instancias virtuales en ejecución que posibilita tener acceso a información sobre la instancia virtual. Teniendo acceso a esta, también podría explotar la vulnerabilidad Falsificación de Petición del Lado del Servidor *(Server-Side Request Forgery, SSRF*) en un proxy web expuesto públicamente para obtener información sensible a través de una petición a la API de Metadados de Instancia.
    Azure tiene el *Azure Instance Metadata Service* (*IMDS*) que es un punto de conexión REST que está disponible en una dirección IP no enrutable conocida (169.254.169.254) y que únicamente se puede acceder desde dentro de la máquina virtual.

En la táctica de **Recopilación** se encuentra la técnica *Data from Cloud Storage Object*, en la que un atacante puede acceder a objetos de datos en un almacén de datos en la nube si no se encuentra apropiadamente securizado.

En la táctica **Exfiltración** se encuentra la técnica *Transfer Data to Cloud Account*, por la cual un atacante puede exfiltrar datos a otras cuentas de Cloud en el mismo proveedor Cloud.

En la táctica de **Impacto** encontramos las siguientes técnicas con el objetivo de manipular, interrumpir o destruir sistemas y datos:

- *Endpoint Denial of Service*: un atacante puede realizar ataques de Denegación de Servicio (*Denial of Service, DoS*) con el objetivo de degradar o interrumpir la

disponibilidad de los servicios (sitios y aplicaciones web, servicios de correo, DNS, etc.) a los usuarios. Estos ataques son realizados agotando los recursos del sistema donde se encuentran alojado estos servicios, o dañando permanentemente el sistema, el servicio o algún componente de este.
Si ataque DoS es realizado por más de una persona o maquina entonces se denomina ataque de Denegación de Servicio Distribuido (*Distributed Denial of Service, DDoS*). La forma más habitual de llevar a cabo este ataque es usando una red de bots (*botnets*), que son maquinas remotas que se encuentran bajo el control del atacante.

- *Service Exhaustation Flood*: Un atacante puede realizar un ataque DoS contra DNS y servicios web. Aunque ataques contra servicios web pueden realizarse de múltiples formas, cabe destacar el ataque en el que el atacante envía un gran número de peticiones HTTP a un servidor web para sobrecargarlo y agotar sus recursos, ataque conocido como inundación HTTP. También existe el llamado ataque de renegociación SSL, en el que un atacante establece una conexión SSL/TLS para realizar un conjunto de peticiones de renegociación del algoritmo criptográfico, lo que tiene un coste computacional, pudiendo impactar en la disponibilidad del servicio.
- *Application Exhaustation Flood*: Un adversario puede atacar repetidamente funcionalidades, que consumen importantes recursos, de aplicaciones web para provocar una denegación de servicio.
- *Application or System Exploitation*: Un adversario puede explotar vulnerabilidades de software para producir una denegación de servicio.

- *Network Denial of Service*: Un adversario puede llevar a cabo una Denegacion de Servicio (DoS) de red, agotando el ancho de banda de la red mediante un gran volumen de tráfico malicioso direccionado hacia un recurso o hacia las conexiones de red y los dispositivos de red de la cual el recurso depende.
  - *Direct Network Flood*: un adversario puede producir una denegación de servicio (DoS) enviando directamente un volumen muy grande de trafico de red hacia la red del servicio atacado. Para producir el desbordamiento son usados normalmente red de bots usando los protocolos de red UDP o ICMP, aunque TCP también puede ser usado.
  - *Reflection Amplification*: Un atacante puede tartar de producir una denegación de servicio reflejando y amplificando un gran volumen de tráfico de red hacia un objetivo, utilizando un servidor intermedio denominado comúnmente "reflector". Destaca el uso de los protocolos DNS y NTP, aunque también se han documentado casos con el protocolo memcache.

A continuación, se indican algunas buenas prácticas:

- Limitar el acceso a la API de Metadatos de Instancia usando un firewall basado en host. Para evitar ataques de Falsificación de Petición del Lado del Servidor (*Server-Side Request Forgery, SSRF*) que permitan acceder a esta API se puede usar un Firewall de Aplicaciones Web (WAF) adecuadamente configurado.
- Los proveedores de servicios en la nube soportan, cuando se accede a recursos en la nube, restricciones basadas en IP. Por lo tanto, se recomienda tener en cuenta listas de IPs permitidas en combinación con la administración de cuentas de usuario para asegurarse que el acceso a datos esta restringido no solo a los usuarios validos sino también a unos rangos de IPs esperadas.
- Establecer restricciones basadas en red para no permitir transferencia de datos a nubes privadas virtuales (*Virtual Private Cloud, VPC*) en las que no se confía.
- Se recomienda aprovecharse de servicios provistos con *Content Delivery Networks* (*CDN*) o proveedores especializados en mitigaciones de Denegación de Servicio (DoS). Filtrar tráfico limítrofe bloqueando las direcciones del origen del ataque, los puertos o bloqueando los protocolos usados. Para defenderse contra inundaciones SYS, activar SYN Cookies.
- Para mitigar ataques de Denegación de Servicio de Red es habitualmente necesario interceptar el tráfico entrante para filtrar el tráfico malicioso del legítimo. Esto puede hacerse a través del Proveedor de Servicios de Internet, un *Content Delivery Network* (*CDN*) o proveedores especializados en mitigaciones DoS. En algunos casos se puede realizar un filtrado local bloqueando las direcciones del origen del ataque, los puertos o bloqueando los protocolos usados. Como respuesta inmediata se puede necesitar un análisis de riesgos asociados a recursos críticos afectados y crear un plan de recuperación de desastres o plan de continuidad del negocio parar responder a los incidentes.
- Se recomienda habilitar mitigaciones contra ataques de denegación de servicio distribuido (DDoS) para todas las aplicaciones y servicios que son críticas para el negocio. Así mismo se aconseja diseñar las aplicaciones para que escalen horizontalmente y puedan satisfacer la demanda de un aumento de carga. Si la aplicación depende de una solo instancia de un servicio, esto produce un único punto de fallo, por lo que se recomienda aprovisionar múltiples instancias para hacer el sistema más resistente y escalable.

En Azure, un control de seguridad contra ataques por denegación de servicio distribuido (DDoS) es *Azure DDoS Protection*, que proporciona dos niveles de servicio:

- *Básico*: integrado y habilitado automáticamente como parte de la plataforma Azure, que monitoriza constantemente el tráfico reduciendo en tiempo real los

ataques a nivel de red más comunes. Las directivas de mitigación están optimizadas para el volumen de región de tráfico de Azure.

- *Estándar*: proporciona capacidades avanzadas de mitigación DDoS, que se adaptan particularmente a los recursos de *Azure Virtual Network*. Las directivas de mitigación están optimizadas para el volumen de tráfico de la aplicación. Proporciona notificación, métricas de ataques y registros de recursos en tiempo real a través de *Azure Monitor*.

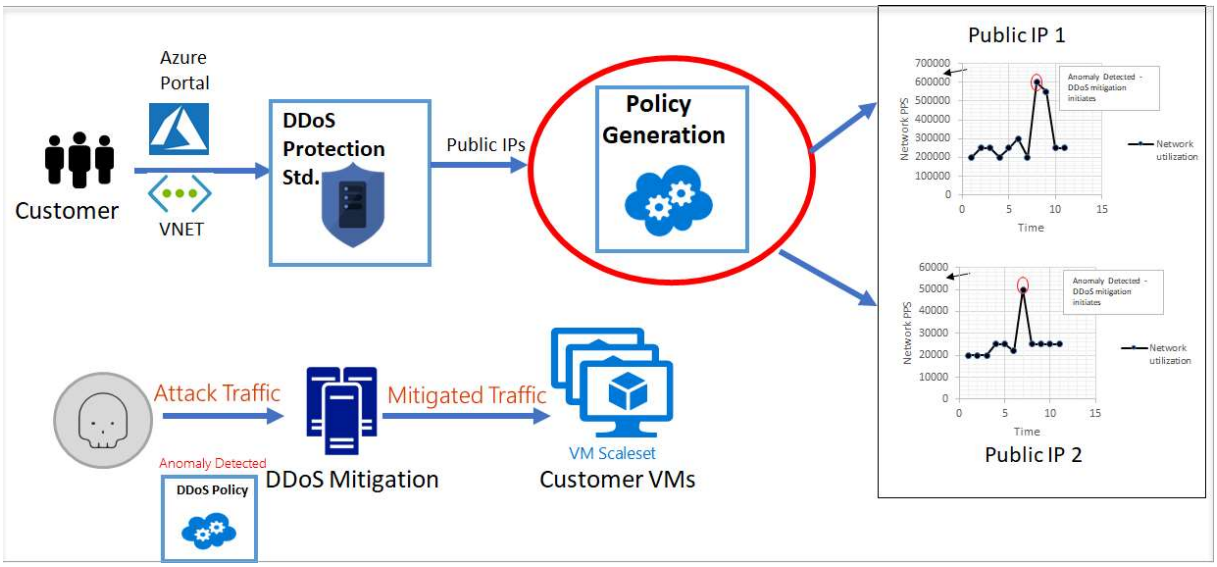

Figura 12. Azure DDoS Protection Standard [45]

6.7.9 Segmentación de Red

Hace referencia a la segmentación física y lógica de la red, con el fin de aislar sistemas, funciones o recursos críticos, y/o que contengan información sensible.

Una adecuada segmentación de la red mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	Acceso Inicial	Persistencia	Descubrimiento
TÉCNICA	*Exploit Public-Facing Application*	*Account Manipulation*	*Network Service Scanning*
	Trusted Relationship	*Account Manipulation: Additional Azure Service Principal Credentials*	
		Create Account	
		Create Account: Cloud Account	

Tabla 11. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con el Segmentación de Red.

En la táctica de **Acceso Inicial** encontramos las siguientes técnicas para intentar acceder a la red:

- *Exploit Public-Facing Application*: un adversario puede intentar beneficiarse de vulnerabilidades en un ordenador o una aplicación accesibles desde internet usando software, datos o comandos.
- *Trusted Relationship*: un atacante puede valerse de terceros que tienen acceso al entorno de la víctima, y en los que esta tiene una relación de confianza.

En la táctica de **Persistencia** encontramos las siguientes técnicas con el objetivo de mantener el acceso a sistemas:

- *Account Manipulation*: un atacante puede alterar cuentas.
  - *Additional Azure Service Principal Credentials*: consiste en añadir credenciales para entidades de servicio de Azure.
- *Create Account*: un atacante puede crear una cuenta local, en un dominio o en un inquilino en la nube (*cloud tenant*) para establecer unas credenciales de acceso complementarias.
  - *Cloud Account*: es una subtecnica de *Create Account*. Un atacante puede crear una cuenta de Cloud.

En la táctica *Descubrimiento*, con la técnica *Network Service Scanning*, un atacante intenta averiguar los servicios que se están ejecutando en servidores remotos. Para ello puede valerse de herramientas para el escaneo de puertos y vulnerabilidades. En entornos Cloud,

un atacante puede intentar obtener servicios ejecutándose en otros servidores Cloud, y si este está conectado a entornos locales también podría descubrir servicios ejecutándose en esos sistemas.

A continuación, se explica que es la segmentación de red y algunas buenas prácticas de esta estrategia para mitigar las técnicas comentadas anteriormente.

La segmentación de red es una estrategia que implica dividir una red en pequeñas redes o segmentos separados por cortafuegos (firewalls). Su finalidad no es solo mejorar el rendimiento de la red, sino aumentar la seguridad de esta, mediante el control del tráfico. Se puede detener todo el tráfico entre partes de la red, o limitar el flujo del mismo basándose en ciertos criterios como el tipo de tráfico, origen, destino, etc.

- Segmentar servidores y servicios expuestos a Internet para que estén separados del resto de la red en una DMZ o en una infraestructura hosting separada. “Una zona desmilitarizada (*Demilitarized Zone, DMZ*) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet” [48].
  Es importante que servidores y dispositivos críticos estén adecuadamente aislados para protegerlos ante ataques.

- Se recomienda configurar controles de acceso y firewall para que servidores, dispositivos, controladores de dominio, es decir, cualquier sistema critico se tenga limitado su acceso. La mayoría de los entornos Cloud soportan separadas instancias virtuales privadas Cloud (Virtual Private Cloud, VPC).

"Las redes virtuales de Azure son similares a una LAN de red local. La idea detrás de una red virtual de Azure es crear una sola red basada en espacios privados de direcciones IP en la que pueden colocar todas las máquinas virtuales de Azure" [50]

Para segmentar lógicamente las subredes, Microsoft recomienda:

- No asignar reglas de permiso con intervalos muy grandes.
- Segmentar el mayor espacio de direcciones en las subredes.
- Crear controles de acceso de red entre subredes
- Minimizar la complejidad evitando redes virtuales y subredes pequeñas.
- Simplificar la administración de reglas de grupos de seguridad de red mediante la definición de grupos de seguridad de aplicaciones (Application Security Groups).

6.7.10 Prevención de Intrusión de Red

Uso de firmas de detección de intrusión para bloquear trafico en los límites de red.

Este tipo de protección mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Descubrimiento**
TÉCNICA	*Network Service Scanning*

Tabla 12. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Prevención de Intrusión de Red

En la táctica *Descubrimiento*, con la técnica *Network Service Scanning*, un atacante intenta averiguar los servicios que se están ejecutando en servidores remotos. Para ello puede valerse de herramientas para el escaneo de puertos y vulnerabilidades. En entornos Cloud, un atacante puede intentar obtener servicios ejecutándose en otros servidores Cloud, y si este está conectado a entornos locales también podría descubrir servicios ejecutándose en esos sistemas.

Se puede implementar sistemas de prevención de intrusiones y detección de intrusiones (*Intrusion Detection System, IDS/Intrusion Prevention System, IPS*) basados en la red para detectar y/o denegar el tráfico malintencionado y escaneo de servicios.

En entornos Azure se puede usar *Azure Firewall* con el filtrado de inteligencia sobre amenazas. Este puede alertar y denegar el tráfico desde y hacia los dominios y las direcciones IP malintencionados conocidos. Esta información proviene de la fuente Inteligencia sobre amenazas de Microsoft.

"Azure Firewall es un servicio de seguridad de red administrado y basado en la nube que protege los recursos de *Azure Virtual Network*. Con *Azure Firewall,* se pueden crear, aplicar y registrar directivas de conectividad de red y de aplicaciones de forma centralizada en suscripciones y redes virtuales. "[52]

"Si ha habilitado el filtrado basado en inteligencia sobre amenazas, las reglas asociadas se procesan antes que cualquiera de las reglas NAT, reglas de red o reglas de aplicación."[53]

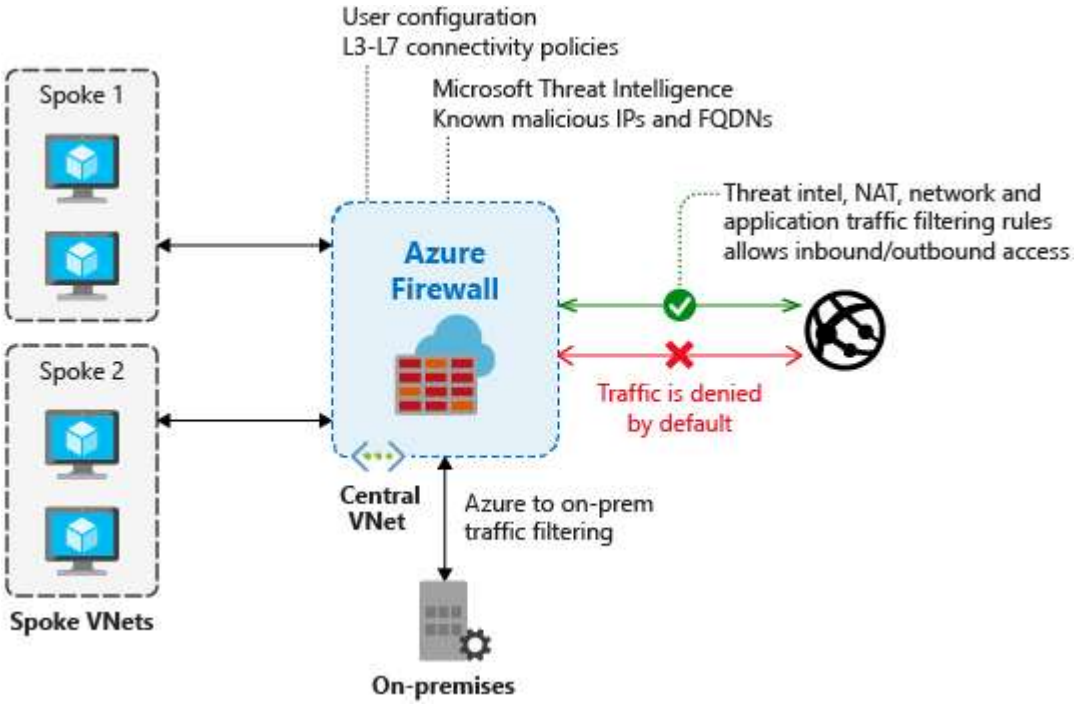

Figura 13. Azure Firewall [52]

6.7.11 Restringir Permisos en Directorios y Ficheros

Consiste en limitar el acceso estableciendo permisos de directorios y ficheros que no son específicos de los usuarios o cuentas con privilegios.

Esto mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Evasión de Defensa**	**Acceso a Credenciales**	**Recopilación**
TÉCNICA	*Impair Defenses*	*Unsecured Credentials*	*Data from Cloud Storage Object*
		Unsecured Credentials: Credentials In Files	

Tabla 13. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Restricción de Permisos en Directorios y Ficheros.

En la táctica de **Evasión de Defensa** encontramos la siguiente técnica con el objetivo de que el atacante no sea detectado:

- *Impair Defenses*: consiste en alterar componentes en los sistemas para dificultar o desactivar mecanismos de defensa, como firewalls o antivirus. También se incluiría la manipulación o eliminación de elementos para auditar actividad maliciosa.

En la táctica de **Acceso a Credenciales** encontramos la siguiente técnica:

- *Unsecured Credentials*: consiste en buscar en los sistemas y conseguir credenciales que se encuentran almacenadas de una forma insegura. Estas credenciales pueden estar en múltiples ubicaciones, por ejemplo, en ficheros de texto plano, repositorios del sistema operativo o de aplicaciones, o en otros ficheros como los de certificados claves privadas.
    - *Credentials In Files*: esta subtecnica consiste en localizar credenciales almacenadas en ficheros.

En la táctica de **Recopilación**, con la técnica *Data from Cloud Storage Object*, un atacante puede acceder a objetos de datos en un almacén de datos en la nube si no se encuentra apropiadamente securizado.

Como buenas practicas para mitigar las técnicas anteriormente mencionadas, se recomienda:

- Asegurarse que se establecen adecuados permisos en los ficheros para evitar que un adversario desactive o interfiera en servicios de seguridad o de registro de datos.
- Restringir la compartición de ficheros a directorios específicos a los que únicamente tengan acceso los usuarios que necesitan tener acceso a los mismos.
- Utilizar listas de control de acceso (*Access Control List, ACL*) en los sistemas de almacenamiento y en objetos. Una ACL es una lista de permisos asociados a un objeto, y que especifica que usuarios o procesos de sistema tienen permiso de acceso al objeto y que operaciones pueden realizar sobre dicho objeto. [55]

Para proteger los recursos en Azure, se puede usar el control de acceso basado en rol (RBAC) para asignar permisos a usuarios, grupos y aplicaciones en un cierto ámbito (una suscripción, un grupo de recursos o un único recurso). Una asignación de roles consta de tres elementos: entidad de seguridad, definición de rol y ámbito. Es importante utilizar el principio de privilegio mínimo y la separación de funciones

Se pueden utilizar los roles integrados de Azure para establecer permisos a los usuarios. Los cuatro roles integrados fundamentales son:

- *Propietario*: tiene acceso total a todos los recursos, incluido el derecho a delegar este acceso a otros.
- *Colaborador*: puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.
- *Lector*: puede ver los recursos existentes de Azure.
- *Administrador de acceso de usuario:* permite administrar el acceso de los usuarios a los recursos de Azure.

El rol de *Propietario, Colaborador* y *Lector* se aplican a todos los tipos de recursos.

Además de estos roles existen otros roles integrados que permiten la administración de recursos específicos de Azure, como el rol *Colaborador de máquina virtual*, que permite al usuario crear y administrar máquinas virtuales.
Si los roles integrados no satisfacen las necesidades específicas, es posible crear roles de manera personalizada.

6.7.12 Restringir Permisos en el Registro

La restricción de la posibilidad de modificar valores (hives y keys) en el Registro de Windows mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Evasión de Defensa**
TÉCNICA	Impair Defenses

Tabla 14. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con las restricciones en los permisos para modificar el registro.

En la táctica de **Evasión de Defensa** encontramos la técnica *Impair Defenses*, que consiste en alterar componentes en los sistemas para dificultar o desactivar mecanismos de defensa, como firewalls o antivirus, así como manipulación o eliminación de elementos para auditar actividad maliciosa.

Se recomienda establecer los permisos adecuados sobre el registro para evitar que un atacante puede desactivar o alterar controles de seguridad, y de registro y auditoria.

6.7.13 Copias de Seguridad de Datos

Realizar copias de seguridad o respaldos de datos (backups) de los sistemas de los usuarios y de servidores críticos. Es importante securizar estas copias, y los sistemas donde se almacenan para evitar que sean comprometidos o destruidos por un atacante.

Disponiendo de respaldo de datos se mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Impacto**
TÉCNICA	*Defacement*
	Defacement: External Defacement

Tabla 15. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Copias de Seguridad de Datos

En la táctica **Impacto**, tenemos la siguiente técnica:

- *Defacement*: un adversario puede alterar visualmente el contenido disponible interna o externamente en una red. Esto puede incluir lanzar mensajes, intimidar, reivindicar una intrusión, incluir imágenes perturbadoras u ofensivas para causar incomodidad o como medidas de presión, etc.
    - *External Defacement*: un adversario puede alterar sistemas externos de una organización. En esta subtecnica se incluye también engañar o inducir a error a una organización o usuarios. Un ejemplo común es a través de sitios web públicos.

Como buena práctica se recomienda implementar planes de recuperación de desastres que incluyan procedimientos para realizar copias de seguridad de datos regularmente, para que puedan ser restaurados si fuera necesario. Es importante asegurarse que estas estén adecuadamente protegidas.

Azure Backup es un servicio para realizar copias de seguridad de datos en entornos Azure, así como su recuperación. Permite realizar copias de seguridad, entre otros, de entornos locales, máquinas virtuales de Azure, recursos compartidos *Azure Files,* SQL Server en máquinas virtuales de Azure.

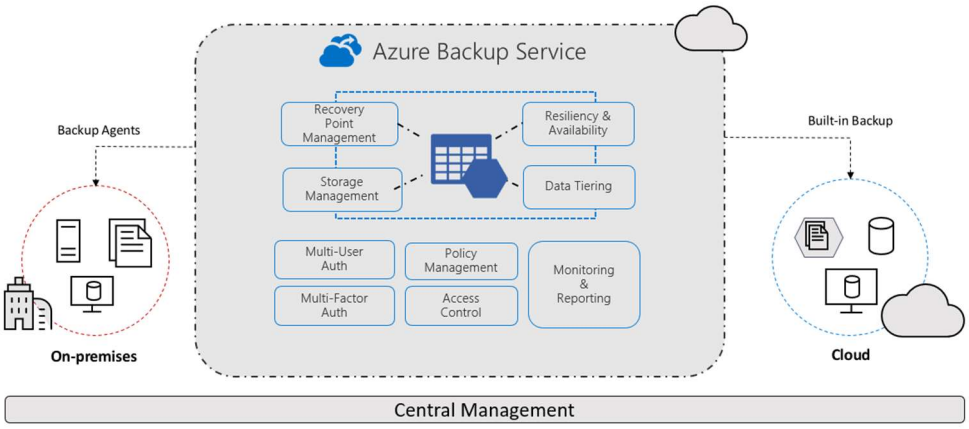

Figura 14. Azure Backup [59]

6.7.14 Configuración del Sistema Operativo

Realizar cambios en la configuración del sistema operativo o a una funcionalidad común del sistema operativo con el resultado de fortificar el sistema.

Con una configuración adecuada del sistema operativo se mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	Persistencia	Acceso a Credenciales	Descubrimiento
TÉCNICA	*Account Manipulation*	*Unsecured Credentials*	*Account Discovery*
	Create Account		*Network Share Discovery*

Tabla 16. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con la Configuración del Sistema Operativo.

En la táctica de **Persistencia** encontramos las siguientes técnicas con el objetivo de mantener el acceso a sistemas:

- *Account Manipulation*: un atacante puede alterar cuentas.

- *Create Account*: un atacante puede crear una cuenta local, en un dominio o en un inquilino en la nube (*cloud tenant*) para establecer unas credenciales de acceso complementarias.

En la táctica de **Acceso a Credenciales** encontramos la siguiente técnica:

- *Unsecured Credentials*: consiste en buscar en los sistemas y conseguir credenciales que se encuentran almacenadas de una forma insegura.

En la táctica de **Descubrimiento** encontramos las siguientes técnicas:

- *Account Discovery*: un atacante puede intentar obtener una lista de cuentas de un sistema o entorno.
- *Network Share Discovery*: un atacante intenta buscar en sistemas remotos carpetas y discos compartidos con el objetivo de identificar fuentes de información y potenciales sistemas. La compartición de ficheros en redes Windows utiliza el protocolo SMB. Las redes virtuales en la nube pueden contener recursos compartidos de red remotos o servicios de almacenamiento de archivos accesibles. Por ejemplo, *Azure Files*, es un servicio que permite crear y utilizar recursos compartidos de archivos en red en la nube mediante el protocolo SMB (*Server Message Block*).

A continuación, se describen algunas buenas practicas relativas a la configuración del sistema operativo para mitigar las técnicas descritas anteriormente.

- Es importante asegurarse tener correcta configuración de seguridad en los servidores críticos para proteger los controladores de dominio, limitando el acceso mediante protocolos y servicios que no son necesarios como por ejemplo el SMB para la compartición de ficheros.
- Se recomienda deshabilitar la posibilidad de recuperar el historico de los comandos ejecutados por el usuario (fichero .bash_history) para evitar el compromiso de credenciales almacenas de una manera insegura.
- Se puede prevenir que se enumeren las cuentas de administrador cuando una aplicación es elevada mediante UAC. Se puede deshabilitar mediante *GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: E numerate administrator accounts on elevation.*
- Para limitar que los usuarios puedan enumerar comparticiones en la red, se recomienda habilitar la politica de grupo de Windows "*Do Not Allow Anonymous Enumeration of SAM Accounts and Shares*"

6.7.15 Configuración del Software

La configuración de software puede prevenir riesgos relacionados con su operativa.

Una adecuada configuración del software mitiga el uso de las tácticas y técnicas que se muestran en la siguiente tabla:

TÁCTICA	**Evasión de Defensa**
TÉCNICA	*Unused/Unsupported Cloud Regions*

Tabla 17. Matriz Tácticas/Técnicas de MITRE ATT&CK para Azure mitigadas con Configuración de Software

La técnica *Unused/Unsupported Cloud Regions*, asociada a la táctica Evasion de Defensa, un atacante puede crear instancias de Cloud en regiones de servicios geográficos no utilizados para evitar ser detectado. Es frecuente que clientes solo usen un subconjunto de regiones disponibles y pueden no monitorizar otras regiones. Por eso, si un atacante crea recursos en una región no usada, podría actuar sin ser detectado.

Como mitigación los proveedores de servicios en la nube pueden permitir a los clientes desactivar regiones no usadas.

6.7.15 Otras buenas prácticas

Otras buenas practicas para mejorar la seguridad en entornos Cloud serían: Actualización del software, encriptar información sensible, seguir guías para securizar DevOps, considerar retirar aplicaciones antiguas (*legacy systems*), realizar auditorías, escaneos periódicos de vulnerabilidades y test de penetración, y concienciación/formación de los usuarios.

CAPÍTULO 7. CONCLUSIONES Y PROPUESTAS

En este último capítulo, se presentan las conclusiones de este TFM, y se sugieren algunas propuestas para trabajos futuros y posibles ampliaciones.

7.1 CONCLUSIONES

La computación en la nube es ya el presente, las personas y las organizaciones necesitan conectarse desde cualquier lugar, con la posibilidad de usar múltiples dispositivos. Esto implica que el perímetro ya no se encuentra delimitado. Asimismo, los ciberataques continúan incrementándose. Todo esto implica que es necesario entender las diferencias a nivel de seguridad entre los entornos tradicionales y los de Cloud, y cómo fortificar estos últimos entornos.

La elaboración de este TFM me ha permitido explorar y profundizar mis conocimientos de seguridad en entornos Cloud, Azure, MITRE ATT&CK, indicadores de ataque y las fases del ciclo de vida de un ciberataque.

7.2 TRABAJO FUTURO Y POSIBLES AMPLIACIONES

Para finalizar este último capítulo, se detallan algunas propuestas de trabajo futuro y posibles ampliaciones:

- En primer lugar, incluir más relación con MITRE Shield[65], que MITRE está desarrollando para capturar y organizar el conocimiento sobre defensa activa. Esta base de

conocimiento se ha publicado recientemente (agosto de este año), y aunque se incluye algo en este TFM, sería interesante profundizar en trabajos futuros.

- En segundo lugar, cubrir en profundidad técnicas de ATT&CK específicas para Office 365.

BIBLIOGRAFÍA

LIBROS Y ARTICULOS

[Chr19] Practical Cloud Security: A Guide for Secure Design and Deployment, Chris Dotson, (2019), O'Reilly

[Mic19] Security best practices for Azure solutions (April 2019), Microsoft.

[CCN19] Guía de seguridad TIC CCN-STIC 884A: Guía de configuración segura para Azure (Diciembre 2019), Centro Criptológico Nacional.

[MIT20] MITRE ATT&CK: Design and Philosophy https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[Nil19] Machine Learning for Monitoring Attacks in the Cloud, Nils van Noort http://essay.utwente.nl/82147/1/vanNoort_BA_EEMCS.pdf

ENLACES INTERNET

[1] Ciberseguridad del teletrabajo durante la pandemia, International Monetary Fund. https://www.imf.org/~/media/Files/Publications/covid19-special-notes/Spanish/sp-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx

[2] El COVID-19 y su impacto en Ciberseguridad, Vector ITC. https://www.vectoritcgroup.com/tech-magazine/cybersecurity/el-covid-19-y-su-impacto-en-ciberseguridad/

[3] El spam se incrementa en el primer trimestre de 2020, Computing. https://www.computing.es/seguridad/noticias/1118964002501/spam-se-incrementa-primer-trimestre-de-2020.1.html

[4] ¿Qué es Threat Hunting y por qué es necesario?, Panda Security. https://www.pandasecurity.com/spain/mediacenter/adaptive-defense/threat-hunting-por-que-necesario/

[5] ¿Cuáles son las diferencias entre los IOC y los IOA?, Cytomic.
https://www.cytomic.ai/es/threat-hunting/diferencias-entre-ioc-y-los-ioa/

[6] IOC Security: Indicators of Attack vs. Indicators of Compromise, CrowdStrike.
https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/

[7] Indicators of Attack (IoA), McAfee.
https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-indicators-of-attack.pdf

[8] The Pyramid of Pain, David J. Bianco.
https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

[9] Threat Hunting: La Piramide del Dolor [I], Segu-Info.
https://blog.segu-info.com.ar/2019/11/threat-hunting-la-piramide-del-dolor-i.html

[10] Emulating Attacker Activities and The Pyramid of Pain, Stephan Chenette, AttackIQ.
https://attackiq.com/2019/06/26/emulating-attacker-activities-and-the-pyramid-of-pain/

[11] El replanteamiento de la ciberseguridad, David Barroso.
https://www.slideshare.net/lostinsecurity/el-replanteamiento-de-la-ciberseguridad

[12] The Pyramid of Pain, EventTracker.
https://www.eventtracker.com/blog/2015/february/the-pyramid-of-pain/

[13] PHDays 2018 Threat Hunting Hands-On Lab.
https://www.slideshare.net/heirhabarov/phdays-2018-threat-hunting-handson-lab-97951462

[14] Inteligencia de Amenazas - Cazando ataques, Javier Díaz-Evans, A3Sec.
https://blog.a3sec.com/inteligencia-de-amenazas-cazando-ataques

[15] Threat Hunting with Cyber Kill Chain, Suwitcha Musijaral.
https://www.slideshare.net/suwitcha1/threat-hunting-with-cyber-kill-chain

[16] Kill chain, Wikipedia.
https://en.wikipedia.org/wiki/Kill_chain

[17] Adversary Emulation Plans, MITRE.
https://attack.mitre.org/resources/adversary-emulation-plans/

[18] MITRE releases emulation plan for FIN6 hacking group, more to follow. https://www.zdnet.com/article/mitre-releases-emulation-plan-for-fin6-hacking-group-more-to-follow/

[19] ATT&CK for Enterprise Introduction, MITRE. https://attack.mitre.org/resources/enterprise-introduction/

[20] How to Use MITRE ATT&CK, MARK DUFRESNE , Elastic. https://www.elastic.co/pdf/how-to-use-mitre-attack

[21] How to Be a Savvy ATT&CK Consumer. https://medium.com/mitre-attack/how-to-be-a-savvy-attack-consumer-63e45b8e94c9

[22] MITRE ATT&CK Cloud Matrix, MITRE. https://attack.mitre.org/matrices/enterprise/cloud/

[23] Autenticación de múltiples factores, Wikipedia https://es.wikipedia.org/wiki/Autenticación_de_múltiples_factores

[24] Creación de una entidad de servicio de Azure con la CLI de Azure, Microsoft. https://docs.microsoft.com/es-es/cli/azure/create-an-azure-service-principal-azure-cli?view=azure-cli-latest

[25] SAINTCON 2018 - Bryce Kunz - Blue cloud of Death: Red Teaming Azure. https://www.youtube.com/watch?v=wQ1CuAPnrLM

[26] Introducción a los servicios principales de Azure Storage, Microsoft. https://docs.microsoft.com/es-es/azure/storage/common/storage-introduction

[27] Referencia a API de REST de Azure Storage, Microsoft. https://docs.microsoft.com/es-es/rest/api/storageservices/

[28] Blob service API de REST, Microsoft. https://docs.microsoft.com/es-es/rest/api/storageservices/blob-service-rest-api

[29] Security recommendations for Blob storage, Microsoft. https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations

[30] Introducción a Azure Multi-Factor Authentication en una organización, Microsoft. https://docs.microsoft.com/es-es/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

[31] Procedimientos recomendados para la administración de identidades y la seguridad del control de acceso en Azure, Microsoft. https://docs.microsoft.com/es-es/azure/security/fundamentals/identity-management-best-practices

[32]¿Qué es el firewall de aplicaciones web de Azure?, Microsoft.
https://docs.microsoft.com/es-es/azure/web-application-firewall/overview

[33] Firewall de aplicaciones web de Azure en Azure Application Gateway, Microsoft.
https://docs.microsoft.com/es-es/azure/web-application-firewall/ag/ag-overview

[34] Reglas y grupos de reglas de CRS de Firewall de aplicaciones Web, Microsoft.
https://docs.microsoft.com/es-es/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=owasp31

[35] Attractive Accounts for Credential Theft, Microsoft.
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/attractive-accounts-for-credential-theft

[36] Implementing Least-Privilege Administrative Models, Microsoft.
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

[37] Securing privileged access for hybrid and cloud deployments in Azure AD, Microsoft.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-admin-roles-secure

[38] The Essential 8 Strategies to Mitigate Cybersecurity Incidents.
https://redpiranha.net/news/essential-8-strategies-mitigate-cyber-security-incidents

[39] NIST Special Publication 800-63B Digital Identity Guidelines.
https://pages.nist.gov/800-63-3/sp800-63b.html

[40] A Brief Summary of NIST Password Guidelines.
https://www.enzoic.com/nist-password-guidelines/

[41] Azure Instance Metadata Service (IMDS) , Microsoft.
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/instance-metadata-service

[42] Server Side Request Forgery, OWASP.
https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

[43] What is a Denial-of-Service Attack?
https://www.mcafee.com/blogs/consumer/identity-protection/denial-service-attack/

[44] Virtual Private Cloud, Wikipedia.
https://en.wikipedia.org/wiki/Virtual_private_cloud

[45] Azure DDoS Protection Standard overview, Microsoft.
https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview

[46] Azure DDoS Protection - Designing resilient solutions, Microsoft.
https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-best-practices

[47] Azure security baseline for Azure DDoS Protection Standard, Microsoft.
https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-protection-security-baseline

[48] Zona desmilitarizada (informática),Wikipedia.
https://es.wikipedia.org/wiki/Zona_desmilitarizada_(informática)

[49] Información general sobre los servicios de red de Azure, Microsoft.
https://docs.microsoft.com/es-es/azure/networking/networking-overview

[50] Procedimientos recomendados de seguridad de la red de Azure, Microsoft.
https://docs.microsoft.com/es-es/azure/security/fundamentals/network-best-practices

[51] Sistema de detección de intrusos, Microsoft.
https://es.wikipedia.org/wiki/Sistema_de_detección_de_intrusos

[52]¿Qué es Azure Firewall?, Microsoft.
https://docs.microsoft.com/es-es/azure/firewall/overview

[53] Filtrado basado en inteligencia sobre amenazas de Azure Firewall, Microsoft.
https://docs.microsoft.com/es-es/azure/firewall/threat-intel

[54] Security Control: Network Security, Microsoft.
https://docs.microsoft.com/en-us/azure/security/benchmarks/security-control-network-security

[55] Access-control list, Wikipedia.
https://en.wikipedia.org/wiki/Access-control_list

[56] What is Azure role-based access control (Azure RBAC)?, Microsoft.
https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

[57] Understand Azure role definitions, Microsoft.
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

[58] Azure built-in roles, Microsoft.
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

[59] What is the Azure Backup service?, Microsoft.
https://docs.microsoft.com/en-us/azure/backup/backup-overview

[60] Diagrama de Azure Multi-Factor Authentication, Channel 9.
https://channel9.msdn.com/Blogs/Azure/WA-MFA-Overview

[61] Overview of Azure Multi-Factor Authentication for your organization, Microsoft.
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

[62] CALDERA
https://github.com/mitre/caldera

[63] Infection Monkey
https://github.com/guardicore/monkey

[64] ATTPwn
https://github.com/ElevenPaths/ATTPwn

[65] MITRE Shield, MITRE.
https://shield.mitre.org/