Universidad Europea

MÁSTER UNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

TRABAJO FIN DE MÁSTER

Plan de continuidad de negocio de un file server ante un ataque de malware en Cloud

Autor
Luis Alonso Talavera Trevejo

Director del Trabajo Fin de Máster
Pablo González Pérez

CURSO 2021-2022

RESUMEN

A raíz de la pandemia suscitada en el año 2019, uno de los modelos tecnológicos que se empezó adoptar con mayor rapidez; es la computación en la nube (Cloud Computing, por sus siglas en inglés), tal es así que Microsoft reportó en el año 2020 un aumento del 775% en almacenamiento en nube.

Sin embargo, la adopción de este modelo tecnológico trajo consigo un aumento considerable de ataques maliciosos a los servicios que se encuentran alojados en cada una de las nubes disponibles en el mercado. Por ejemplo, Microsoft en su informe anual de Defensa Digital reportó un promedio de ataque anual de ransomware de 100 millones de ataques en último año fiscal (2020 - 2021), a diferencia del año fiscal predecesor que fue de un aproximado de 60 millones. El informe anual también nos muestra que los 05 principales sectores atacados son los siguientes: comercio minorista (13%), los servicios financieros (12%), la industria manufacturera (12%), la Administración pública (11%) y la sanidad (9%).

Debemos entender que la información más valiosa que tiene toda organización son sus datos, es por eso por lo que los ciberdelincuentes tratan constantemente de secuestrar los datos de toda organización; por consiguiente, también podemos mencionar que solo el 65% de las empresas que pagaron el rescate pudieron recuperar sus datos mientras que el 29% solo pudo recuperar su información de manera parcial.

Por consiguiente, el presente proyecto de fin de máster se ha centrado en implementar una estrategia de continuidad de negocio para un file server de cualquier organización, también es importante señalar que este trabajo está orientado a sistemas operativos Windows Server 2012 R2 en adelante, pues se ha tomado como premisa que el 74,49% de los ataques de ransomware se dan sobre el sistema operativo en mención; por otro lado, la guía o procedimiento se ha desarrollado sobre la nube de Microsoft.

Finalmente, es importante señalar que según las pruebas ejecutadas se ha pedido evidenciar que el rango de RPO es de 03 a 05 minutos, mientras que en un esquema tradicional puede tomar a 01 hora como mínimo; por otro lado, el RTO se ha reducido a 10 minutos, mientras que en un esquema tradicional puede tomar 02 horas como mínimo.

En conclusión, podemos indicar que hemos mejorado el SLA con respecto al esquema tradicional.

ABSTRACT

As a result of the pandemic that arose in 2019, one of the technological models that began to be adopted more quickly; is cloud computing (Cloud Computing, for its acronym in English), so much so that Microsoft reported in 2020 an increase of 775% in cloud storage.

However, the adoption of this technological model brought with it a considerable increase in malicious attacks on the services that are hosted in each of the clouds available on the market. For example, Microsoft in its annual Digital Defense report reported an average annual ransomware attack of 100 million attacks in the last fiscal year (2020 - 2021), as opposed to the previous fiscal year, which was approximately 60 million. The annual report also shows us that the 05 main sectors attacked are the following: retail (13%), financial services (12%), manufacturing (12%), public administration (11%) and health (9%).

We must understand that the most valuable information that any organization has is its data, that is why cybercriminals constantly try to hijack the data of any organization; therefore, we can also mention that only 65% of the companies that paid the ransom were able to recover their data while 29% were only able to partially recover their information.

Therefore, this master's thesis project has focused on implementing a business continuity strategy for a file server of any organization, it is also important to point out that this work is oriented to Windows Server 2012 R2 operating systems onwards, since It has taken as a premise that 74.49% of ransomware attacks occur on the operating system in question; on the other hand, the guide or procedure has been developed on the Microsoft cloud.

Finally, it is important to point out that according to the tests carried out, it has been requested to show that the RPO range is from 03 to 05 minutes, while in a traditional scheme it can take at least 01 hour; on the other hand, the RTO has been reduced to 10 minutes, while in a traditional scheme it can take at least 02 hours.

In conclusion, we can indicate that we have improved the SLA with respect to the traditional scheme.

AGRADECIMIENTOS

Un agradecimiento especial a mis padres (Luis Talavera y Juana Trevejo) por darme la sabiduría y valores y así forjar en mí el aprendizaje de manera constante.

Un agradecimiento especial a pareja Katherinne Oyarce por apoyarme en todos mis emprendimientos y darme el soporte necesario en cada paso que doy.

Índice

RESUMEN 3

ABSTRACT 4

1. INTRODUCCIÓN 11

2. ESTADO DE LA CUESTIÓN 13

3. DESCRIPCIÓN DEL PROBLEMA 18

4. DESCRIPCIÓN DEL PROBLEMA 20

4.1 Objetivos 20

4.2 Metodología 20

4.3 Planificación 32

4.4 Implementación 32

5. PRUEBAS Y VALIDACIÓN 57

5.1 Evasión de AMSI 57

5.2 Actividad inusual con IP maliciosa 59

5.3 Detección automática del malware 61

5.4 Ejecución de malware 64

5.5 Restauración de un archivo 68

6. RESULTADOS 71

4.1 Objetivo General 01 71

4.2 Objetivo General 02 71

4.3 Objetivo General 03 71

4.4 Objetivo General 04 72

7. CONCLUSIONES 73

8. TRABAJOS FUTUROS 75

9. REFERENCIAS 76

Índice de Figuras

Figura 1 Evolución del Ransomware (Microsoft, ¿Que es el Ransomware según Microsoft?, 2022) 12

Figura 2 Patrón del Ransomware (Microsoft, ¿Que es el Ransomware según Microsoft?, 2022) 14

Figura 3 Estadística de Sistemas Operativos (AV-TEST, 2019) 14

Figura 4 Estadística Global del Estado del Ransomware 2021 (Sophos, 2021)..... 16

Figura 5 Factores que intervienen en la metodología de la investigación (QuestionPro, s.f.) ... 21

Figura 6 Recomendación de Permisos CSA (Alliance, 2017) 27

Figura 7 Inicio de Sesión en el portal de Microsoft Azure 33

Figura 8 Arquitectura de Servicios en el portal de Microsoft Azure 34

Figura 9 Buscar Microsoft Defender for Cloud en el portal de Microsoft Azure 35

Figura 10 Microsoft Defender for Cloud en el portal de Microsoft Azure 36

Figura 11 Creación del servicio de la cuenta de almacenamiento en Microsoft Azure 37

Figura 12 Creación del Azure File en la cuenta de almacenamiento en Microsoft Azure 37

Figura 13 Creación del servicio de Azure File Sync en Microsoft Azure..... 38

Figura 14 Creación del servicio de Azure Automatización en Microsoft Azure 39

Figura 15 Creación del servicio de Azure Backup en Microsoft Azure..... 39

Figura 16 Creación del servicio de Log Analytics en Microsoft Azure..... 40

Figura 17 Creación del servicio de Máquina Virtual en Microsoft Azure..... 41

Figura 18 Asociación de un disco de Datos a la Máquina Virtual en Microsoft Azure..... 41

Figura 19 Creación del servicio de Logic App en Microsoft Azure 42

Figura 20 Creación de Azure File Share en Almacenamiento en Microsoft Azure 43

Figura 21 Proceso de instalación del agente en la máquina virtual de file server..... 44

Figura 22 Finalización de la instalación del agente en la máquina virtual de file server 44

Figura 23 Ingreso de credenciales en agente de Azure File Sync..... 45

Figura 24 Ingreso de credenciales en agente de Azure File Sync..... 46

Figura 25 Visualización del registro del agente instalado en servidor file server. 46

Figura 26 Creación del Grupo de Sincronización en Azure File Sync de Microsoft Azure..... 47

Figura 27 Visualización del Grupo de Sincronización creado en Azure File Sync de Microsoft Azure 47

Figura 28 Configuración de Grupo de Sincronización en Azure File Sync de Microsoft Azure ... 48

Figura 29 Visualización de información sincronizada en File Share ... 49

Figura 30 Visualización de información en servidor de File server ... 49

Figura 31 Configuración de Azure Backup con la cuenta de almacenamiento ... 50

Figura 32 Configuración de Azure Backup con la cuenta de almacenamiento ... 50

Figura 33 Visualización de la cuenta de ejecución en cuenta de automatización en Microsoft Azure ... 51

Figura 34 Visualización de runbook generado en la cuenta de automatización en Microsoft Azure ... 51

Figura 35 Script de Powershell que genera un snapshot en Azure Backup en Microsoft Azure 53

Figura 36 Creación de flujo aplicación de generación de snapshot en Logic App en Microsoft Azure ... 54

Figura 37 Instalación de agente asociado a Log Analytics. ... 55

Figura 38 Visualización del agente instalado en servidor de File server ... 55

Figura 39 Asociación de Microsoft Defender con Logic App en Microsoft Azure ... 56

Figura 40 Ejecución de código AMSI ... 57

Figura 41 Detección de código AMSI ... 57

Figura 42 Generación de Flujo en LogicApps a partir de AMSI ... 58

Figura 43 Generación de Script en Azure Automation a partir de AMSI ... 58

Figura 44 Generación de Backup a partir del AMSI ejecutado ... 59

Figura 45 Detección de IP maliciosas ... 59

Figura 46 Generación de Flujo en LogicApps a partir de IP maliciosa ... 60

Figura 47 Generación de Script en Azure Automation a partir de IP maliciosa ... 60

Figura 48 Generación de Backup a partir del IP maliciosa ... 61

Figura 49 Detección de Ransomware en el servidor ... 62

Figura 50 Detección de ransomware Phobos ... 62

Figura 51 Inicio de generación de Flujo en LogicApps a partir de ransomware detectado ... 63

Figura 52 Generación final de Flujo en LogicApps a partir de ransomware detectado ... 63

Figura 53 Generación de Script en Azure Automation a partir de detección de malware ... 64

Figura 54 Generación de backup a partir de de detección de ransomware ... 64

Figura 55 Ransomware ejecutado en nuestro servidor ... 65

Figura 56 Detección de alertas en el servicio de Microsoft Defender for Cloud 65

Figura 57 Generación de trigger en LogicApps 66

Figura 58 Ejecuciones de Azure Automation a partir de ejecución de ransomware 66

Figura 59 Generación de backups a partir del ransomware ejecutado 67

Figura 60 Revisión de un backup generado por la ejecución del ransomware..... 67

Figura 61Visualización de archivo afectado por el ransomware 68

Figura 62 Visualización de un archivo de backup previo 68

Figura 63 Opción de restauración de archivo 69

Figura 64 Opción sobrescribir de restauración de archivos..... 69

Figura 65 Archivo sobrescrito sobre el afectado..... 70

Índice de Tablas

Tabla 1 Amenazas y Riesgos 28

Tabla 2 Nivel de Impacto 29

Tabla 3 Nivel de Impacto por Categoría 29

Tabla 4 Nivel de Probabilidad 30

1. INTRODUCCIÓN

En 1963 el MIT presentó un proyecto de desarrollo de una tecnología que permitiese que una computadora fuese utilizada por dos o más personas de manera simultánea, fue en dicho acontecimiento en el que se dio a conocer el concepto de “cloud computing”, además en el mismo año se dio a conocer la palabra “virtualización” la cual tenía como significado principal la funcionalidad antes señalada. Por otro lado, también es importante señalar que el modelo principal del cloud computing es el de alquilar servicios; por lo que si hacemos una remembranza de los servicios que se han ofrecido alrededor de los años, podemos identificar que a finales de la década de los 90 y a principios del año 2000, comenzaron a brindarse servicios de correo a través de internet, como por ejemplo Yahoo Mail y Hotmail, además de brindar hosting de virtualización de máquinas virtuales.

Hoy en día, la nube ha evolucionado a una escala inigualable en cuanto al ofrecimiento de servicios, éstos actualmente son segmentos por tipos o modelos, dentro de los principales que podemos encontrar en el mercado son IaaS (Infraestructura como Servicio), PaaS (Plataforma como Servicio) y SaaS (Software como Servicio); sin embargo, cabe precisar que existen muchos más modelos de servicios que ofrecen actualmente los proveedores de nube; dentro de los principales destacan Microsoft y Amazon como los líderes del mercado, pero también existen otros proveedores como Google, IBM, entre otros.

También debemos resaltar que en 1989 Joseph Popp, creó el troyano AIDS el cual fue distribuido a través de disquetes que fueron entregados a asistentes de una conferencia sobre el SIDA, dicho evento se le conoce como el primer ataque de ransomware de la historia. Pero éste al igual que el modelo cloud computing también ha evolucionado a un nivel crítico para las organizaciones, pues en caso de que un atacante pueda cumplir el objetivo de infectar archivos con este tipo de malware, las consecuencias para las organizaciones pueden ser en algunos casos hasta la quiebra, por ende, es importante evitar las disrupciones de acceso a la información por parte de los colaboradores de una determina organización. Hoy en día existe una variedad importante de malwares en el ciberespacio, pero el ransomware es la familia de malware que más asecha a la información de toda organización, dentro de los más conocidos tenemos: Cryptolocker, WannaCry, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw, Locky, Petya, Conti, Sodinokibi y Ryuk.

Hoy en día existe un nuevo modelo comercial llamado "**Ransomware como Servicio (RaaS)**" o también llamado "**Ransomware Operado por Humanos**", este nuevo modelo está orientado al alquiler o ventas de herramientas por parte de los atacantes hacia el publico en general, por ende, podemos presumir que los ataques incrementarían de manera exponencial, pues cualquier persona con conocimientos básicos de informática podrá ejecutar cualquier tipo de ataque (Microsoft, Ransomware-as-a-service, 2022).

Por tanto, la nube como el malware a lo largo de los años han ido evolucionando, para el caso de la nube se ha vuelto un servicio indispensable hoy en día, pues este ofrece una variedad de servicios muy potentes e indispensables para toda organización, mientras que los diferentes ransomware cada día se vuelven más robustos y siempre están al asecho de cualquier vulnerabilidad o mala configuración que permita explotarla para evitar el acceso a la información por parte de los colaboradores de cualquier organización.

Finalmente, según (Bachmaier, 2006) indica que el 90% de las organizaciones cierra tras un incidente grave de perdida de datos, además también señala que el 43% de las organizaciones que sufren un destrate nunca se recuperan.

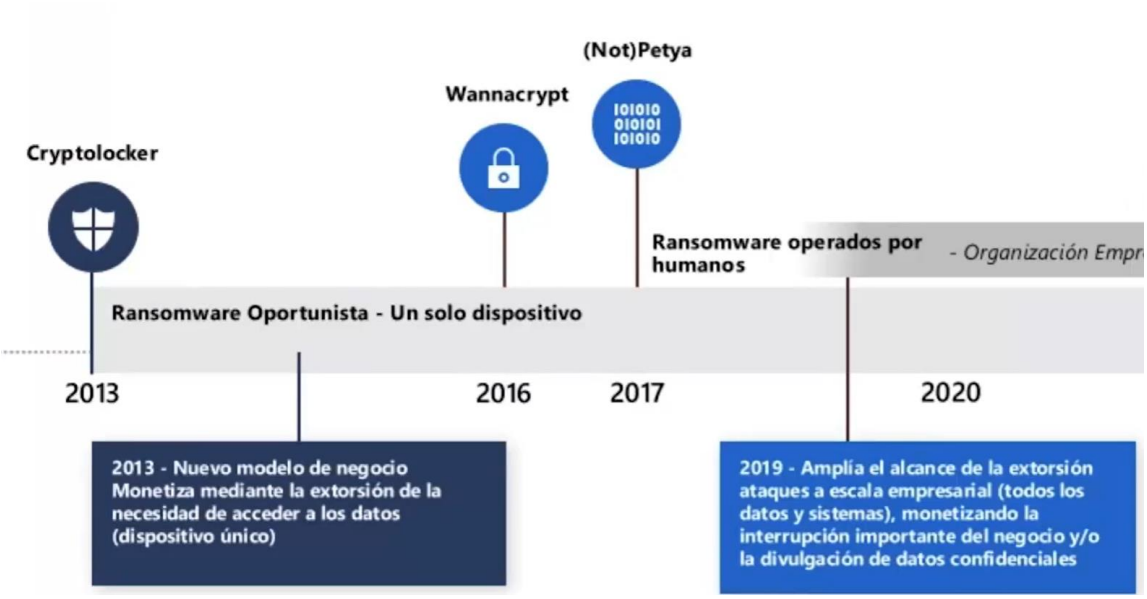

Figura 1 Evolución del Ransomware (Microsoft, ¿Que es el Ransomware según Microsoft?, 2022)

2. ESTADO DE LA CUESTIÓN

A lo largo de los años los malwares han evolucionado de distinta manera, pues a la fecha tenemos una gran variedad de tipos de malware, entre ellas podemos citar backdoors, spyware, virus, gusanos, troyanos, bots, ransomware, ATPs, entre otros. Cada uno de estos, se clasifican por familia de malware. Para hacer la clasificación podemos utilizar diferentes técnicas de clasificación como lo son Sandbox, Anubis, Virus total, entre otros. (Rivera Guevara, 2018) explica muy bien en su trabajo de investigación.

Nuestro trabajo de investigación se centra específicamente en los malware de tipo ransomware, es por eso, que debemos conocer cuáles son las formas de infectarse de este tipo de malware. (Info-lab, 2017) describe claramente las formas más comunes de infectarse. A continuación, se detalle un resumen de cada uno de ellos.

- **Ingeniería Social. –** Esta técnica es una de las más comunes, y se basa específicamente en la mayoría de los casos en engañar y/o inducir a la víctima a la instalación de algún programa malicioso. Por otro lado, es importante precisar que los medios para aplicar este tipo de engaños es correo electrónico, descargas web, redes sociales, entre otros.
- **Vulnerabilidades del Sistema Operativo. –** Entendamos por vulnerabilidad a un defecto y/o brecha de seguridad que permite a un atacante aprovecharse y generar un comportamiento no deseado del sistema. Por ende, el atacante desarrolla un programa o serie de comandos normalmente denominado "**exploit**"; el cual persigue el objetivo principal, ejecutar un exploit para instalar el ransomware. Una vez logrado el cometido, es cuestión de tiempo para que los datos se cifren y de esa manera pidan rescate por ellos.
- **Vulnerabilidades del Red. –** Esta forma de infectarse se da normalmente bajo la técnica de "**man in the middle**", que básicamente sucede cuando un ordenador se conecta a una red que actúa como intermediaria entre el origen y destino; por ejemplo, uno de los dispositivos intermediarios podría encontrarse infectado redirigiendo todo el tráfico hacia el equipo intermedio que modifique el contenido original, con ello genera vulnerabilidades sobre el equipo que finalmente lo recibe; éste tipo de técnica es un escenario usual para introducir el ransomware en los equipos origen y destino.

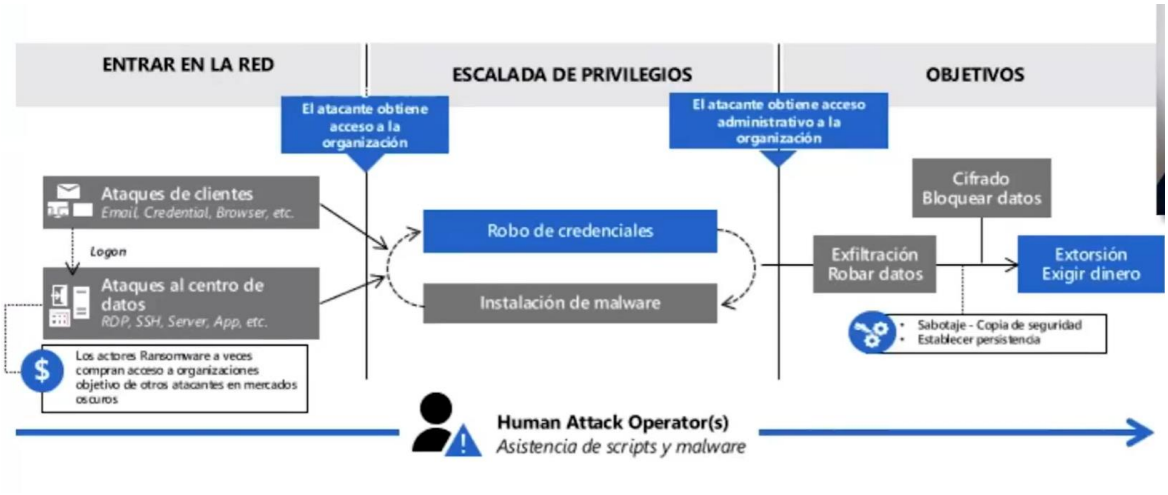

Figura 2 Patrón del Ransomware (Microsoft, ¿Que es el Ransomware según Microsoft?, 2022)

Además, es importante señalar que el presente trabajo de investigación está centrado en el sistema operativo Windows, esto debido a que en según el artículo publicado por (AV-TEST, 2019), que es el instituto de investigación independiente en materia de seguridad informática de Alemania; indica que el sistema operativo en mención se ha convertido en el sistema operativo que más ataques de ransomware recibe hoy en día, teniendo un crecimiento del 51.08% al 74.49%.

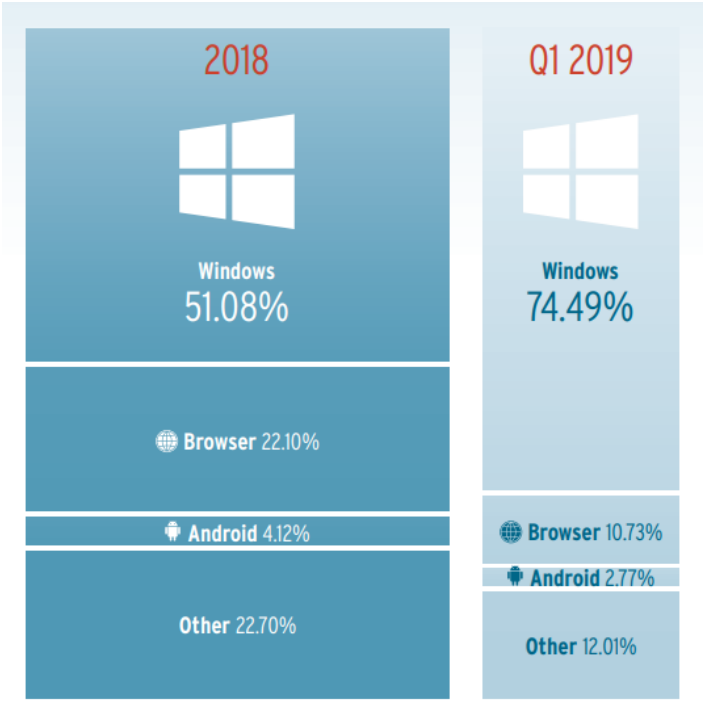

Figura 3 Estadística de Sistemas Operativos (AV-TEST, 2019)

Por otro lado, un informe más reciente de (Virtus Total, 2021), señala que el 95% de los archivos con ransomware detectados fueron ejecutables basados en Windows o vínculos dinámicos (DLL).

En el mundo globalizado en el que nos encontramos, las organizaciones tienen a la información y/o datos como el recurso más importante y valioso que pueden tener en la actualidad; por ende, el ransomware tiene como objetivo principal encriptar la información más valiosa de la organización que puede variar en función al rubro de ésta, una vez que el atacante ha cometido su objetivo, la siguiente etapa es que el atacante se contacte con la organización para pedirle una recompensa por el desencriptamiento de los datos.

Es por ello por lo que en el informe del (Centro Critológico, 2018), indica que en el 2014 se estimaba un promedio de 373$ por equipo infectado, en 2015 de 294$, pero en 2016 la media se situaba en 1077$ dólares según Symantec (2017).

En el informe de (Sophos, 2021), indica que el impacto financiero se ha duplicado, ya que en el 2020 el costo era de $761,106.00 mientras que en el 2021 fue de $1,85 millones; dichos datos a generado un negocio lucrativo para los atacantes, pues el mismo informe indica que la cantidad de organizaciones que pagaron por el rescate aumentó en un 6% entre los años 2020 y 2021 (26% y 32% respectivamente). Sin embargo, es importante señalar que no todas las empresas que pagan recuperan su información, según el informe solo el 65% recuperó su información en su totalidad, mientras que el 29% lo recuperó de forma parcial y el 8% no recuperó su información.

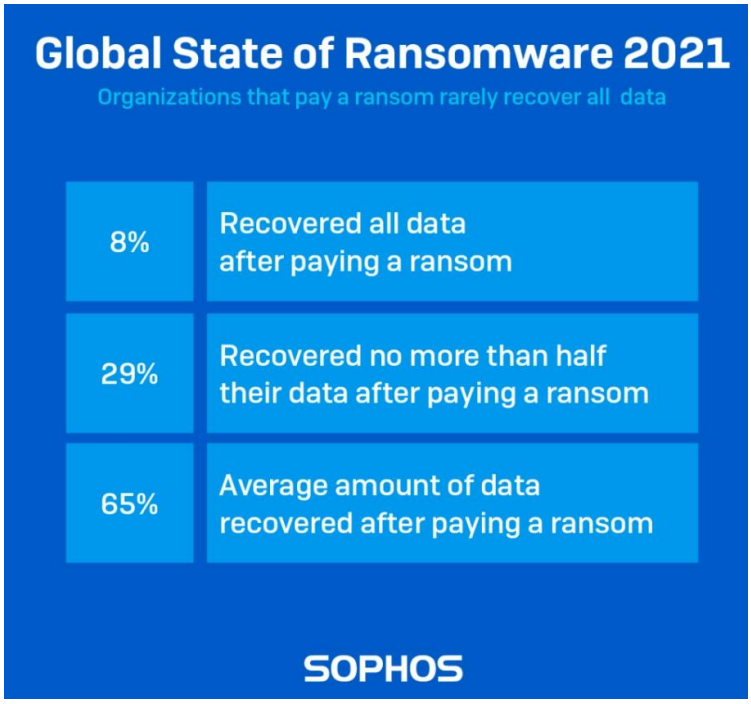

Figura 4 Estadística Global del Estado del Ransomware 2021 (Sophos, 2021)

Por otro lado, el presente trabajo de investigación también se centra, en implementar y configurar de manera correcta los servicios que provee un determinado proveedor de nube, para este caso será la plataforma de Microsoft Azure. Debemos tener en cuenta que los proveedores nube en la actualidad ofrecen tecnologías a gran escala que difícilmente cualquier organización la pueda tener hoy en día, y esta a su vez se puede utilizar en cuestión de minutos, en la misma línea además es importante señalar que estos proveedores en la actualidad cumplen con la mayoría de los estándares que la industria ha publicado (Microsoft, Centro de Cumplimiento, 2022).

Microsoft ha señalado en su último informe de ciberseguridad (Microsoft, Informe Anual de Ciberseguridad, 2021) que analiza más de 24 billones de señales de seguridad cada 24 horas, también se ha descubierto más de 25 técnicas de correo electrónico malicioso, además de 15 mil sitios de phishing fueron neutralizados en tres meses, entre otros.

Finalmente, es importante señalar que la industria ya ha publicado estándares enfocados a la continuidad de negocio. En la actualidad tenemos la norma ISO 22301:2019 (ISO ORG, 2019), el cual está orientada a responder de forma inmediata y de manera adecuada ante cualquier ocurrencia o incidente que afecte de manera directa a un proceso crítico de un determinado

negocio. Se ha identificado que se ha hecho un estudio por parte de (Villacís Onofa, 2018), orientada a la continuidad de negocio de un file server en la nube, pero ésta está orientada a la nube de Google y además está enfocada a desastres naturales y corte de energía electrónica; también es importante señalar que el estudio en mención está enfocado a la ISO mencionada en el presente párrafo. La diferencia con este estudio es que está orientada a un ataque de rasomware y utilizando el proveedor de nube de Microsoft.

3. DESCRIPCIÓN DEL PROBLEMA

Entendamos por ransomware como un tipo de malware cuyo objetivo principal es tomar el control de los datos de una organización y exigirle al dueño de éste el pago de un rescate para su liberación, por eso, que primero debemos entender como es el modus operandi del ransomware.

(Info-lab, 2017), describe las cinco fases del modus operandi que debemos de tener en cuenta. A continuación, se detalla cada uno de ellos:

1. **Infiltración. –** La primera fase, es la cual el ciberdelincuente debe de infiltrarse en el sistema informático de la organización; las maneras de infiltrarse ya se han detallado en el capítulo anterior de este documento.
2. **Búsqueda de objetivo. –** La segunda fase, es la búsqueda, la cual está orientada básicamente a la búsqueda de archivos de interés para la organización, una vez encontrada la información de interés comienza la operación "**cifrado**". Según el tipo de ransomware la forma de cifrado se puede dar de distintas maneras.
3. **Contactar a la víctima. –** La tercera fase, está basada básicamente, en el motivo de este tipo de ataques, el cual es contactar a la víctima y pedir el rescate por la información cifrada. Usualmente los atacantes piden criptomonedas (ejemplo: Bitcoin) como forma de pago y la forma de comunicarse con los atacantes es por la red Tor.
4. **Contactar a los ciberdelincuentes. –** La cuarta fase, esta orienta a la que la organización debe de contactar con los ciberdelincuentes para solicitar las claves de descifrado, previo pago por ello.
5. **Voluntad de los ciberdelincuentes. –** La quinta fase, es la de apelar a la voluntad o honestidad del ciberdelincuente, pues si cumple con la parte que le corresponde, la cual es la entrega de las claves o herramientas que le permita a la organización la recuperación de su información.

Por lo mencionado, podemos mencionar que el problema principal el cual se basa este trabajo de investigación es el de evitar las disrupciones en el acceso de los usuarios a la información corporativa almacenada en un file server debido a un ataque de malware (ransomware). Por otro lado, hemos podido evidenciar que la mayoría de los ataques se orientan a los sistemas

operativos Windows, es por eso, que podemos indicar la disrupción de los accesos estará orientada específicamente a sistemas operativos Windows Server 2012 R2 en adelante.

4. DESCRIPCIÓN DEL PROBLEMA

En este capítulo estará orientado a la descripción de los objetivos, la metodología y la implementación de la propuesta del presente estudio.

4.1 Objetivos

4.1.1 Objetivos Generales

A continuación, se detalla los objetivos generales de la presente investigación.

- Elaborar un plan o guía de continuidad de negocio de un file server ante un ataque de malware en cloud.
- Reducir el tiempo de recuperación (RTO) ante un ataque de malware de un file server.
- Reducir el objetivo de punto de recuperación (RPO) ante un ataque de malware sobre un file server.
- Implementar un plan de continuidad de negocio con los estándares más reconocidos de la industria.

4.1.2 Objetivos Específicos

A continuación, se detallan los objetivos específicos.

- Aumentar la probabilidad de continuidad el servicio de un file server en cloud.
- Aprender a configurar los servicios en la nube de Microsoft Azure para poder implementar una continuidad de negocio.
- Crear un equipo de continuidad de negocio ante una contingencia no planificada.
- Evitar la tensión o crisis en la organización ante un ataque de malware.

4.2 Metodología

4.2.1 Diseño

En la siguiente sección se detallará en primer lugar la metodología que se va a utilizar en el presente estudio. Por otro lado, se hará un análisis de la norma ISO 22301:2019 (ISO ORG, 2019) que está orientado a la continuidad de negocio de algún activo critico de una determinada organización. Finalmente, se detallará los servicios en la nube que se utilizarán para la implementación de los objetivos propuestos.

4.2.2 Metodologías a Utilizar

A continuación, se detallan las metodologías utilizadas en el presente estudio.

4.2.2.1 Metodología Investigativa

La metodología investiga es un conjunto de procedimientos y técnicas que se aplican de manera ordenada y sistemática en la realización de un estudio (Significados, s.f.).

Además, la metodología investigativa tiene como característica principal recopilar diversas técnicas, que permita recopilar datos y sacar conclusiones sobre la investigación que se va a desarrollar. En conclusión, esta metodología está orientada a un proyecto de investigación o estudio, el cual se propone en el siguiente estudio; por eso, esta metodología nos permitirá explorar las diferentes fuentes de información que podemos encontrar en los diferentes orígenes de datos.

A continuación, se muestra los factores claves que tiene la metodología en mención.

Figura 5 Factores que intervienen en la metodología de la investigación (QuestionPro, s.f.)

4.2.2.2 Revisión de la ISO 22301:2019

Este estándar de la industria como ya se ha mencionado en la sección de estado de la cuestión de este documento, esta está orientada a implementar estrategias de continuidad de negocio sobre algún activo critico de una determina organización.

Por otro lado, también es importante señalar que la norma permite supervisar y revisar los resultados de las actividades ejecutadas; de esa manera se garantiza el cumplimiento de este; además la norma permite identificar cada uno de los requerimientos que puede tener la organización, en este caso, estará asociado a los objetivos propuestos previamente.

La norma también señala de manera explícita que se debe de revisar los resultados obtenidos cuando existe una interrupción o cuando se haya activado la estrategia de continuidad de negocio; de esa manera se podrá aplicar mejoras a la estrategia propuesta. A continuación, se detalla las cláusulas que tiene consigo la norma (Villacís Onofa, 2018).

1. **Cláusula 1 Alcance. –** Esta primera cláusula, se dónde se establece lo que se va a implementar, mejorar o asegurar. Usualmente esta cláusula esta alineada a la política propuesta por la organización.
2. **Cláusula 2 Referencias Normativas. –** Esta segunda cláusula, está orientada a recopilar los estándares o normativas publicados por la industria, los cuales servirán de guía para el presente documento, así como también para el despliegue del alcance propuesto.
3. **Cláusula 3 Términos y Definiciones. –** Esta tercera cláusula, es donde se establece los términos y definiciones que se irán detallando en este documento; además esta cláusula es importante para el buen entendimiento al momento del despliegue y/o mantenimiento.
4. **Cláusula 4 Contexto de la Organización. –** Esta cuarta cláusula, se establece el rubro, procesos, entre otros de la organización.
5. **Cláusula 5 Liderazgo. –** Esta quinta cláusula, se debe de involucrar a los colaboradores que participaran en la implementación, sin embargo, es importante señalar que el mejor escenario es involucrar a la alta dirección, de esa manera se podrá llegar al éxito de los objetivos propuestos.
6. **Cláusula 6 Planificación. –** Esta sexta cláusula, se identifican los objetivos estratégicos que se deberá de cumplir al momento de implementar la continuidad de negocio. Además, también se deben de identificar los riesgos y requisitos en función al alcance.
7. **Cláusula 7 Soporte. –** Esta séptima cláusula, es la que nos permite identificar los colaboradores que cuenten con experiencia en la implementación de las actividades, además de que puedan responder de manera inmediata ante cualquier incidente.
8. **Cláusula 8 Operación. –** Esta octava cláusula, es donde se pone en marcha las actividades planificadas, además es importante tener en cuenta el impacto y los riesgos que se pueden tener al momento de hacer la implementación.
9. **Cláusula 9 Evaluación de Desempeño. –** Esta novena cláusula, está orientada a la realización de seguimiento de las funcionalidades implementadas, dicho seguimiento se debe de hacer mediante objetivos, metas, procesos, entre otros.

10. **Cláusula 10 Mejoras. –** Esta décima cláusula, está orientada a la revisión constante de los cambios que tiene toda organización, por consiguiente, es importante revisar de manera constante la eficacia y eficiencia de las actividades y procedimientos que se encuentran activos.

4.2.2.3 Implementación de la Metodología

En esta sección se desarrollará de implementación norma ISO22301:2019 según las cláusulas detalladas de manera previa en este documento.

1. Alcance. – El presente trabajo de investigación se limita de manera general a describir una guía o procedimiento para poder implementar de manera correcta un plan de continuidad de negocio de un file server en la nube.

Por consiguiente, se detalla el siguiente alcance:

- La guía o procedimiento se basará específicamente en sistemas operativos Windows Server 2012 R2 en adelante.
- La guía o procedimiento se basará específicamente en la nube de Microsoft Azure.
- La guía o procedimiento se basará específicamente con el ramsomware phobos en cualquiera de sus versiones.

2. Referencias Normativas. – A continuación, se detalla las referencias normativas publicadas por la industria en la cual se han basado el presente proyecto de investigación.

- **CSA. –** La Cloud Security Alliance (CSA), es una guía de seguridad para áreas críticas en un enfoque cloud. Dicha guía está separada por dominios, para nuestro proyecto de investigación vamos a trabajar con el Dominio 6: Plano de Gestión y Continuidad de Negocio (Alliance, 2017).
- **CIS. –** El Centro para la Internet Segura (CIS), donde se detallan una serie de controles críticos que se deben de implementar para mitigar los ataques más frecuentes contra sistemas y redes. Esta guía está separada por controles, para nuestro proyecto de investigación vamos a trabajar con el Control 11: Recuperación de Datos (Security, 2021).

3. Términos y Definiciones. – A continuación, se detalla los términos y definiciones más importantes se deben de tener en cuenta para el buen entendimiento de la implementación de la solución.

- **IaaS. –** Infraestructura como servicio (IaaS, por sus siglas en inglés), es un tipo de servicio en la nube que ofrece servicios esenciales de procesamiento, almacenamiento y redes a petición y/o demanda procesamiento del usuario (Microsoft, Qué es IaaS, s.f.).
- **PaaS. –** Plataforma como servicio (PaaS, por sus siglas en inglés), es un entorno de desarrollo e implementación completo sobre la nube, con recursos completos sobre alguna funcionalidad o feature especifico (ejemplo: base de datos, web sites, almacenamientos, iis, etc.), y puede ser a petición y/o demanda del usuario (Microsoft, Qué es PaaS, s.f.).
- **SaaS. –** Software como servicio (SaaS, por sus siglas en inglés), es una aplicación sobre la nube donde los usuarios se conecta a través de internet para usarlas, básicamente es alquilar una aplicación alojada en la nube (Microsoft, Qué es SaaS, s.f.).
- **BCP. –** Plan de continuidad de negocio (BCP, por sus siglas en inglés), es una guía o procedimiento donde se describe cual es el procedimiento para seguir para que la organización pueda seguir funcionando durante una interrupción no planificada (IBM, 2020).
- **RTO. –** Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés), está orientado al tiempo máximo que una empresa define para la recuperación de un activo critico que ha sido afectado por una contingencia (Acktib, 2021).
- **RPO. –** Objetivo de Punto de Recuperación (RPO, por sus siglas en inglés), está relacionado con la copia de seguridad de los datos de un determinado evento, es decir, define el tiempo máximo de la última copia de seguridad que el negocio puede permitirse perder ante una contingencia (Acktib, 2021).
- **DraaS. –** Recuperación ante Desastre como Servicio (DraaS, por sus siglas en inglés), es un modelo de servicio en la nube que permite a las organizaciones en la nube almacenar copias de seguridad en la nube, para luego recrear los servicios en la nube ante una contingencia no planificada (VMWARE, s.f.).
- **Microsoft Defender for Cloud. –** Es un Servicio de Microsoft Azure, que permite administrar la seguridad y revisar las amenazas tanto servicios en la nube como

servicios en entornos locales (Microsoft, ¿Qué es Microsoft Defender for Cloud?, 2022).

- **Azure Files. –** Es un servicio de Microsoft Azure, que ofrece recursos que permite compartir archivos totalmente administrados por Microsoft mediante el protocolo SMB (Microsoft, ¿Qué es Azure Files?, 2022). Dicho servicio es un tipo de almacenamiento que ofrece el servicio de almacenamiento de Microsoft Azure, a continuación, se adjunta la lista de tipos de almacenamiento que ofrece dicho servicio (Microsoft, Tipos de almacenamiento del servicio de Almacenamiento de Microsoft Azure, 2022)
- **Phobos. –** Es un malware de tipo ransomware que encripta los datos y bloquea los archivos almacenados hasta que la organización afectada pague por el rescate (PcRisk, 2021).
- **Powershell. –** Es una solución de automatización de tareas multiplataforma formada por Shell de línea de comandos (Microsoft, ¿Qué es PowerShell?, 2022)**.**
- **Microsoft Azure. –** Es una plataforma de Microsoft que provee diferentes servicios en la nube con servidores desplegados a nivel mundial (Microsoft, ¿Qué es Azure?, s.f.)

4. Contexto de la Organización. – Cuando implementemos nuestro BCP, debemos detallar claramente el rubro al cual pertenece la organización, además también es importante especificar las áreas que tiene la organización y sobre todo es importante indicar los servicios que brinda.

5. Liderazgo. – Es importante identificar al equipo de respuesta que se deberá de considerar ante una contingencia no planificada. A continuación, se detalla los posibles equipos a considerar.

- **Equipo de Gestión de Contingencia. –** Es el equipo encargado de aplicar el procedimiento normado de manera correcta para la contingencia; este equipo puede ejecutar actividades en paralelo o en algunos casos puede ser más que suficiente una persona. Por otro lado, es importante señalar que siempre se debe de tener al menos un colaborador de este equipo activo 24x7 o 8x5, esto dependerá del negocio y la criticidad del activo.

- **Líder de Equipo de Gestión de Contingencia. –** Es el responsable de guiar y verificar que el equipo de gestión de contingencia aplique de manera correcta el procedimiento normado. Además, dicho líder también es responsable de coordinar de manera interna con los lideres y/o miembros de otros equipos involucrados. Por otro lado, es importante señalar que siempre se debe contar con un líder de equipo activo 24x7 o 8x5, esto dependerá del negocio y la criticidad del activo.
- **Responsable Jurídico de la Organización. –** Es el responsable de verificar que en la contingencia no planificada, no exista ningún problema de tipo legal, pues en caso exista, éste debe de reportar a las autoridades competentes e inclusive al CEO de la organización en caso sea necesario.
- **Equipo de Respuesta al Incidente. –** Es el equipo encargado de poder restaurar el activo principal afectado en el menor tiempo posible. Por otro lado, es importante señalar que siempre se debe de tener al menos un colaborador de este equipo activo 24x7 o 8x5, esto dependerá del negocio y la criticidad del activo.
- **Equipo Forense. –** Es el equipo encargado de investigar, identificar y recopilar la evidencia del ataque suscitado. Por otro lado, es importante señalar que siempre se debe de tener al menos un colaborador de este equipo activo 24x7 o 8x5, esto dependerá del negocio y la criticidad del activo.

Por otro lado, según CSA es importante que los equipos a ejecutar actividades tengan los permisos que solamente necesitan, es decir, siempre se debe brindar los permisos mínimos en lugar de dar una gama mucho más amplia de permisos.

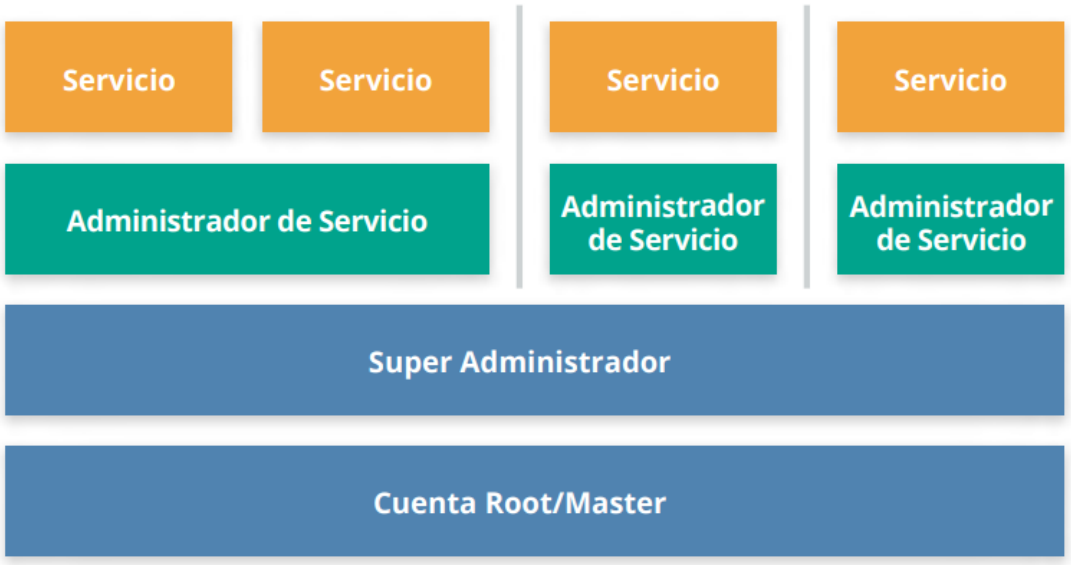

Figura 6 Recomendación de Permisos CSA (Alliance, 2017)

6. Planificación. – Para la planificación se establecerán los mismos objetivos generales y específicos detallados en el punto 4.1 de este documento. Por otro lado, en la siguiente tabla se detalla las amenazas y riesgos que se deberá de tener en cuenta.

N° Item	Tipo Factor	Amenaza	Situación del Riesgo
1	Factor Económico	La empresa que implementó el procedimiento puede tener una disminución económica que le impida mantener los servicios mínimos activos	• La solución del BCP posiblemente no funcione de manera correcta. • Rotación de personal que limite ejecutar las actividades de mantenimiento y de contingencia no planificada.
2	Factor Interno	Los directivos de la organización no se encuentran involucrados en la solución implementada.	• Demora en la aprobación de presupuesto para la implementación y mantenimiento de la solución. • Falta de manejo de la crisis del activo afectado.

3	Factor Humano	Contar con miembros del equipo con conocimientos limitados en la herramienta desplegada.	• La solución de contingencia no puede funcionar de la manera esperada, puesto que el procedimiento no se aplicó de manera correcta.
4	Factor Tecnológico	No aplicar las actualizaciones y mantenimiento de seguridad de la solución implementada.	• Los atacantes pueden explotar las vulnerabilidades y de esa manera baipasear el BCP implementado. • Al ser una solución en nube, los fabricantes de manera constante están actualizando los servicios, en caso no se haga un monitoreo de lo mencionado puede que no funcione el BCP de la forma esperada.

Tabla 1 Amenazas y Riesgos

7. Soporte. – A continuación, se detalla los recursos humanos y tecnológicos que se deberán de considerar para la implementación de la solución BCP en la nube.

- **Recursos Tecnológicos. –** A continuación, se detalla los servicios tecnológicos que debemos de considerar.
  - Internet.
  - Suscripción de Microsoft Azure.
  - Laptop u ordenador.
  - File server.
- **Recursos Humanos. –** Se deben de considerar los equipos que se detallaron el punto 5 en la sección de liderazgo de este documento.

8. Operación. – A continuación, se detalla el impacto que se debe de tener en cuenta para la implementación de la solución del BCP.

- **Análisis del Impacto del Negocio. –** El impacto es un factor importante que se debe de medir en caso de que ocurra una contingencia no completada en nuestro activo crítico al que hemos aplicado nuestra solución de BCP, por ello, lo primero que vamos a desarrollar en esta sección es nuestra evaluación de riesgo de nuestro activo crítico. A continuación, se detalla la tabla de nivel de impacto.

Nivel	Nivel de Impacto
1	Bajo
2	Medio Bajo
3	Moderado
4	Alto
5	Muy Alto

Tabla 2 Nivel de Impacto

A continuación, se detalla el nivel de impacto por categoría.

Categoría	Nivel de Impacto				
	1	2	3	4	5
Interrupción del servicio	El servicio funciona de manera correcta	El servicio se interrumpe hasta en un 20%	El servicio se interrumpe hasta en un 40%	El servicio se interrumpe hasta en un 60%	El servicio se interrumpe más de un 60%
Seguridad o Ciberseguridad	El incidente de ciberseguridad lo conoce solamente el área de TI y podría causar una interrupción del servicio.	El incidente de ciberseguridad lo conoce solamente el área de TI y ha comenzado a causar una interrupción en el servicio.	El incidente de ciberseguridad lo conoce toda la organización y se ha interrumpido el servicio hasta el 50% de la organización.	El incidente de ciberseguridad lo conoce toda la organización y se ha interrumpido el servicio en su totalidad para toda la organización.	El incidente de ciberseguridad se conoce públicamente y se ha interrumpido en su total para toda la organización.

Tabla 3 Nivel de Impacto por Categoría

A continuación, se muestra los niveles de probabilidad.

Probabilidad	Nivel	Frecuencia
Improbable	1	Se puede presentar una vez al año, pero no todos los años
Raro	2	Se puede presentar una vez al año.
Moderado	3	Se puede presentar entre 2 y 4 veces al año.
Probable	4	Se puede presentar de al menos una vez de manera trimestral
Muy Probable	5	Se puede presentar más de una vez cada dos meses.

Tabla 4 Nivel de Probabilidad

A continuación, se muestra la forma que permite medir el nivel del riesgo.

Nivel del Riesgo = Nivel de Impacto x Probabilidad

En función a la realidad de cada organización se deberá de identificar sus riesgos y deberá aplicar la formula antes propuesta para poder obtener el nivel del riesgo. Además, en función al resultado deberán de implementar las acciones más convenientes para cada riesgo.

- **Estrategias de Continuidad de Negocio. –** A continuación, se detalla algunas estrategias que se deberá a considerar.
    - Contar con una guía o procedimiento detallado donde se explique la forma de implementar la solución de BCP que tiene por tenor el título de este documento.
    - Monitoreo constante del funcionamiento la solución BCP implementada.
    - Pruebas cada cierto periodo del funcionamiento de la solución BCP implementada.

- Según el nivel de criticidad del activo, implementar redundancia de zona geográfica de los datos sincronizados en la nube.
- Contar siempre con colaboradores capacitados en las tecnologías que utiliza la solución BCP implementada.

- **Procedimiento para la Continuidad de Negocio. –** A continuación, se detalla algunos procedimientos a tomar en cuenta durante una contingencia no planificada.
  - Una vez identificado el incidente, se deberá de informar a través de los canales oficinales (intranet, correo, etc.) a toda la organización del incidente suscitado.
  - Determinar el impacto que provoca la interrupción.
  - El equipo deberá aplicar el procedimiento de contingencia detallado en este documento.
  - Dar a conocer de manera precisa a la alta dirección las medidas que se están tomando de forma inmediata para resolver la interrupción.
  - Aplicar pruebas de integridad de datos, que permita validar si la información es la correcta según el RPO aplicado.

9. Evaluación de Desempeño. – La evaluación de desempeño se debe de realizar de manera periódica, esto debe de ser defino por la organización según la criticidad del activo. A continuación, se brinda algunas recomendaciones que se deberán de ejecutar en dichas revisiones para mejorar el rendimiento de la solución.

- Ejecución de auditorías periódicas para validar la implementación de la norma 22301:2019.
- Validación de la consistencia a la información sincronizada en la nube.
- Revisión y aplicación (en caso sea necesario) de las nuevas características que implementa el fabricante a nivel de los servicios en la nube que estamos utilizando.

10. Mejoras. – La mejora continua es una estrategia que se debe de implementar de manera constante en cualquier solución tecnológica que una organización implementa. Según la ISO 22301:2019 la cual está basada el presente trabajo de investigación, también indica que se debe de identificar de manera constante que actividades y procesos se deberán de mejorar, la identificación de las mejoras se deberá de ejecutar según la

criticidad del activo. A continuación, se detalla algunas recomendaciones de mejoras que se deberá de validar.

- Capacitación periódica a los colaboradores según el nivel de rotación del personal.
- Monitoreo constante de la solución implementada.
- Pruebas trimestrales o según el nivel de criticidad del activo de la solución BCP que se encuentra en marcha, esto con el fin de que funcione de manera correcta al momento que se requiera.
- Revisar de manera constante el procedimiento y/o guía para identificar mejoras o retirar procedimientos ya no soportados.

4.3 Planificación

A continuación, se detalla las actividades ejecutadas para llevar al éxito del proyecto de investigación.

Nombre de tarea	Duración
Cronograma de Plan de Continuidad de Negocio de un file server ante un ataque de malware en Cloud	**109 días**
Análisis del Planteamiento del TFM	**37 días**
Revisión de la Literatura	10 días
Justificación de las normas	6 días
Definición de la realidad actual de los procedimientos de las organizaciones	20 días
Reunión con el tutor	1 día
Descripción del Problema	**29 días**
Planteamiento de los Objetivos Generales	8 días
Planteamiento de los Objetivos Específicos	4 días
Logros a alcanzar	4 días
Metodología	8 días
Planificación	4 días
Reunión con el tutor	1 día
Pruebas y Validación	**17 días**
Pruebas	8 días
Resultados	8 días
Reunión con el tutor	1 día
Conclusiones y Bibliografía	**17 días**
Conclusiones	8 días
Bibliografía	8 días
Reunión con el tutor	1 día
Preparación Sustentación	**9 días**
Elaboración de material para sustentación de TFM	8 días
Sustentación de TFM	1 día

4.4 Implementación

En esta sección se desarrollará la guía que permitirá implementar con una estrategia de contingencia de un file server hacia la nube de Microsoft Azure. Para comenzar la fase de implementación, se asume que la organización cuenta con un colaborador especialista en las

tecnologías a implementar, además cuenta con una suscripción en la nube publica de Microsoft Azure, recordemos que dicha nube la puedes contratar de diferentes maneras, en la siguiente url (Microsoft, Oferta de Microsoft Azure, s.f.) podrás encontrar las modalidades de adquisición. El primer paso es iniciar sesión en el portal de Microsoft Azure en la siguiente url: https://portal.azure.com/.

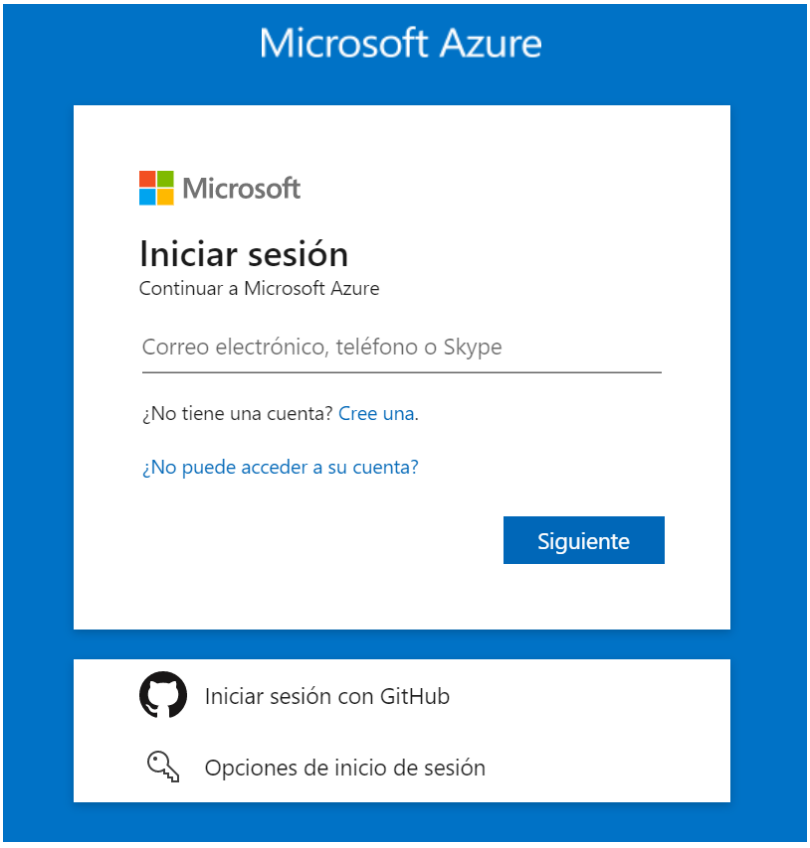

Figura 7 Inicio de Sesión en el portal de Microsoft Azure

Por otro lado, debemos de tener en consideración los permisos que debemos de tener en cuenta para la implementación de la solución, por ende, se señala que con los permisos de "colaborador" serían más que suficiente para implementar la funcionalidad en mención. En caso se requiera conocer cuáles son los tipos de permisos que se pueden manejar en Microsoft Azure, les dejo a continuación la siguiente url (Microsoft, Roles integrados de Azure, 2022).

4.4.1 Arquitectura de Servicios en Microsoft Azure

A continuación, se muestra de manera gráfica todos los servicios que se deberán de habilitar en Microsoft Azure.

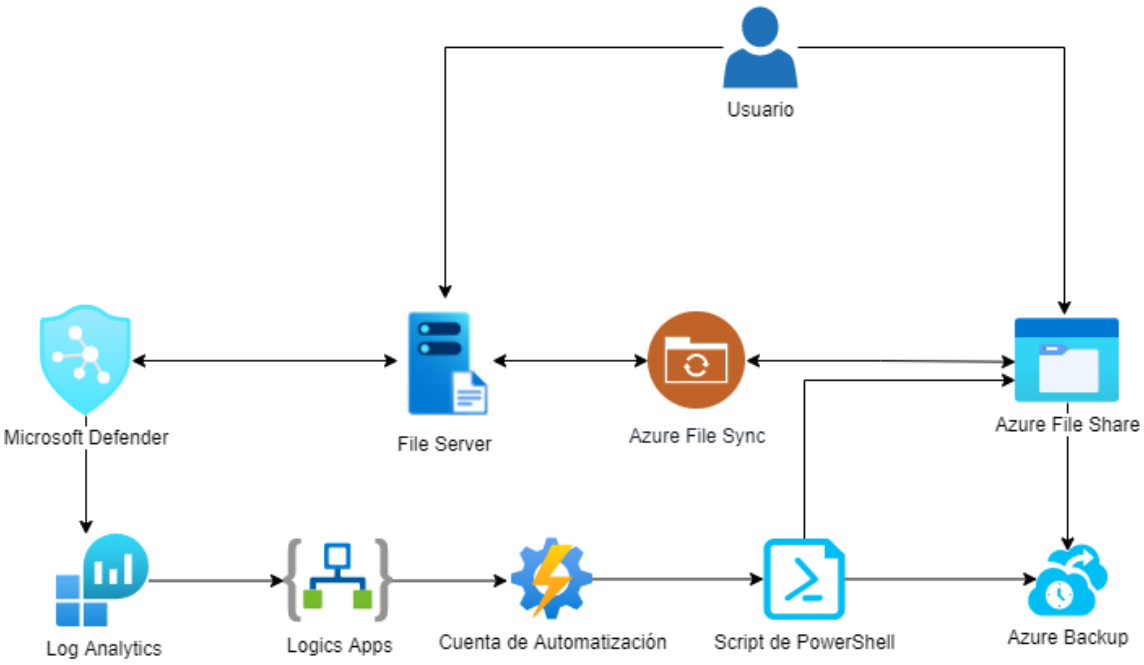

Figura 8 Arquitectura de Servicios en el portal de Microsoft Azure

4.4.2 Habilitación de Servicios

A continuación, se detalla los servicios que se deben de habilitar en Microsoft Azure.

4.4.2.1 Creación del Servicio de Microsoft Defender for Cloud

Hay varias formas de encontrar el servicio de Microsoft Defender for Cloud, pero la manera más fácil es colocando el nombre en el buscador que trae consigo el portal de Microsoft Azure, en la siguiente imagen se puede apreciar cómo se visualiza al momento de buscar el nombre.

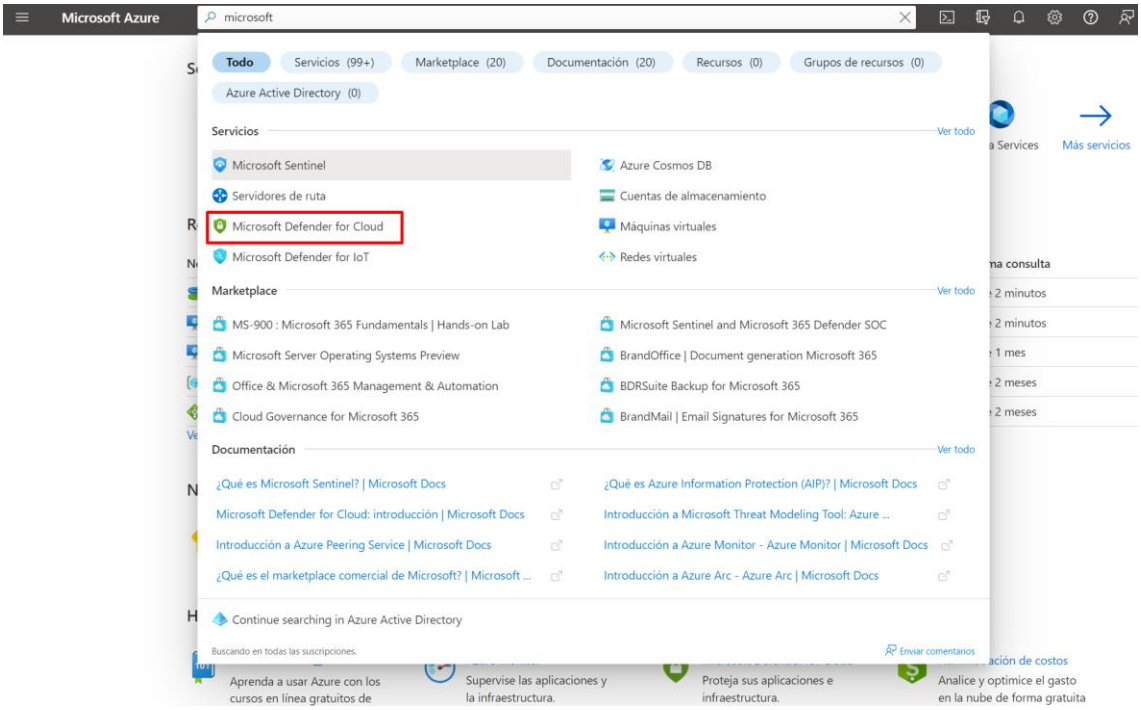

Figura 9 Buscar Microsoft Defender for Cloud en el portal de Microsoft Azure

El sigue paso que nosotros debemos de ejecutar es el de habilitar todas las funcionalidades que trae consigo el servicio, por ello, nosotros debemos de dar clic en el botón actualizar que se muestra en la parte inferior de la imagen a continuación. Es muy importante señalar que, al momento de ejecutar dicho servicio, Microsoft Azure iniciará a empezar a facturar por los servicios que protege, por lo tanto, si queremos tener mayor referencia de los costos que se pueden incurrir, sugiero revisar los costos de manera previa (Microsoft, Costos de Microsoft Defender for Cloud, 2022).

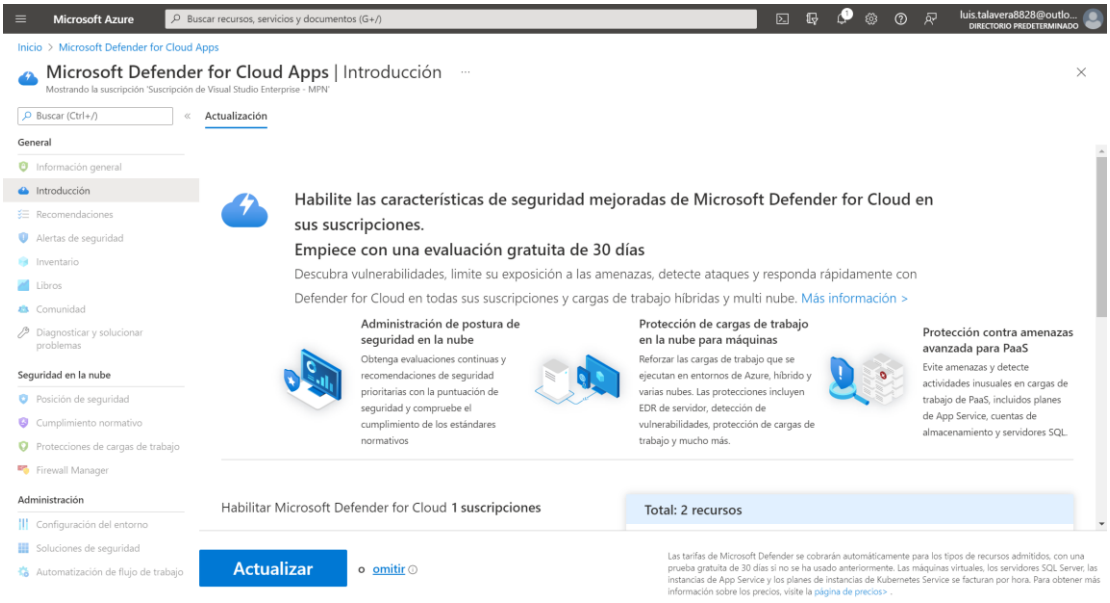

Figura 10 Microsoft Defender for Cloud en el portal de Microsoft Azure

4.4.2.2 Creación del Servicio de Azure Files

El servicio de Azure files, nos permitirá almacenar la información (carpetas y archivos) del disco de nuestro servidor file server. Además, también es importante señalar que al momento de crear el servicio podemos escoger el tipo de redundancia que tendrá nuestro servicio, esto va a depender de los controles y criticidad que tiene el servidor file server de la organización, recordemos que esto varía según la organización, es importante señalar que dicha configuración tendrá un efecto a nivel de costos al momento de efectuar los pagos respectivos, a continuación se deja la referencia de los costos en el que se incurrirá al momento de crear el servicio (Microsoft, Costos de Azure FIles, 2022).

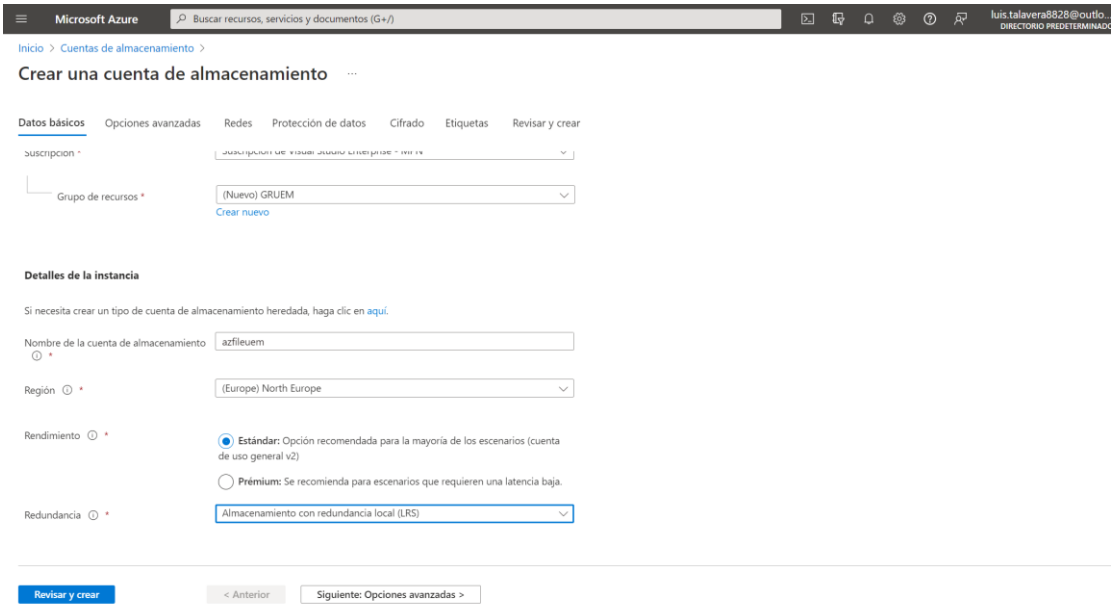

Figura 11 Creación del servicio de la cuenta de almacenamiento en Microsoft Azure

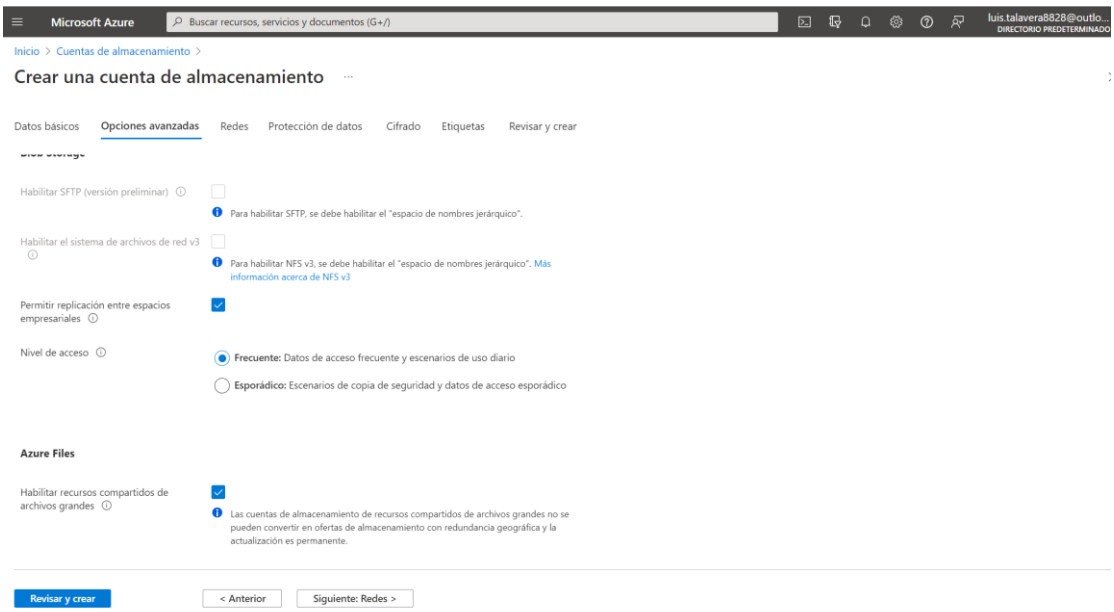

Figura 12 Creación del Azure File en la cuenta de almacenamiento en Microsoft Azure

4.4.2.3 Creación del Servicio de Azure File Sync

Este servicio nos va a permitir sincronizar la información almacenada (carpetas y archivos) en el disco de nuestro file server hacia el servicio de Azure File, además es importante señalar que la información se sincronizada de manera inmediata, también es importante señalar que dicha sincronización depende del ancho de banda que pueda tener cada organización; por lo

que se recomienda ejecutar pruebas de sincronización antes de poner en producción la solución.

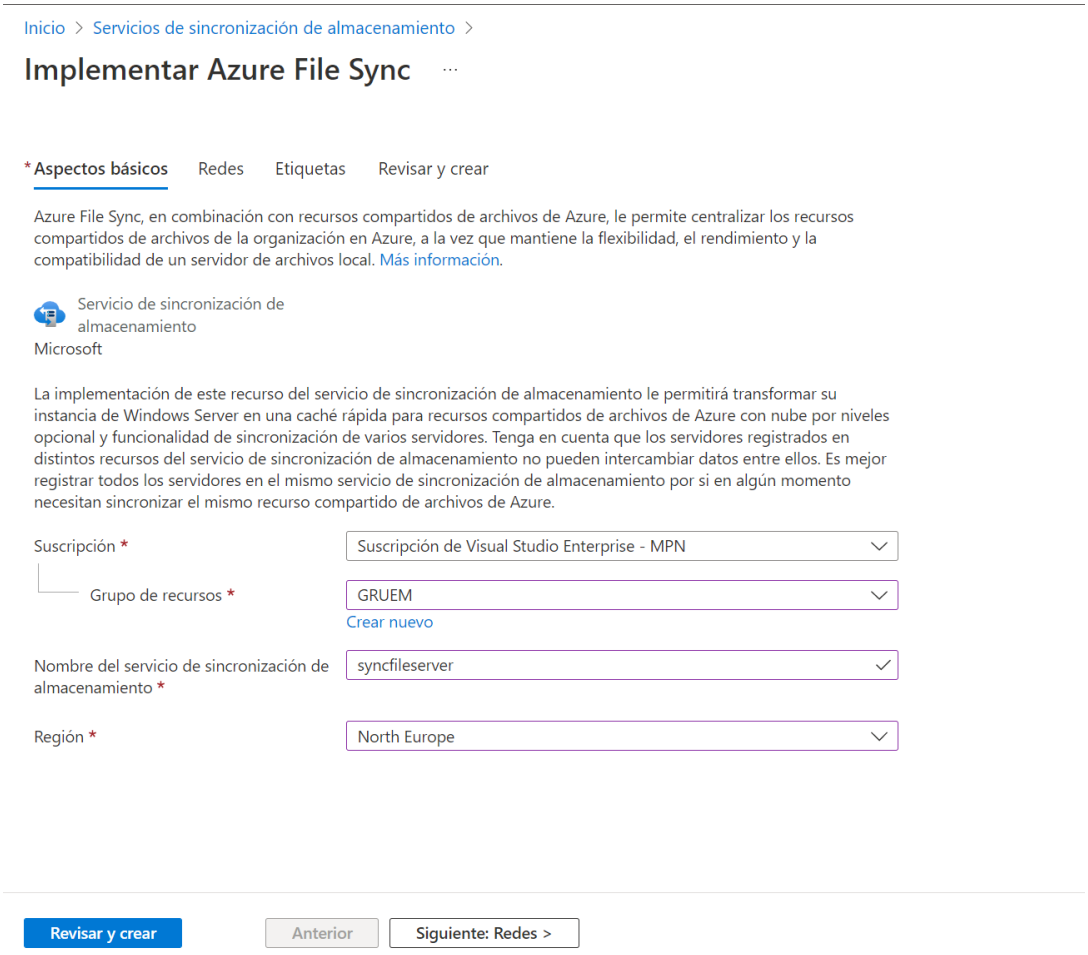

Figura 13 Creación del servicio de Azure File Sync en Microsoft Azure

4.4.2.4 Creación del Servicio de Cuenta de Automatización

El servicio de Cuenta de Automatización es un servicio que permite ejecutar procesos en backend de script que se puedan programar o personalizar, en nuestro caso es un servicio que nos va a permitir ejecutar un script en powershell, el cual al momento de ejecutarse permitirá generar un Backup o snapshot de toda la 38información almacenada en nuestro servicio de Azure File, a continuación se deja la referencia de los costos en el que se incurrirá al momento de crear el servicio (Microsoft, Costos de Azure Automatización, 2022).

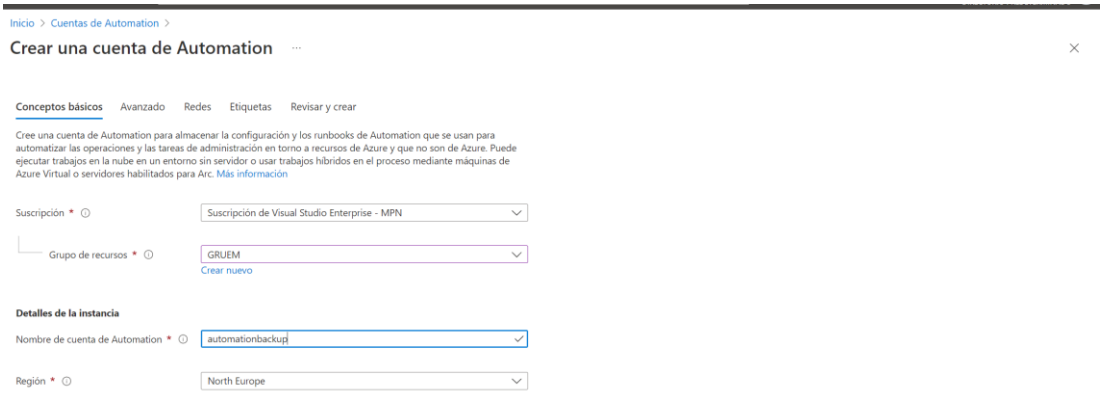

Figura 14 Creación del servicio de Azure Automatización en Microsoft Azure

4.4.2.5 Creación del Servicio de Azure Backup

El servicio de Azure Backup nos va a permitir almacenar los snapshot o instantáneas de la información almacenada en el Azure File, a continuación, se deja la referencia de los costos en el que se incurrirá al momento de crear el servicio (Microsoft, Costos de Azure Backup, 2022).

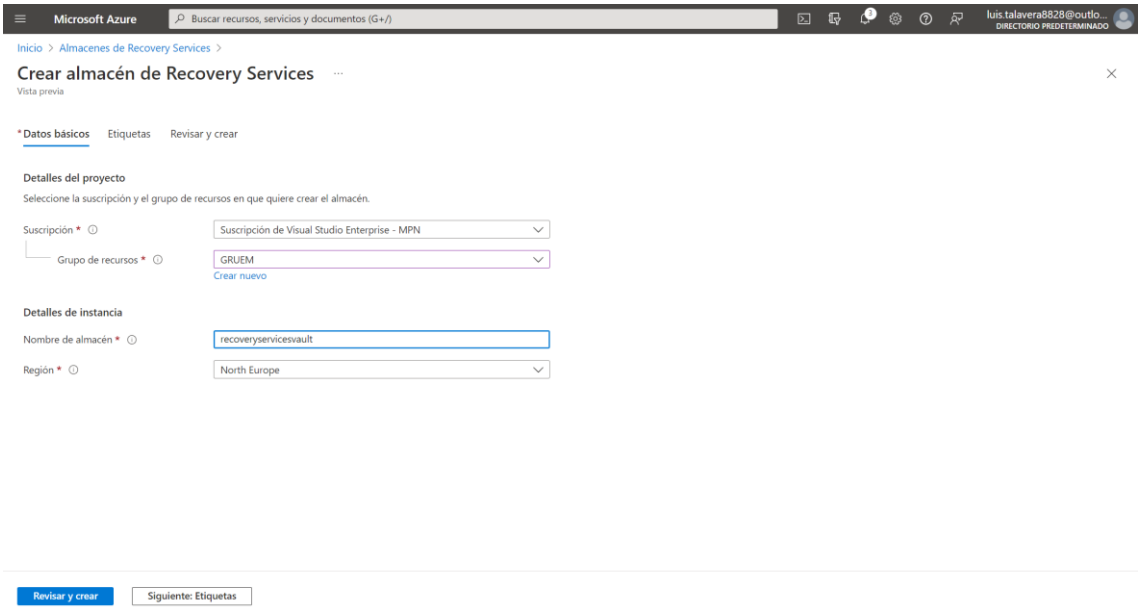

Figura 15 Creación del servicio de Azure Backup en Microsoft Azure

4.4.2.6 Creación del Servicio de Log Analytics

Este servicio nos permitirá recopilar y almacenar toda la información de nuestra máquina virtual file server, se deja la referencia de los costos en el que se incurrirá al momento de crear el servicio (Microsoft, Costos de Log Analytics, 2022).

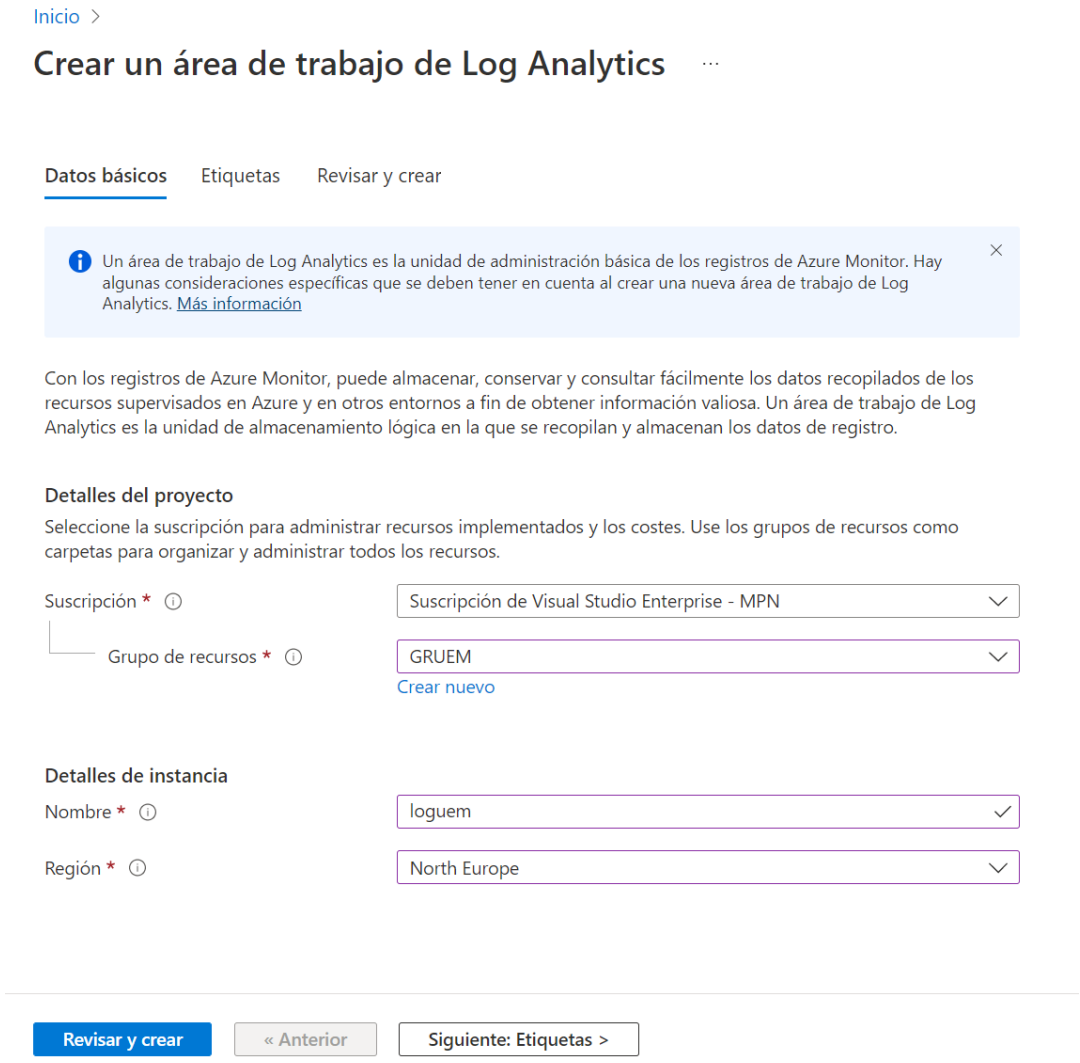

Figura 16 Creación del servicio de Log Analytics en Microsoft Azure

4.4.2.7 Creación del Servicio de Máquina Virtual

La máquina virtual alojada en Microsoft Azure permitirá alojar toda la información almacenada por los colaboradores de una determinada organización, esta será alojada en un disco virtual que estará asociado a la máquina virtual. A continuación, se deja la referencia de los costos en el que se incurrirá al momento de crear el servicio.

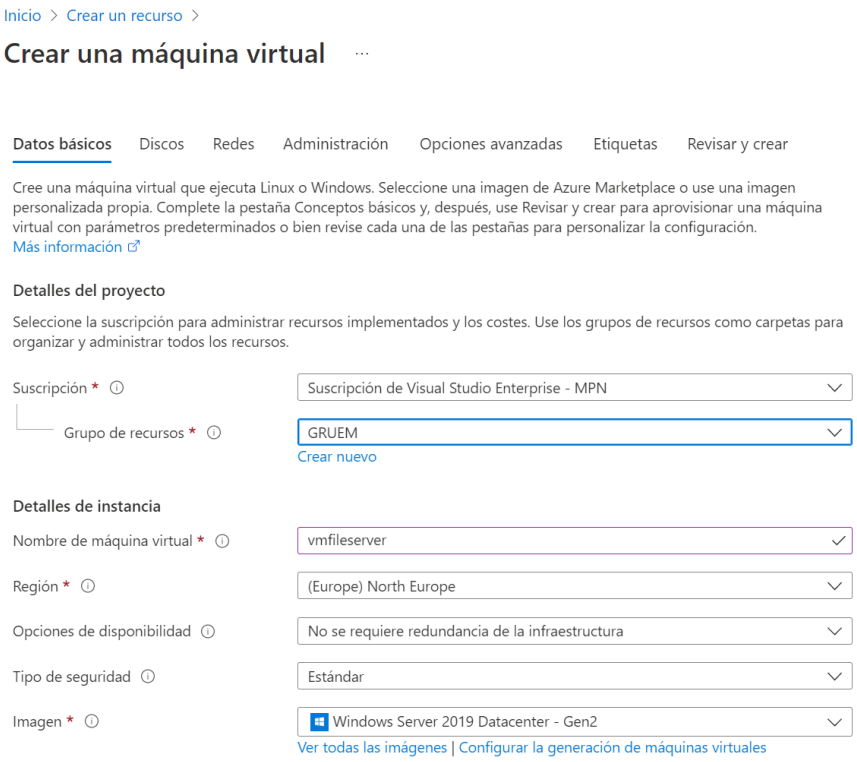

Figura 17 Creación del servicio de Máquina Virtual en Microsoft Azure

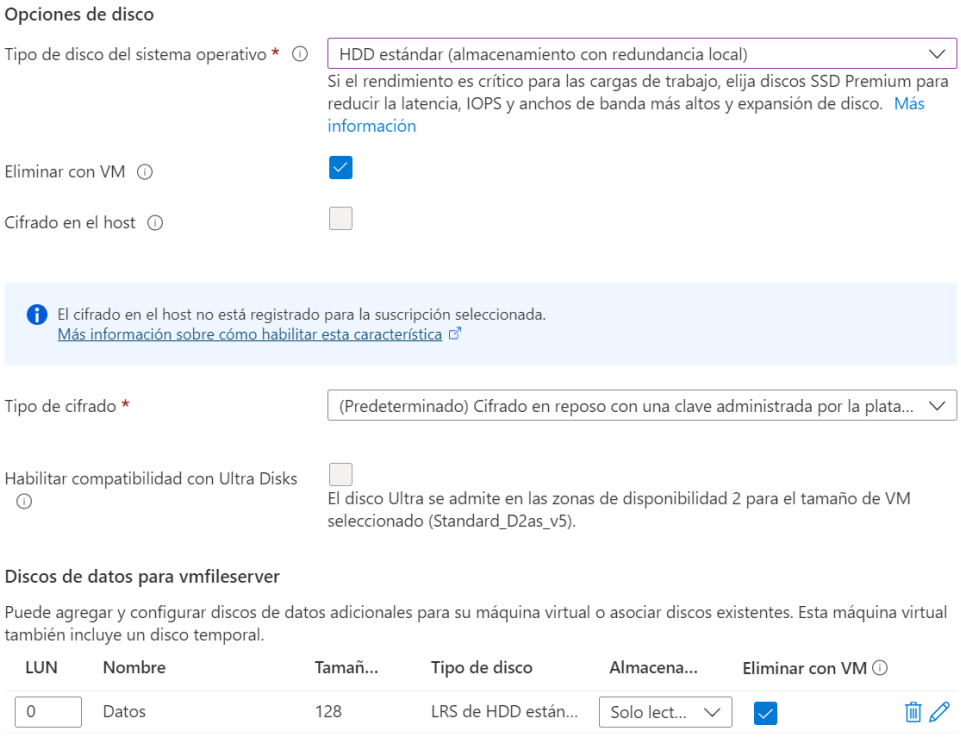

Figura 18 Asociación de un disco de Datos a la Máquina Virtual en Microsoft Azure

4.4.2.8 Creación del Servicio de Logic App

El servicio de Logic App nos va a permitir ejecutar un flujo de actividades en el cual integraremos el servicio de Microsoft Defender con el servicio de Azure Backup, mediante el servicio de Cuenta de Automatización, a continuación, se deja la referencia de los costos en el que se incurrirá al momento de crear el servicio (Microsoft, Costos de Log Analytics, 2022).

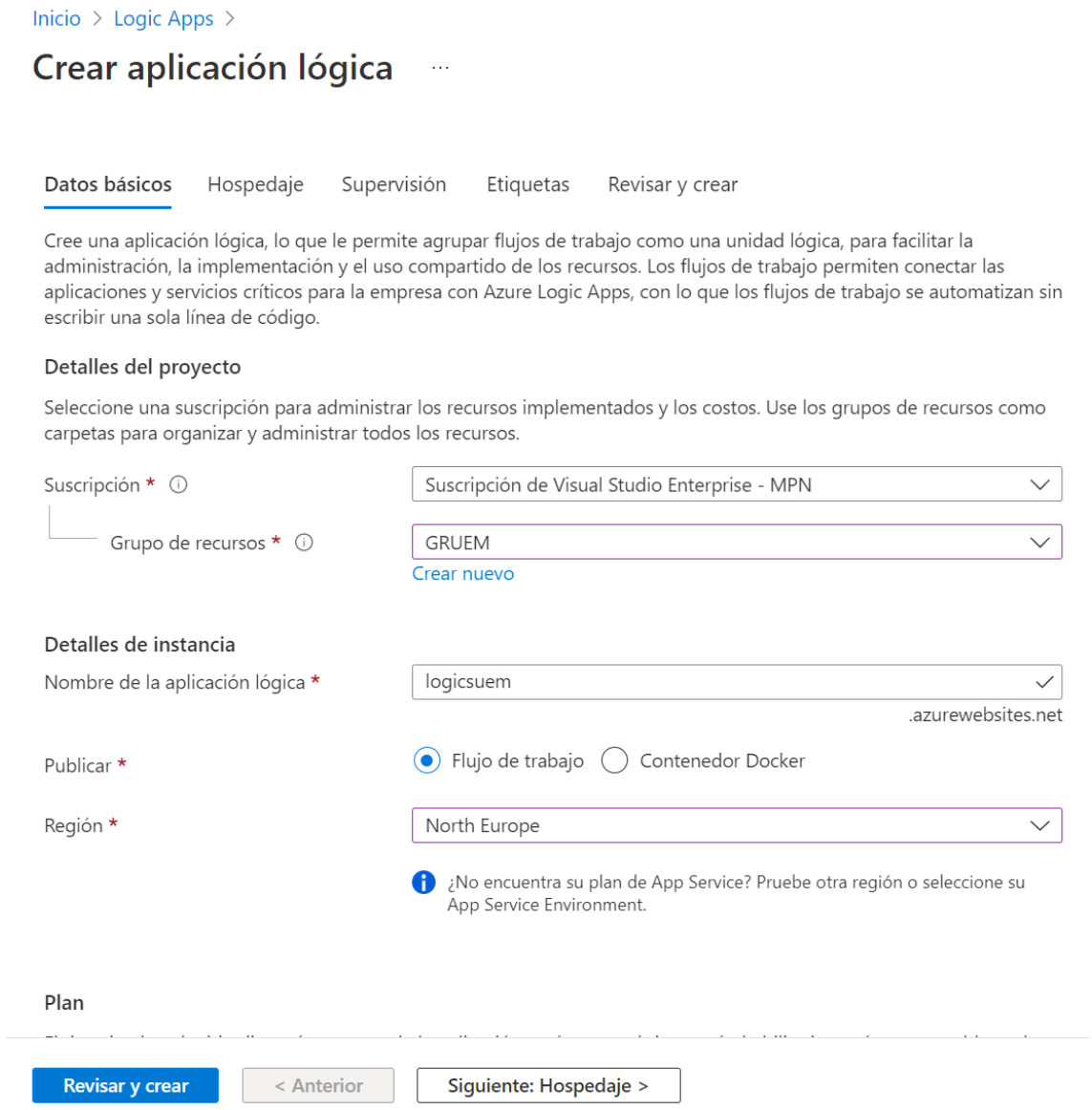

Figura 19 Creación del servicio de Logic App en Microsoft Azure

4.4.3 Configuración de los Servicios

4.4.3.1 Creación Azure File Share

El almacenamiento de tipo de file share nos va a permitir alojar todas las carpetas y archivos que serán sincronizados con el servidor de file server, en este punto es importante escoger el nivel de performance que tendrá el file share, puesto según su elección mayor o menor rapidez al momento de consultar los datos.

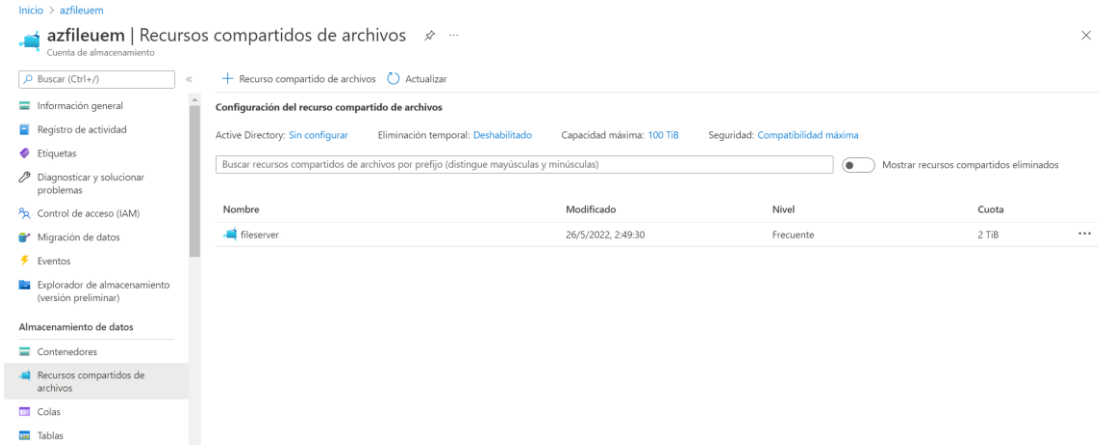

Figura 20 Creación de Azure File Share en Almacenamiento en Microsoft Azure

4.4.3.2 Configuraciones en Azure File Sync

A continuación, se detalla las configuraciones implementadas en el servicio de Azure File Sync.

- **Instalación de Agente de Azure File Sync. –** Para que el servicio de sincronización de almacenamiento detecte la información almacenada se debe de instalar un agente en la máquina virtual donde se encuentra alojada la información de la organización, para este caso nuestro servidor de file server. El agente se puede descargar de la siguiente url https://www.microsoft.com/en-us/download/details.aspx?id=57159; es importante señalar, que la instalación no tiene mayor complejidad para completarla.

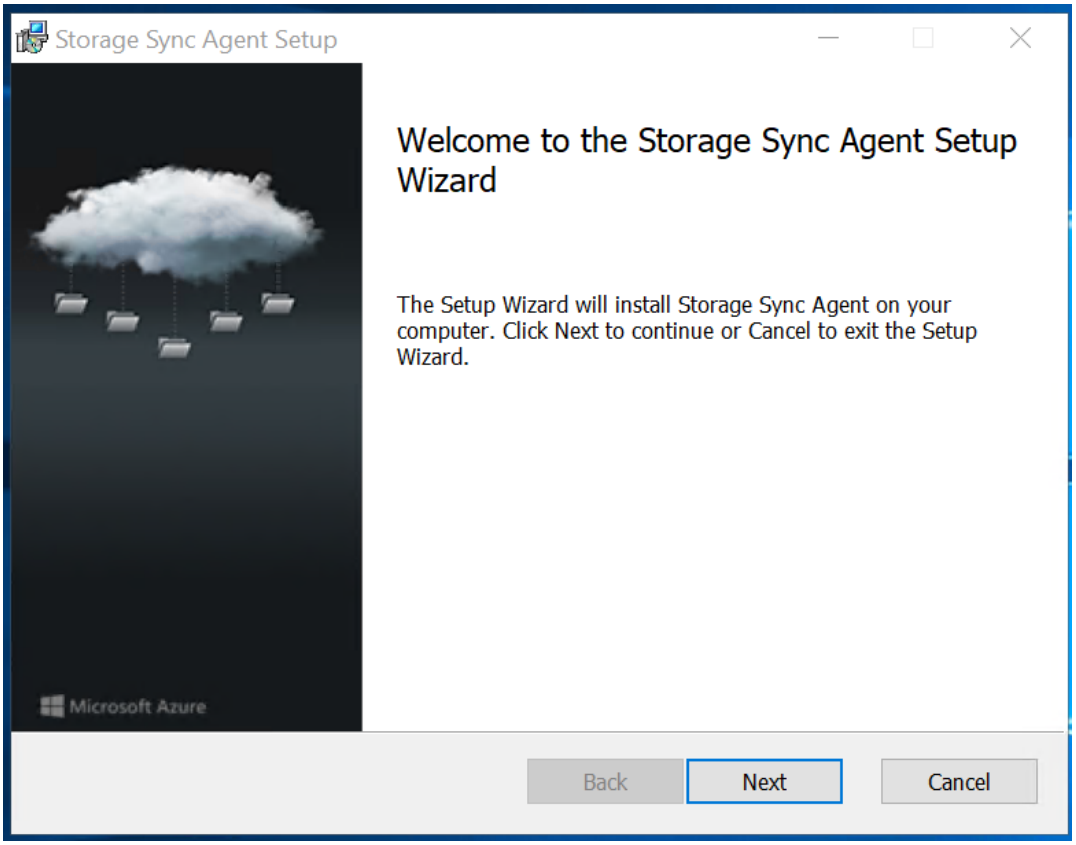

Figura 21 Proceso de instalación del agente en la máquina virtual de file server

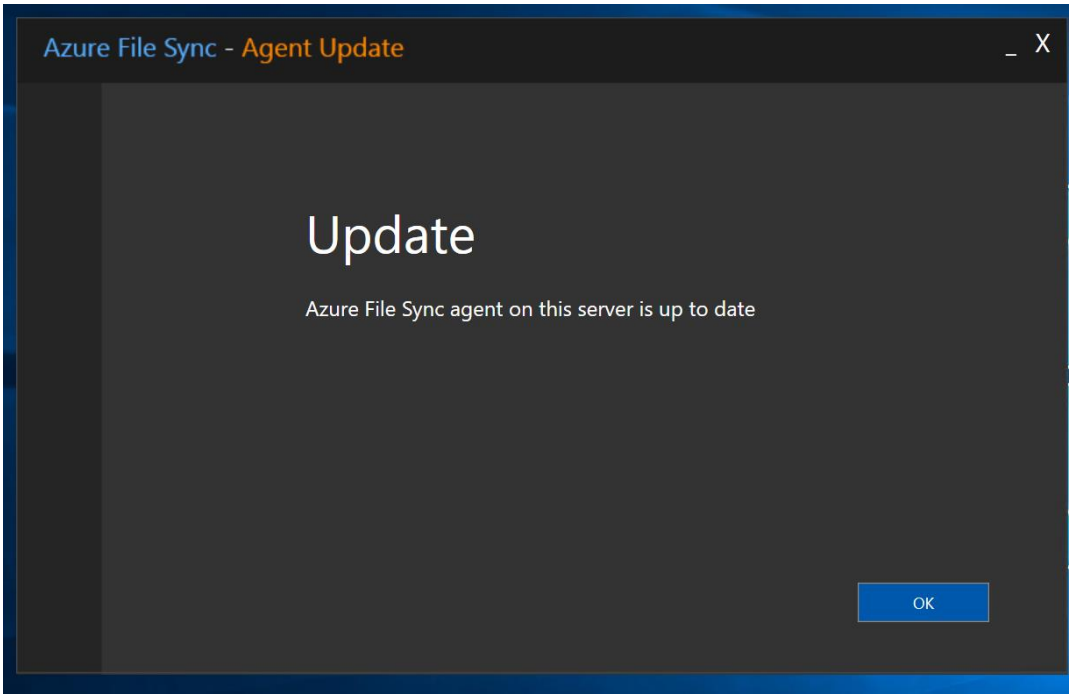

Figura 22 Finalización de la instalación del agente en la máquina virtual de file server

Una vez instalado el agente en nuestra máquina de file server, el siguiente paso que debemos de ejecutar es el de ingresar nuestras credenciales de acceso al portal de Microsoft Azure, de esa manera podremos asociar nuestra máquina virtual con nuestro servicio de sincronización de almacenamiento.

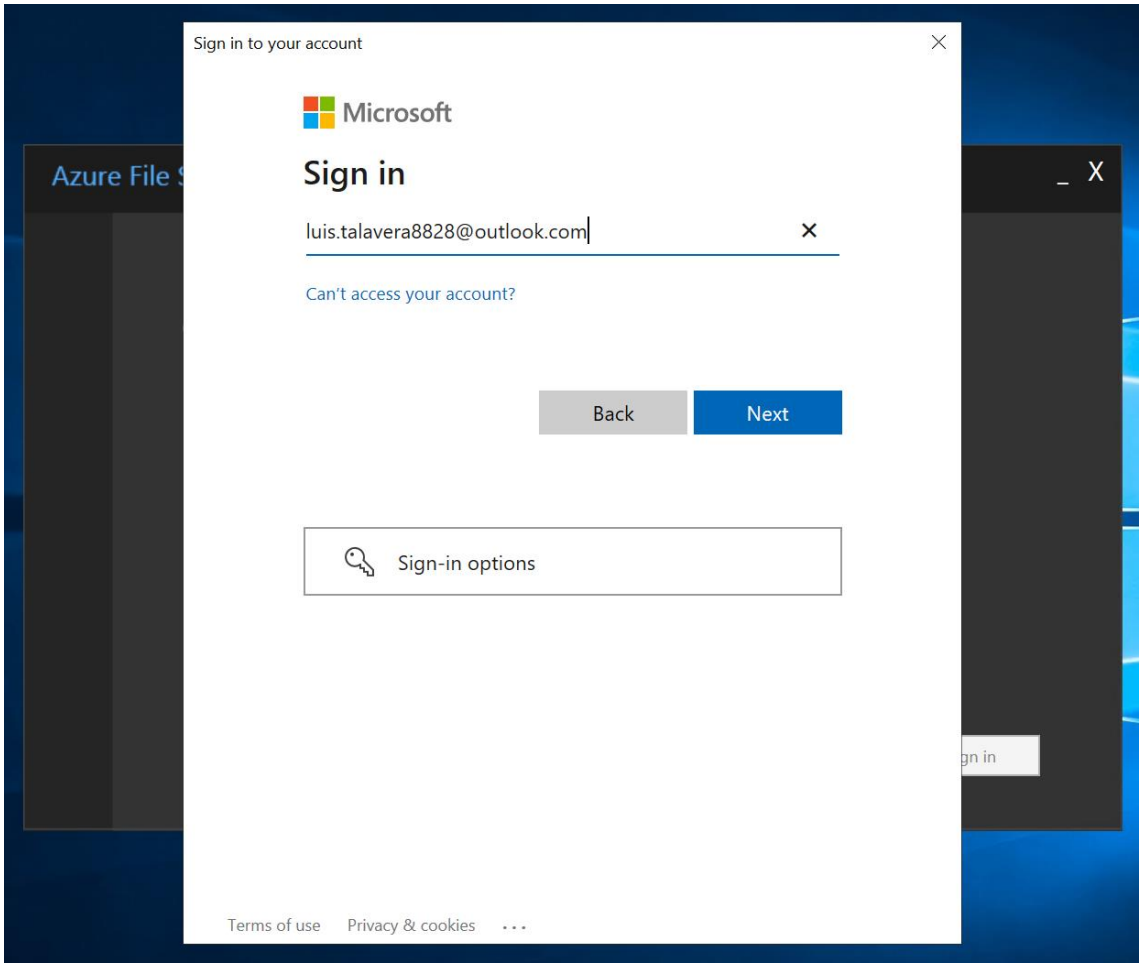

Figura 23 Ingreso de credenciales en agente de Azure File Sync

Después de a ver ingresado nuestras credenciales, el siguiente paso que debemos de ejecutar, es el de seleccionar nuestra suscripción, grupo de recursos y el storage sync services que se creo de manera previa.

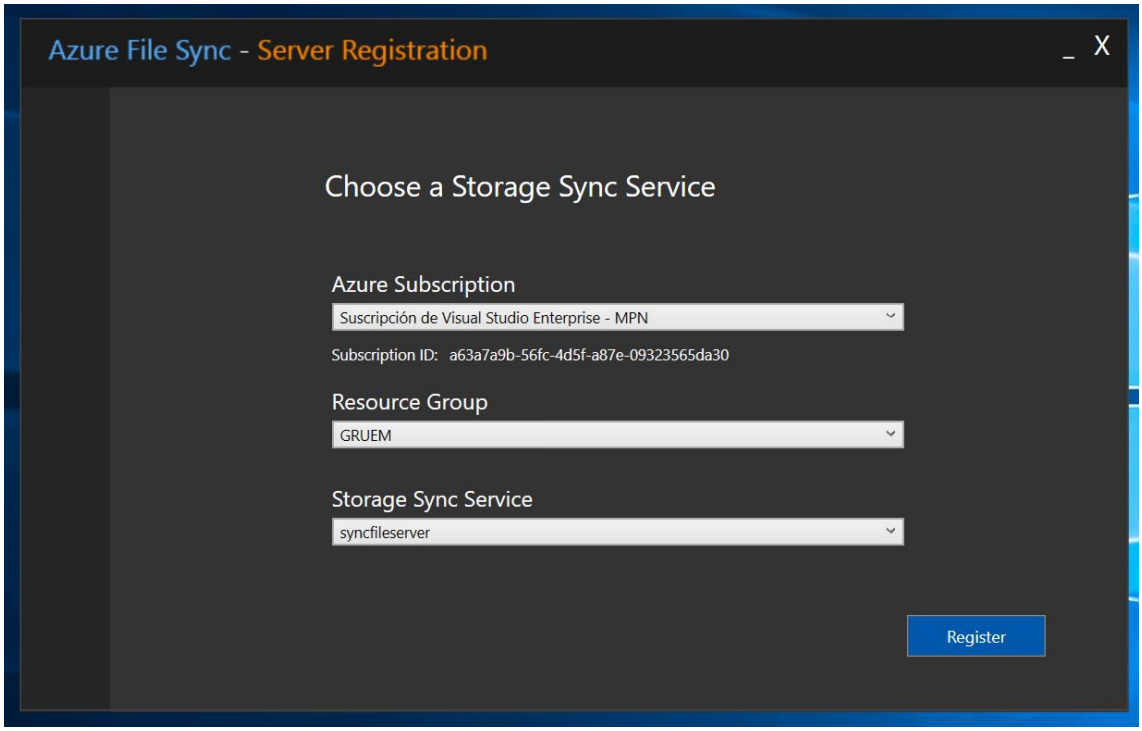

Figura 24 Ingreso de credenciales en agente de Azure File Sync

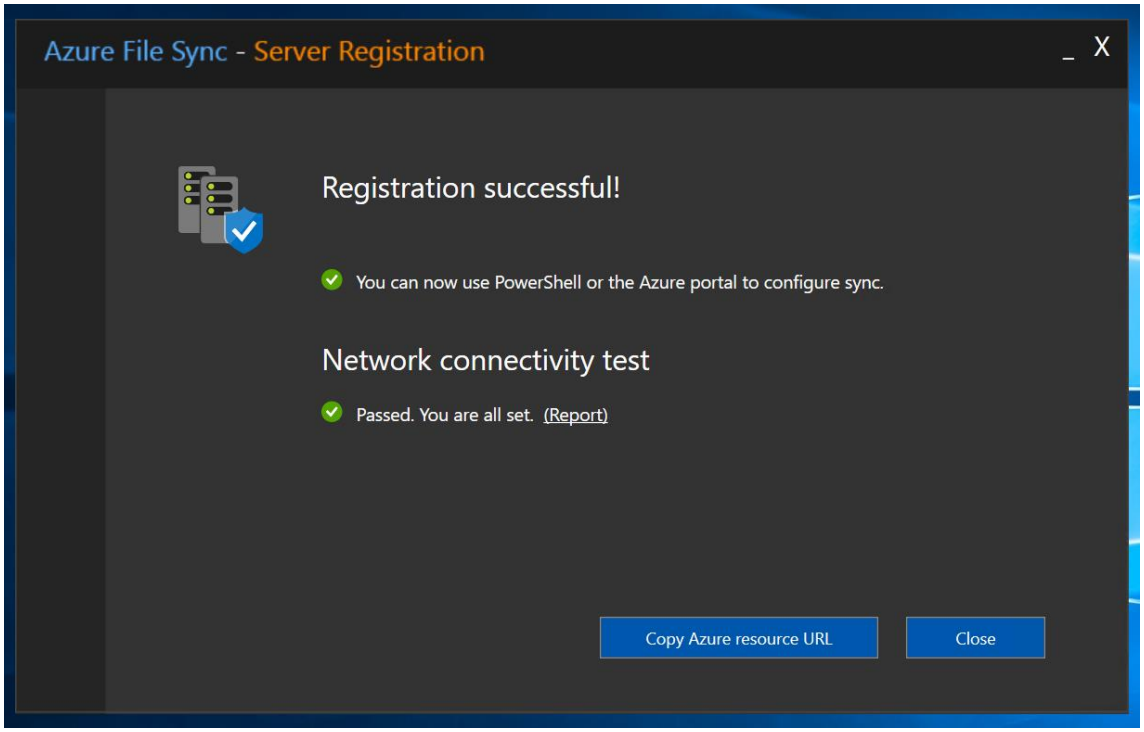

Figura 25 Visualización del registro del agente instalado en servidor file server.

- **Creación del grupo de sincronización. –** Dentro del servicio de Azure File Sync, debemos de crear un grupo de sincronización el cual va a permitir asociar y sincronizar de manera constante la información del disco de la máquina virtual con el recurso compartido de archivos de azure file.

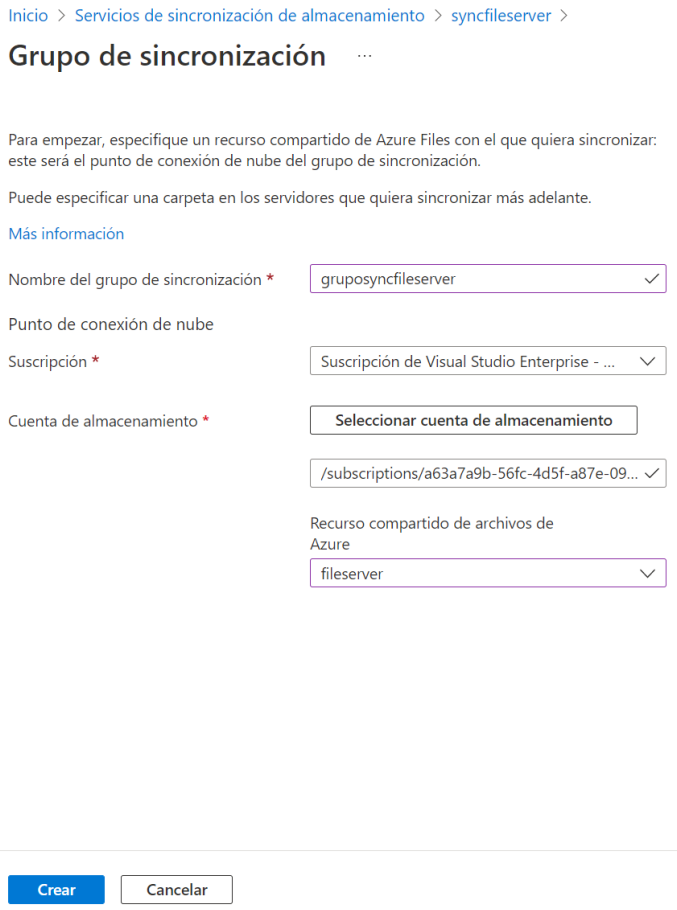

Figura 26 Creación del Grupo de Sincronización en Azure File Sync de Microsoft Azure

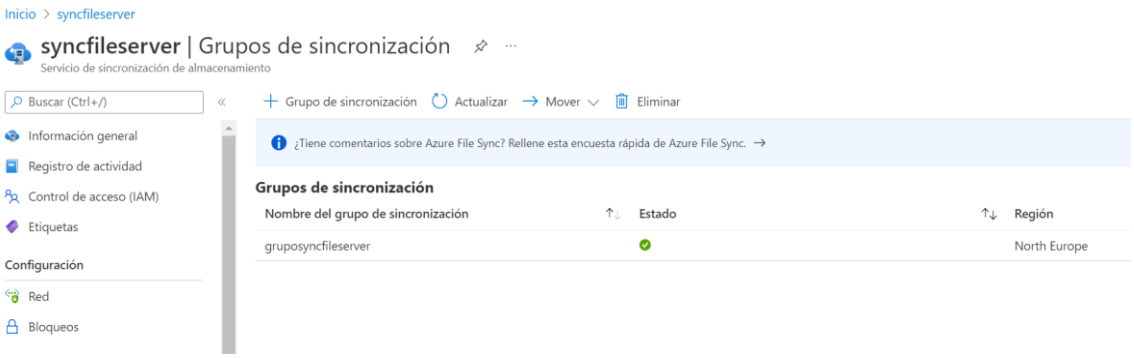

Figura 27 Visualización del Grupo de Sincronización creado en Azure File Sync de Microsoft Azure

- **Configuración del grupo de sincronización. –** Ahora que ya tenemos creado el grupo de sincronización, lo que debemos de configurar, es asociar nuestro servidor colocando también la ruta donde se encuentran almacenados nuestros archivos; en caso deseen explorar con mayor detalle la configuración avanzada que tiene dicha configuración la pueden encontrar en la siguiente url (Microsoft, Configuración de Sincronización Grupo de Sincronización, 2022).

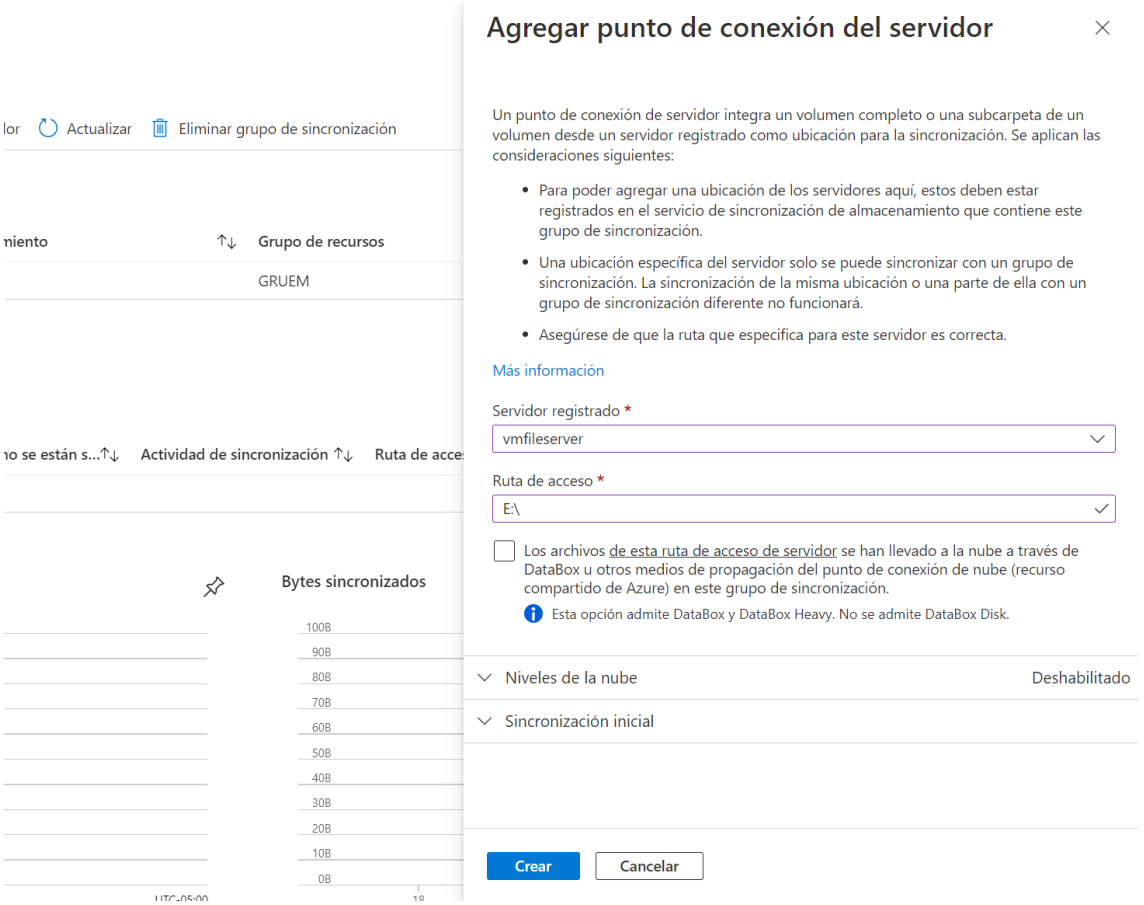

Figura 28 Configuración de Grupo de Sincronización en Azure File Sync de Microsoft Azure

Como se puede visualizar en la figura 26, la información se encuentra sincronizando y el tiempo de sincronización inicial va a depender de la cantidad de información y del ancho de banda que cuente la organización. Es importante señalar, que la sincronización se hace de manera automática según la detección de agregar, editar o eliminar que encuentre la herramienta en la ruta configurada.

Una vez terminada la sincronización, vamos a poder visualizar la información sincronizada.

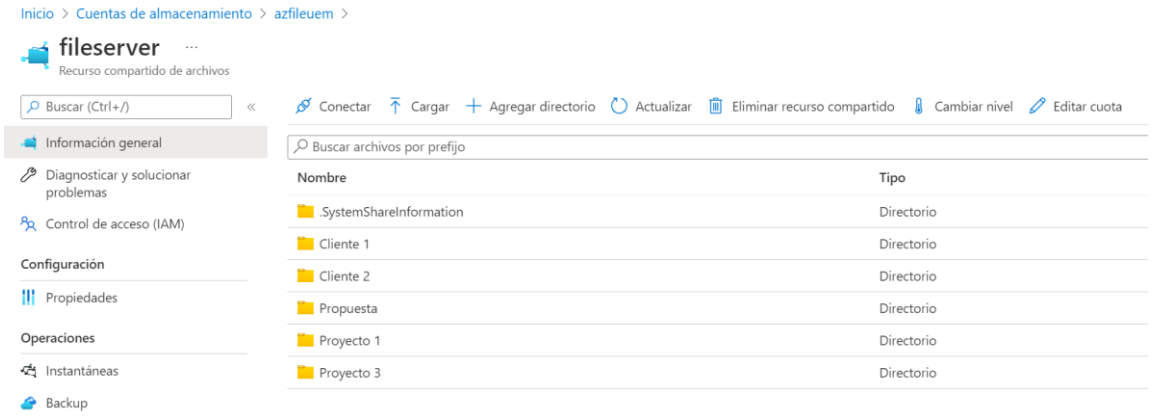

Figura 29 Visualización de información sincronizada en File Share

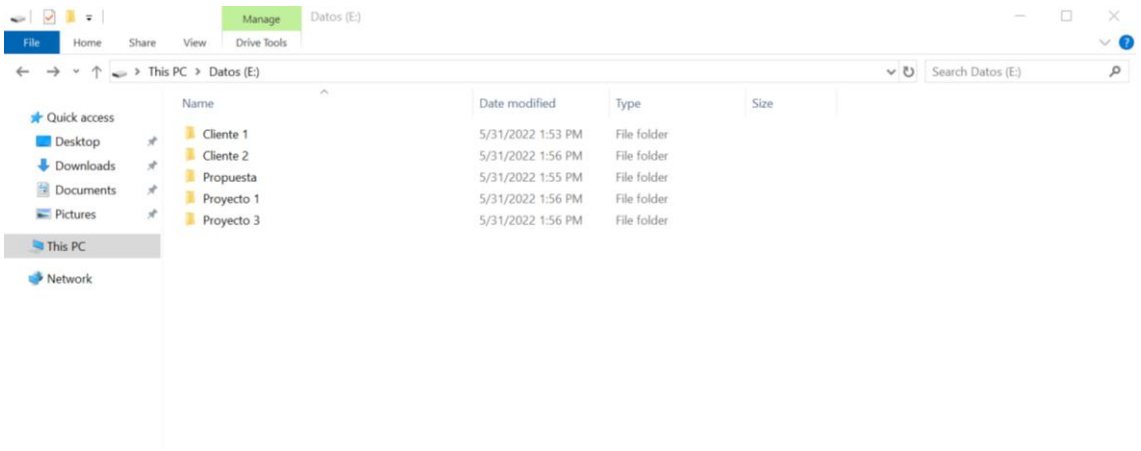

Figura 30 Visualización de información en servidor de File server

4.4.3.3 Configuración en servicio de Azure Backup

A continuación, se detalla las configuraciones implementadas en el servicio de Azure Backup.

- **Configurar Azure Backup con cuenta de almacenamiento. –** El siguiente paso que demos de ejecutar, es el de configurar una política de Backup para el servicio de Azure File de la cuenta de almacenamiento creado y configurado previamente, es importante señalar que cada empresa puede configurar diferentes políticas retención, que serán en función a sus necesidades y procedimientos.

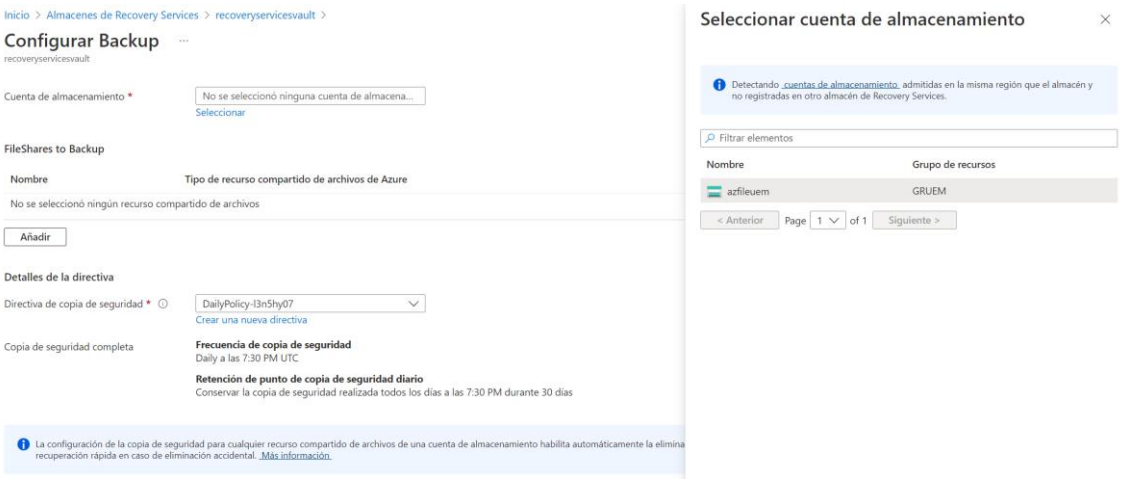

Figura 31 Configuración de Azure Backup con la cuenta de almacenamiento

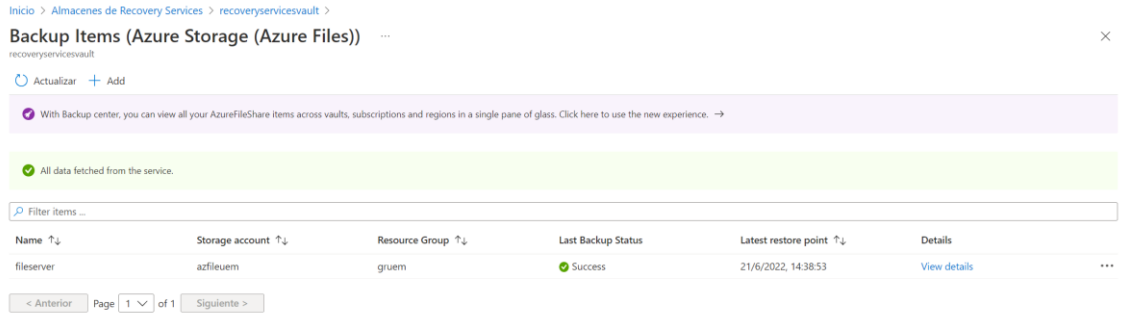

Figura 32 Configuración de Azure Backup con la cuenta de almacenamiento

4.4.3.4 Configuración en servicio de Cuenta de Automatización

A continuación, se detalla las configuraciones implementadas en el servicio de cuenta de automatización.

- **Creación de una cuenta de ejecución. –** La cuenta de ejecución nos permitirá ejecutar las tareas programadas que configuraremos en los próximos pasos, por ende, se debe de habilitar una y colocar una fecha de caducidad, es importante tener una fecha próxima y renovarla de manera constante, ya sea trimestral o anualmente, según política de la organización.

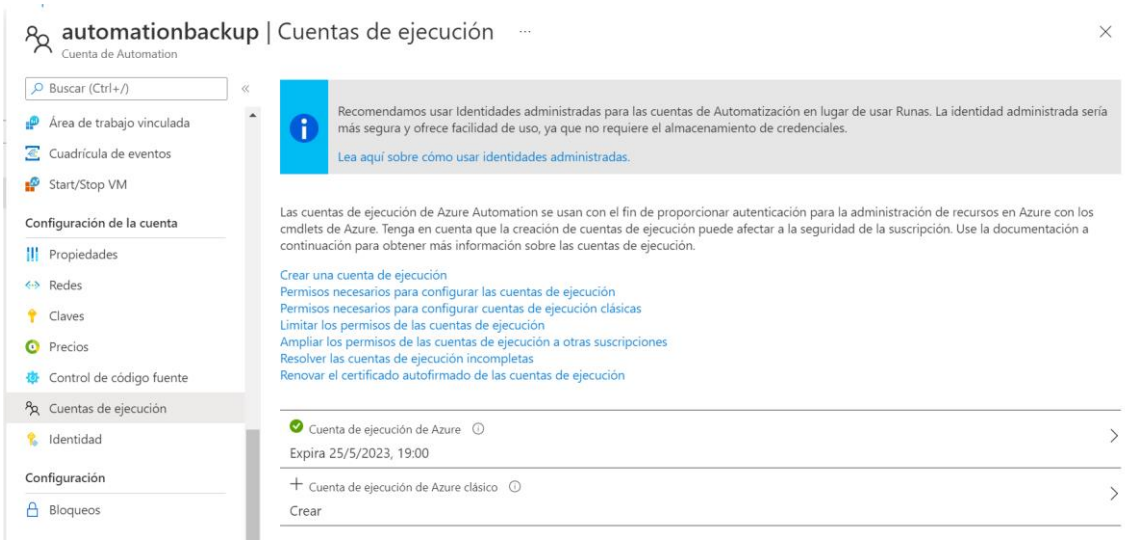

Figura 33 Visualización de la cuenta de ejecución en cuenta de automatización en Microsoft Azure

- **Creación de runbook. –** El runbook se va a ejecutar de manera automática cada vez que el servicio de Microsoft Defender detecte alguna anomalía, dicho runbook será ejecutado por el flujo de Logic App que éste se ejecutará cada vez el servicio de Microsoft Defender detecte alguna anomalía. Es importante señalar que el runbook ejecutará un código de Powershell que al momento de ejecutarse generará un snapshot del Azure File que está asociado al del Azure Backup, es decir, el snapshot lo genera el Azure Backup pero será llamado a generar por la runbook.

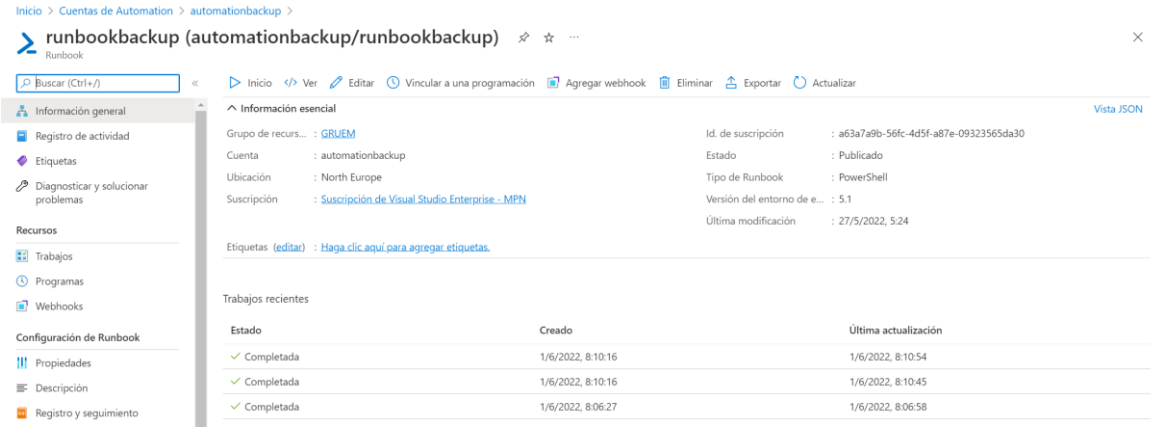

Figura 34 Visualización de runbook generado en la cuenta de automatización en Microsoft Azure

```
<#
.DESCRIPTION
Script de runbook que permite Generar un snapshot del File Shared de Azur
e File de Microsoft Azure.

.NOTES
Filename  : runbookbackup
Author    : Luis Talavera
Version   : 1.0
Date      : 26/05/2022
#>

Param (
    [Parameter(Mandatory = $true)][ValidateNotNullOrEmpty()]
    [String] $AzureSubscriptionId,
    [Parameter(Mandatory = $true)][ValidateNotNullOrEmpty()]
    [String] $VaultName,
    [Parameter(Mandatory = $true)][ValidateNotNullOrEmpty()]
    [String] $AzureFileShare,
    [Parameter(Mandatory = $false)][ValidateNotNullOrEmpty()]
    [Int] $RetentionDays = 30
)

$connectionName = "AzureRunAsConnection"

Try {
    #! Get the connection "AzureRunAsConnection "
    $servicePrincipalConnection = Get-AutomationConnection -
Name $connectionName
    Write-Output "Iniciando Sesion en Microsoft Azure"
    Add-AzureRmAccount -ServicePrincipal `
        -TenantId $servicePrincipalConnection.TenantId `
        -ApplicationId $servicePrincipalConnection.ApplicationId `
        -
CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
Catch {
    If (!$servicePrincipalConnection) {
        $ErrorMessage = "Conexión al $connectionName no encontrada"
        throw $ErrorMessage
    }
    Else {
        Write-Error -Message $_.Exception
        throw $_.Exception
    }
}

Select-AzureRmSubscription -SubscriptionId $AzureSubscriptionId
```

```
$currentDate = Get-Date
$RetailTill = $currentDate.AddDays($RetentionDays)
Write-
Output ("Los puntos de recuperación (RPO), se conservarán hasta el " + $R
etailTill)

#! Set ARM vault resource
Write-Output ("Trabajando en la bóveda: " + $VaultName)
$vault = Get-AzureRmRecoveryServicesVault -Name $vaultName
Set-AzureRmRecoveryServicesVaultContext -Vault $vault
$containers = Get-AzureRmRecoveryServicesBackupContainer -
ContainerType AzureStorage
Write-
Output ("Número de contenedores de copia de seguridad obtenidos: " + $con
tainers.Count)

ForEach ($container in $containers) {
    Write-
Output ("Trabajando en contenedores: " + $container.FriendlyName)
    #$fileshare = Get-AzureRmRecoveryServicesBackupItem -
WorkloadType AzureFiles -Container $container | `
    #Where-Object {$_.Name -like "*$AzureFileShare*"}
    $fileshare = Get-AzureRmRecoveryServicesBackupItem -
WorkloadType AzureFiles -Container $container
    If ($fileshare) {
        Write-Output ("Trabajando en File Share: " + $fileshare.Name)
        Backup-AzureRmRecoveryServicesBackupItem -Item $FileShare -
ExpiryDateTimeUTC $RetailTill
    }



}
Write-Output ("")
```

Figura 35 Script de Powershell que genera un snapshot en Azure Backup en Microsoft Azure

4.4.3.5 Configuración en servicio de Logic App

A continuación, se detalla las configuraciones implementadas en el servicio de Logic App.

- **Creación de flujo de aplicación. –** El flujo de aplicación será asociado al servicio de Microsoft Defender, pues este cada vez que detecte la anomalía enviará una petición para que desencadene una ejecución en el runbook, por ende, en nuestro flujo nosotros asociamos como desencadenador al servicio de Microsoft Defender y como

actividad desencadenadora debemos de configurar todos los parámetros de nuestra dé cuenta de automatización, que incluye nuestro runbook que genera el snapshot.

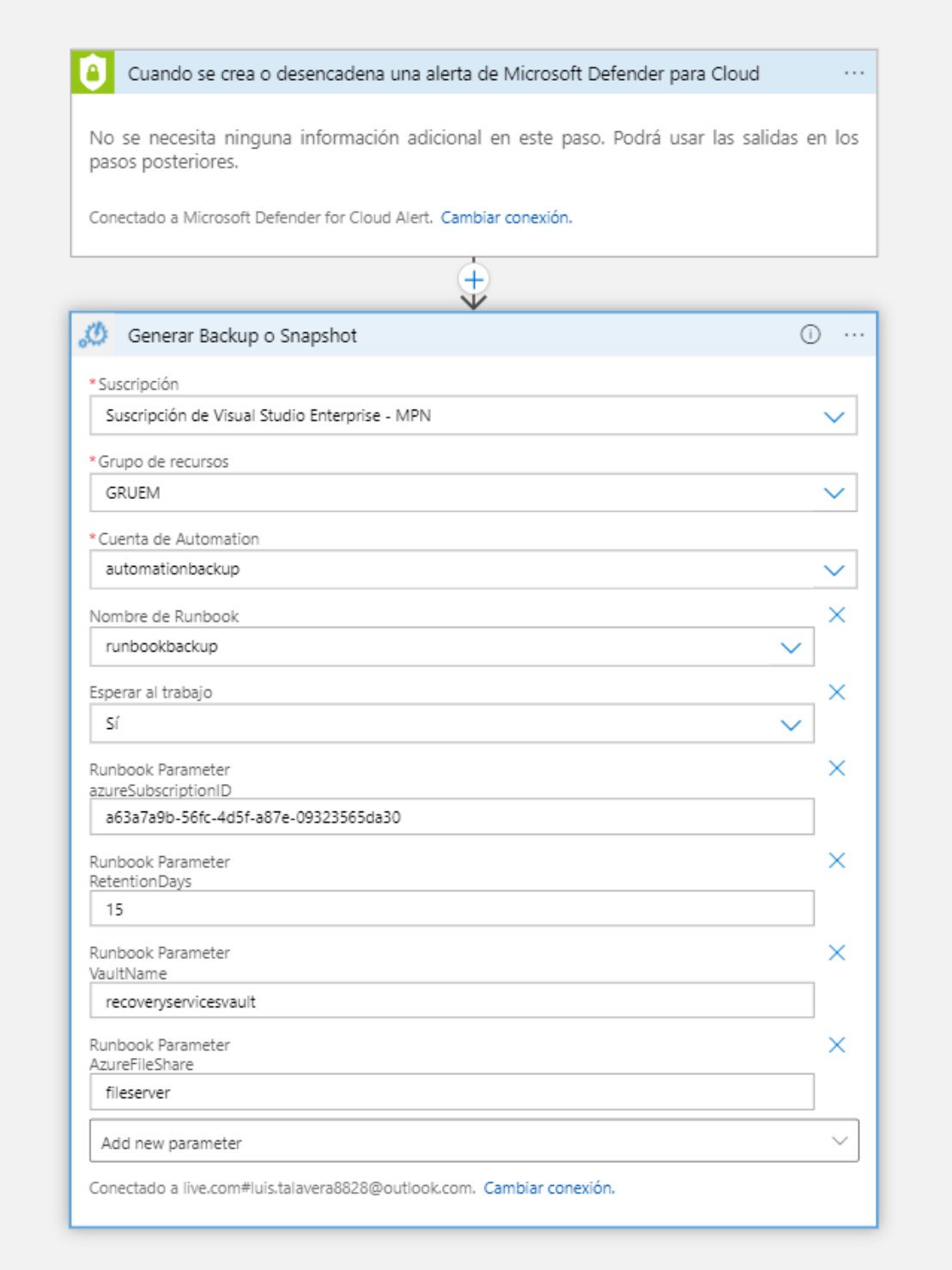

Figura 36 Creación de flujo aplicación de generación de snapshot en Logic App en Microsoft Azure

4.4.3.6 Configuración en servicio de Microsoft Defender

A continuación, se detalla las configuraciones implementadas en el servicio de Azure File Sync.

- **Instalación de agente. –** Para que el servicio de Microsoft Defender detecte cualquier anomalía en la máquina virtual habilitada, (Alcance de anomalías para máquinas virtuales que detecta el servicio (Microsoft, Detección de Anomalías de Microsoft Defender, 2022)), se debe de instalar el agente en la máquina virtual en el servicio de Microsoft Defender y luego asociarla al servicio de log analitycs creado previamente y el cual será encargado de almacenar y recopilar la información de la máquina virtual.

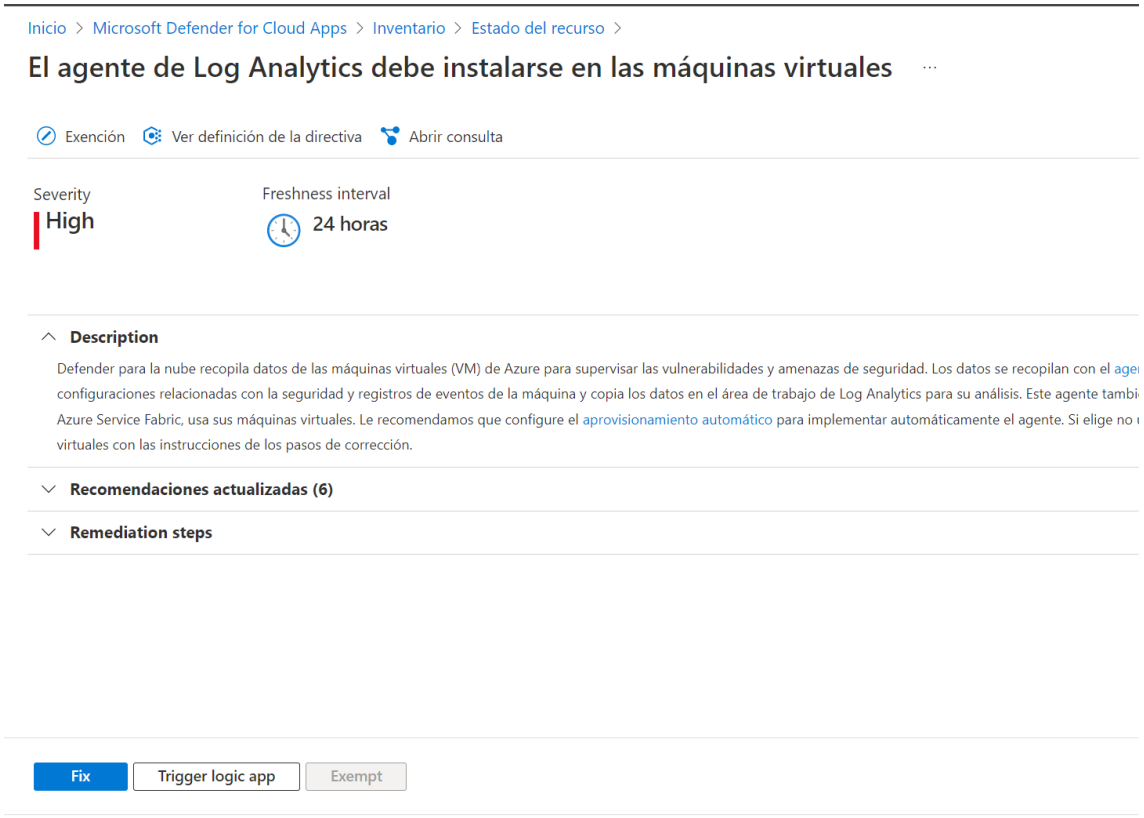

Figura 37 Instalación de agente asociado a Log Analytics.

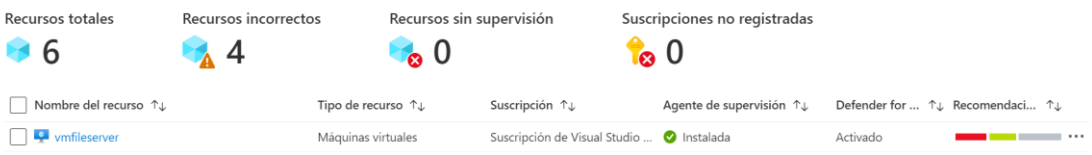

Figura 38 Visualización del agente instalado en servidor de File server

- **Asociación de Flujo de Logic App. –** Cada vez que el sensor de Microsoft Defender detecte alguna anomalía en la máquina virtual, este deberá de generar un snapshot, esto será generado un el flujo de logic app que será el orquestador con los demás servicios, es por ello que debemos de asociar nuestra maquina virtual con un nuestro servicio de logic app que contiene el flujo previamente ya configurado.

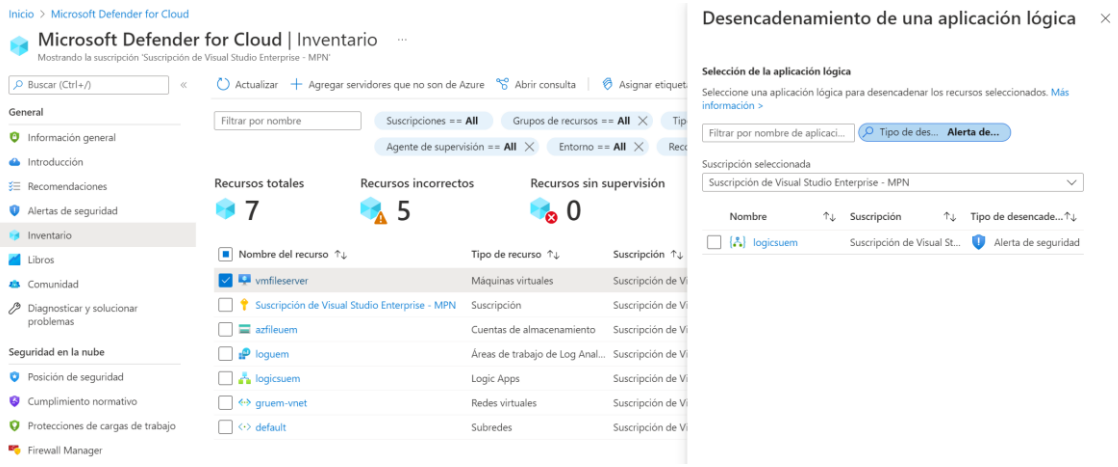

Figura 39 Asociación de Microsoft Defender con Logic App en Microsoft Azure

5. PRUEBAS Y VALIDACIÓN

A continuación, se detalla las pruebas ejecutadas.

5.1 Evasión de AMSI

Esta primera prueba podemos observar cuando un atacante desea hacer un bypass de AMSI, en tal sentido podemos apreciar como la herramienta de Microsoft Defender for Cloud detecta dicho bypass, por ende, dicho servicio procederá a iniciar el flujo de las actividades de los demás componentes.

1. Ejecución del ransomware en nuestra máquina virtual de file server.

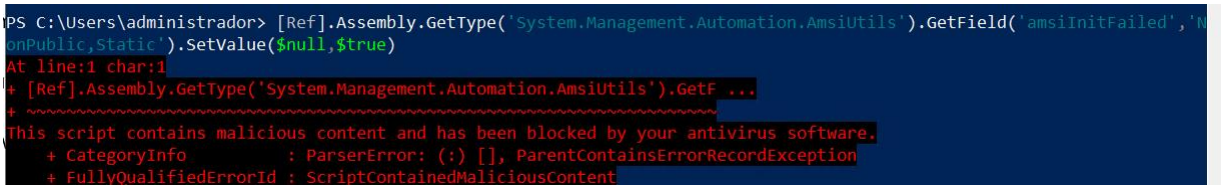

Figura 40 Ejecución de código AMSI

2. Detección del bypass de AMSI en el servicio de Microsoft Defender for Cloud.

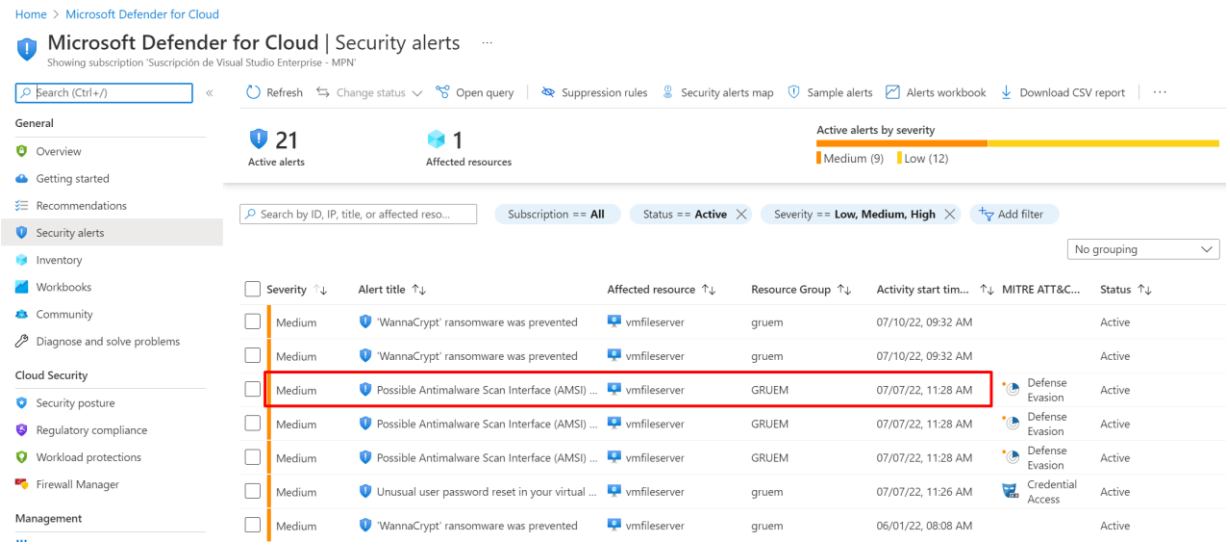

Figura 41 Detección de código AMSI

3. De forma automática el flujo de Logic Apps implementado, se ha ejecutado de manera satisfactoria.

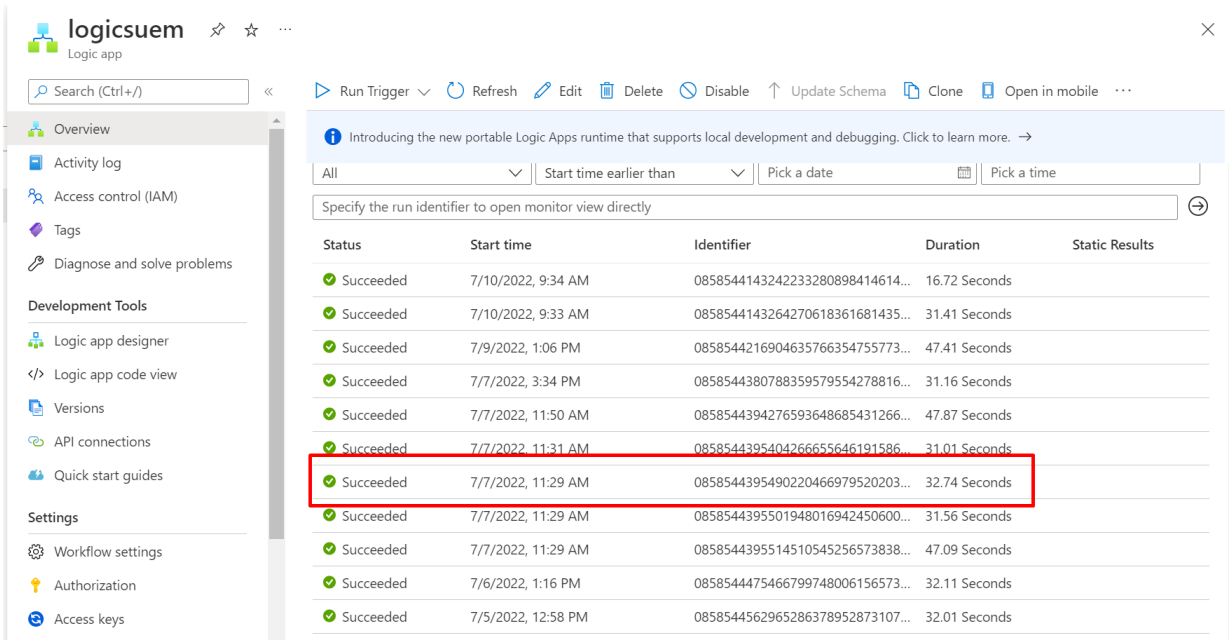

Figura 42 Generación de Flujo en LogicApps a partir de AMSI

4. Luego podemos visualizar que el job del servicio de Azure Automation se ha ejecutado de manera correcta.

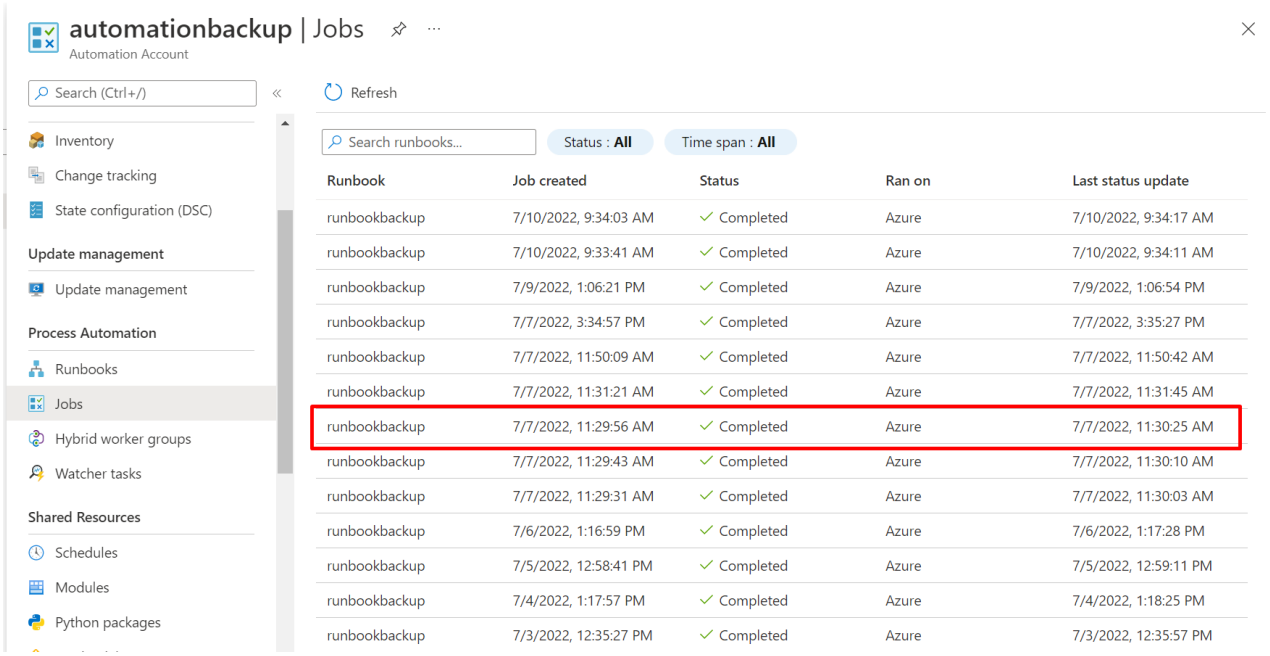

Figura 43 Generación de Script en Azure Automation a partir de AMSI

5. Finalmente, podemos ver el Backup generado de nuestra información almacenada en nuestro file server.

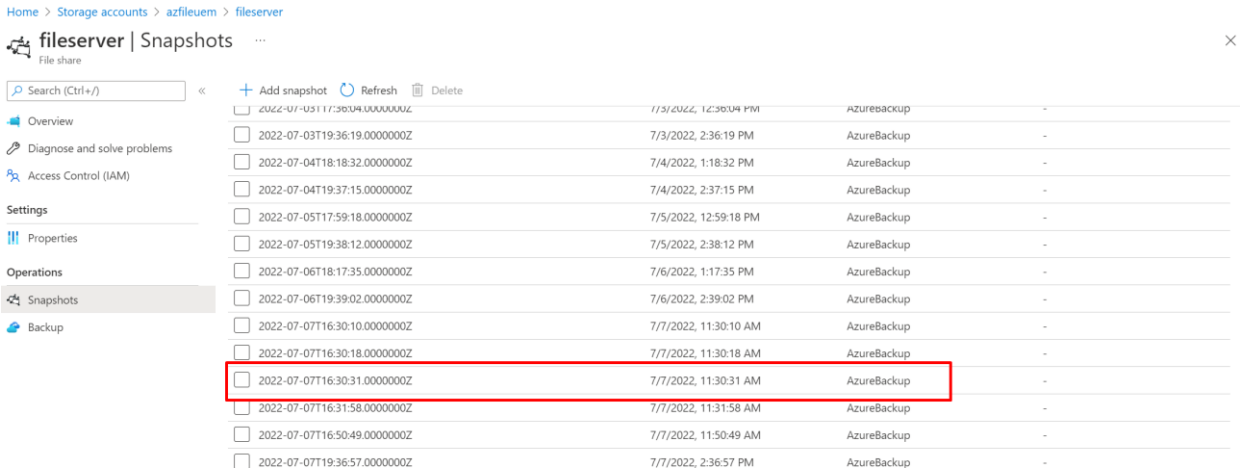

Figura 44 Generación de Backup a partir del AMSI ejecutado

5.2 Actividad inusual con IP maliciosa

Esta segunda prueba podemos observar cuando un atacante efectúa un escaneo de nuestros servidores que se visualizan a través de internet a través de una IP pública, en tal sentido podemos apreciar como la herramienta de Microsoft Defender for Cloud detecta dicho tráfico de entrada inusual, por ende, dicho servicio procederá a iniciar el flujo de las actividades de los demás componentes.

1. Detección de IP en el servicio de Microsoft Defender for Cloud.

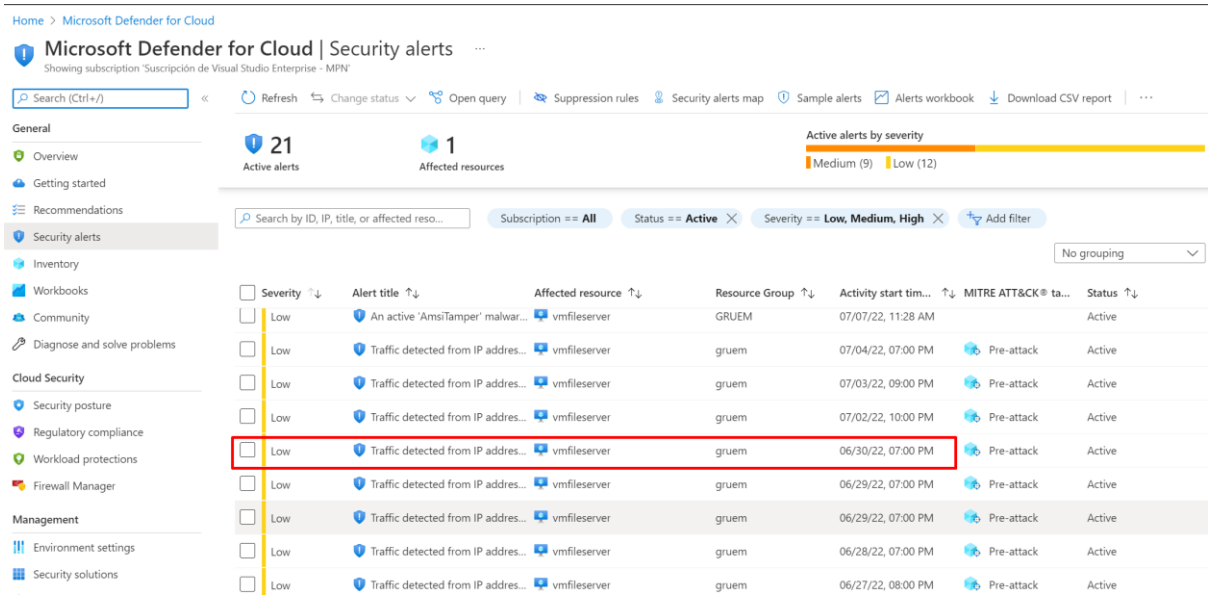

Figura 45 Detección de IP maliciosas

2. De forma automática el flujo de Logic Apps implementado, se ha ejecutado de manera satisfactoria.

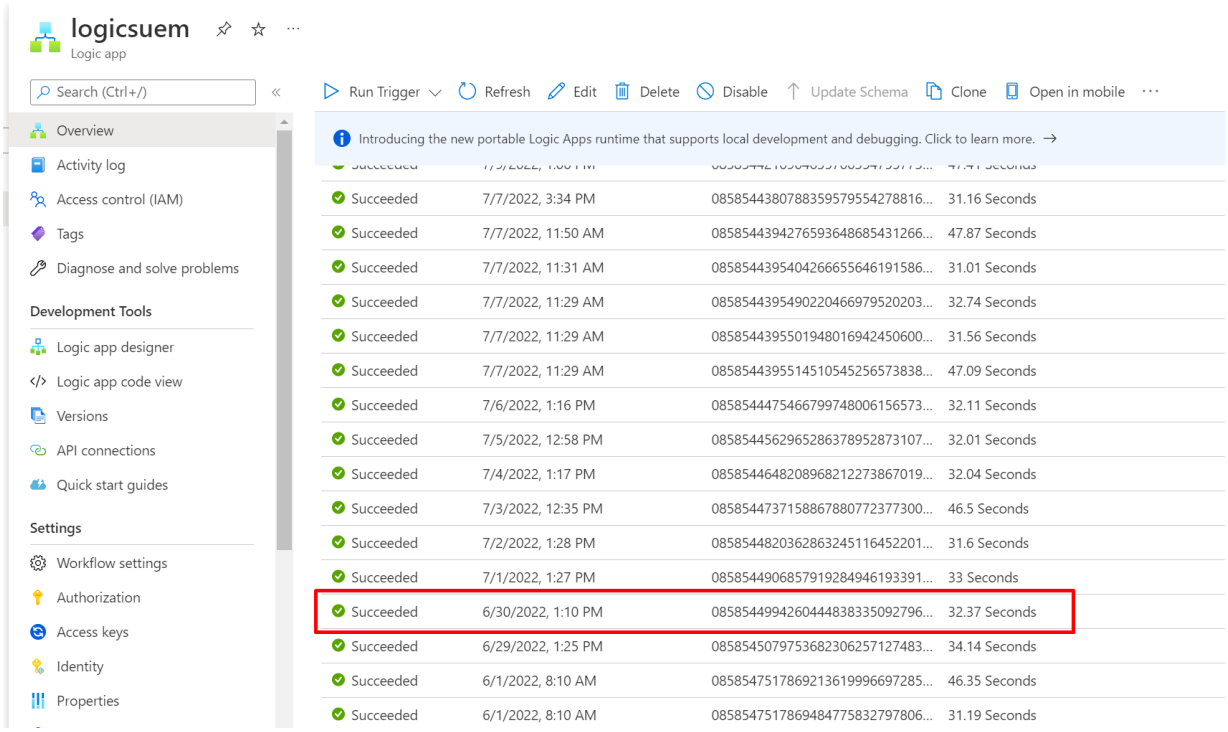

Figura 46 Generación de Flujo en LogicApps a partir de IP maliciosa

3. Luego podemos visualizar que el job del servicio de Azure Automation se ha ejecutado de manera correcta.

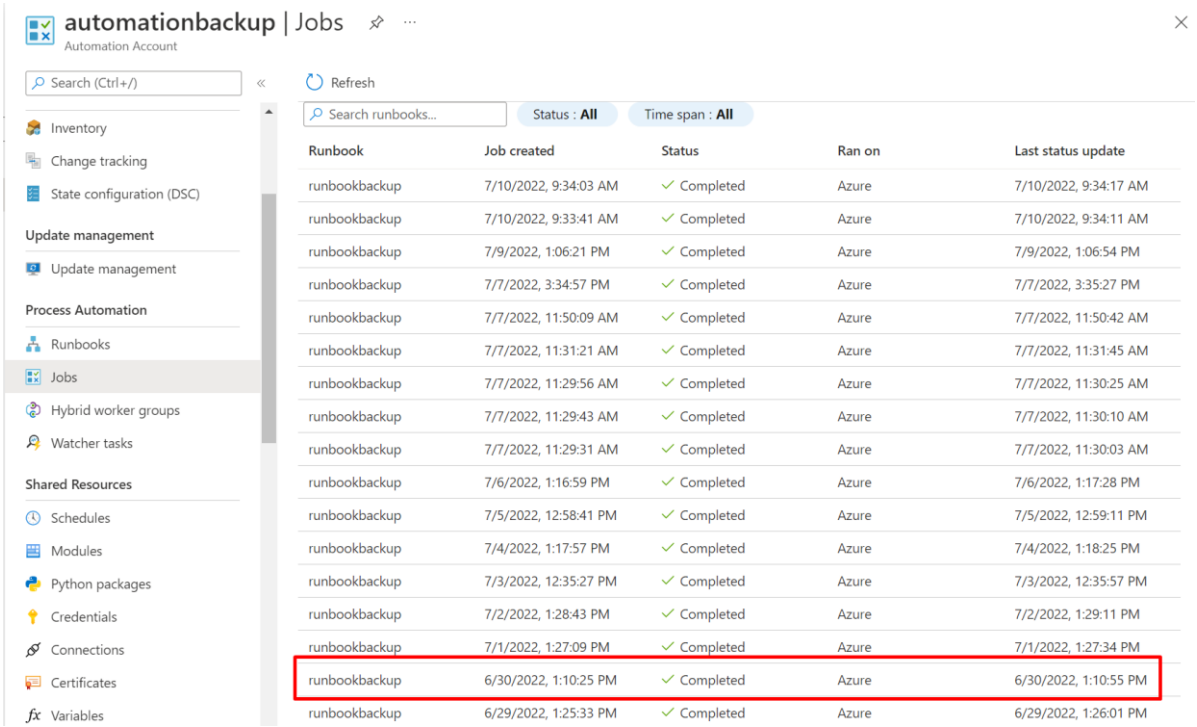

Figura 47 Generación de Script en Azure Automation a partir de IP maliciosa

4. Finalmente, podemos ver el Backup generado de nuestra información almacenada en nuestro file server.

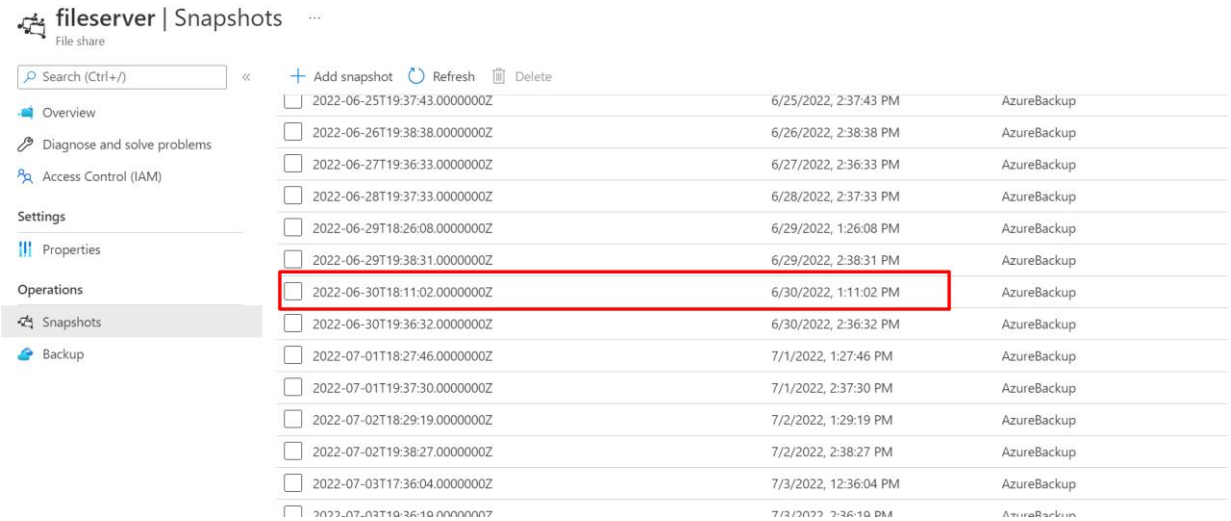

Figura 48 Generación de Backup a partir del IP maliciosa

5.3 Detección automática del malware

Esta tercera prueba podremos observar la detección automática de un archivo ransomware cuando se encuentra en nuestro servidor.

1. Ingreso del archivo ransomware en nuestro servidor file server.

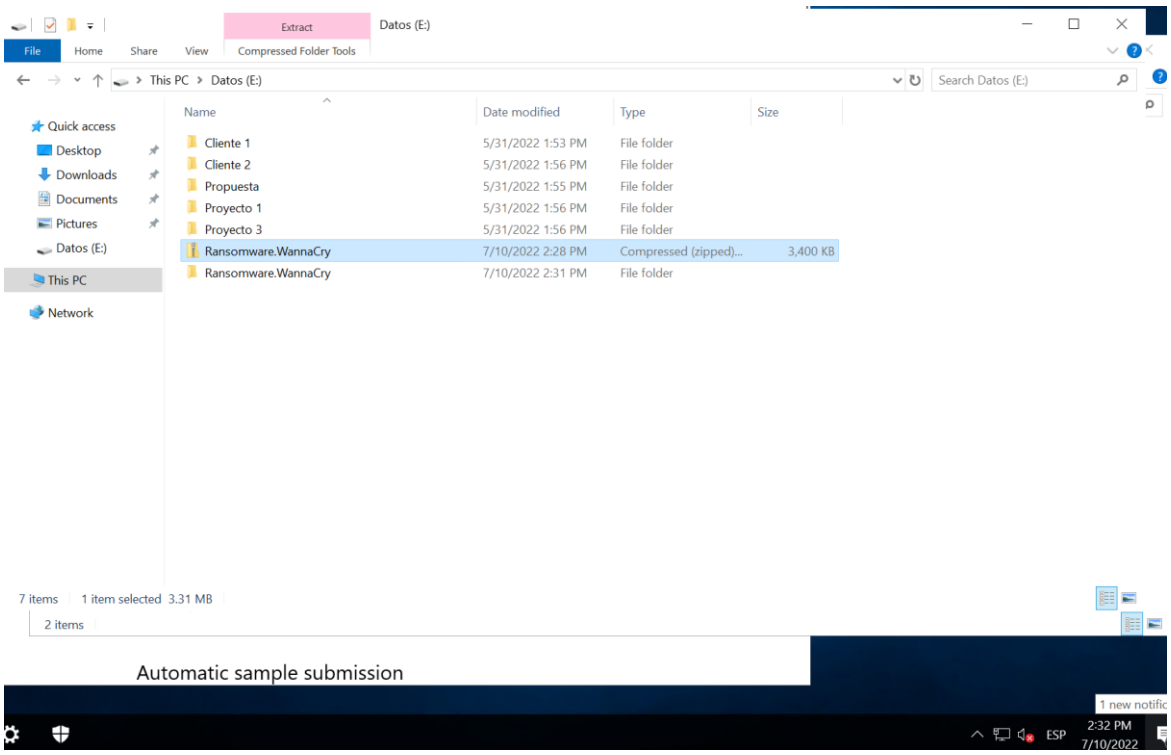

Figura 49 Detección de Ransomware en el servidor

2. Detección del archivo rasomware en el servicio de Microsoft Defender for Cloud.

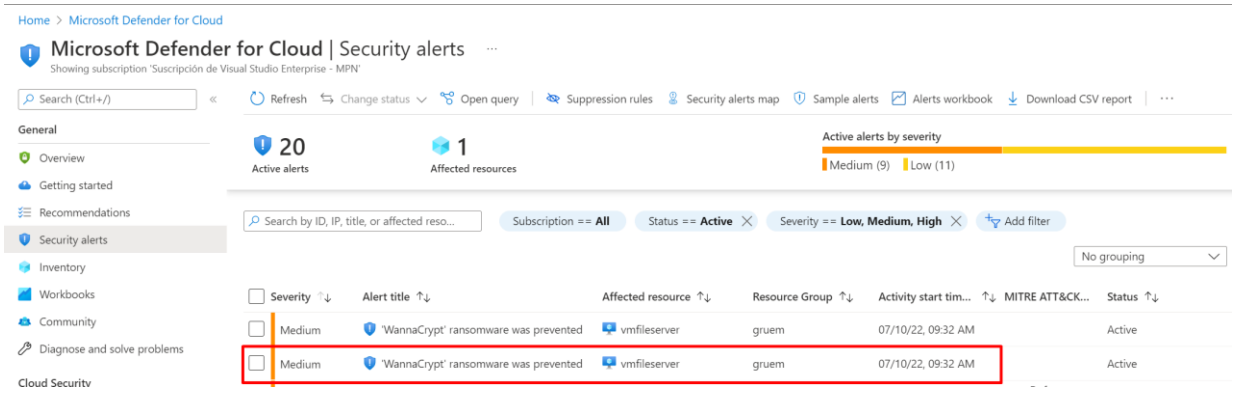

Figura 50 Detección de ransomware Phobos

3. De forma automática el flujo de Logic Apps implementado empieza a ejecutarse.

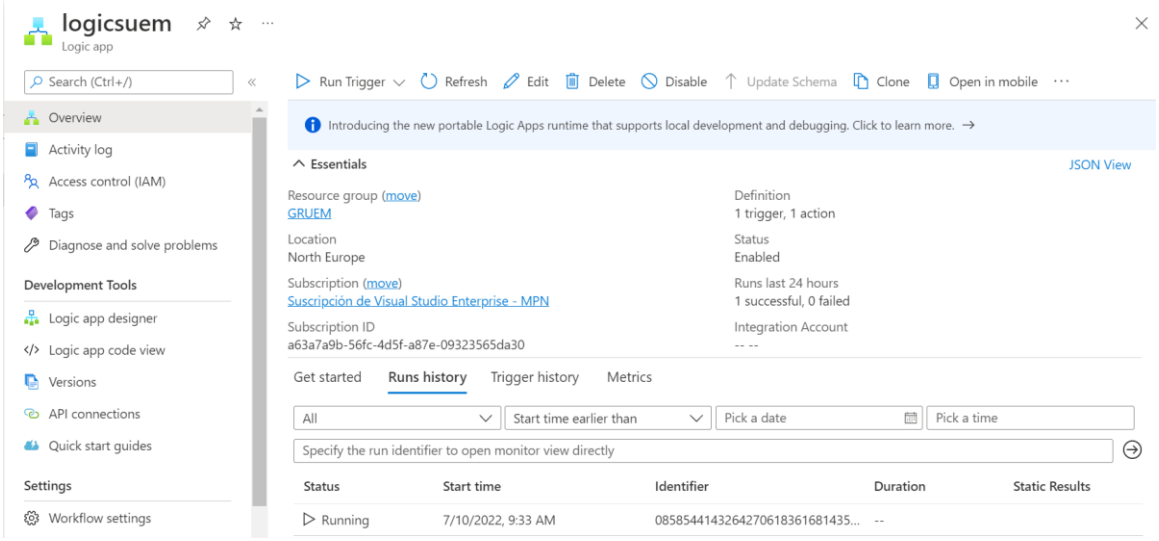

Figura 51 Inicio de generación de Flujo en LogicApps a partir de ransomware detectado

4. Al cabo de unos segundos podemos evidenciar que el servicio se ha ejecutado de manera correcta.

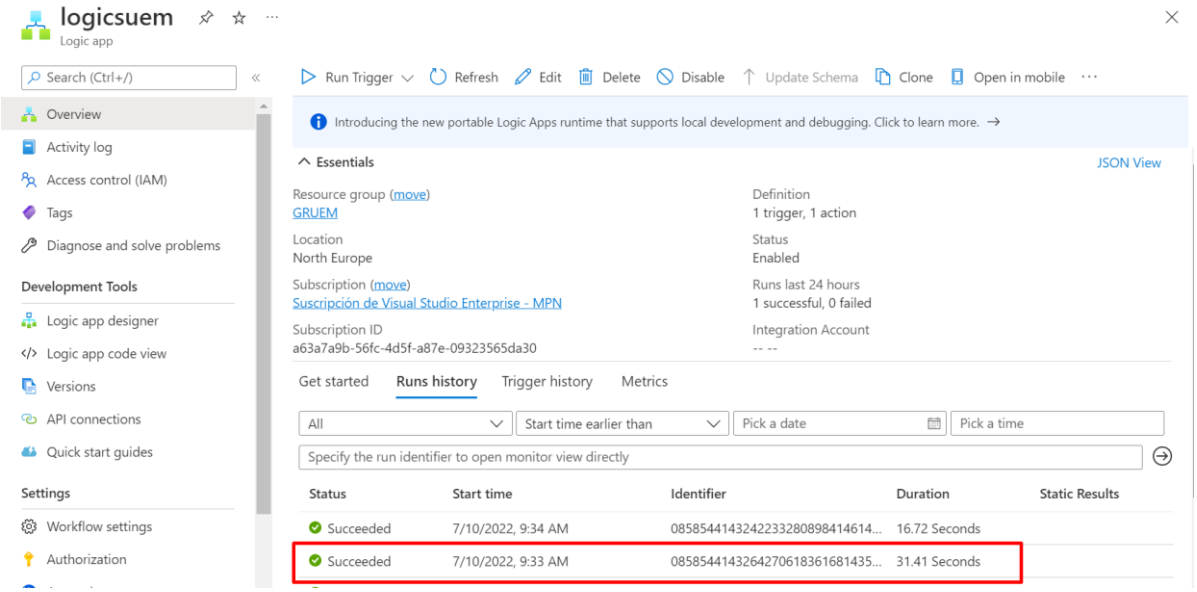

Figura 52 Generación final de Flujo en LogicApps a partir de ransomware detectado

5. Luego podemos visualizar que el job de servicio de Azure Automation también se ha ejecutado de manera correcta.

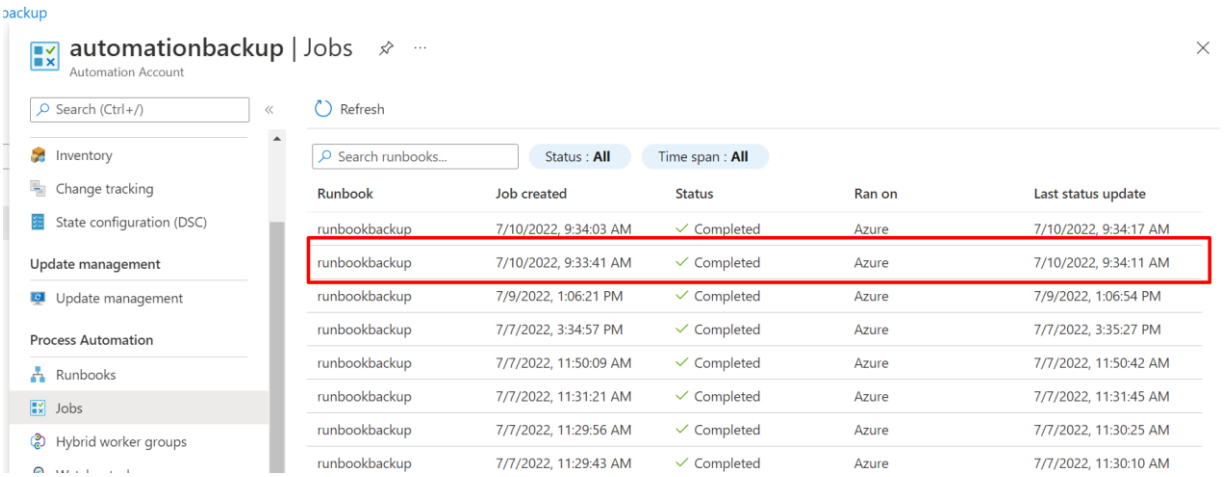

Figura 53 Generación de Script en Azure Automation a partir de detección de malware

6. Finalmente, podemos ver el Backup generado de nuestra información almacenada en nuestro file server.

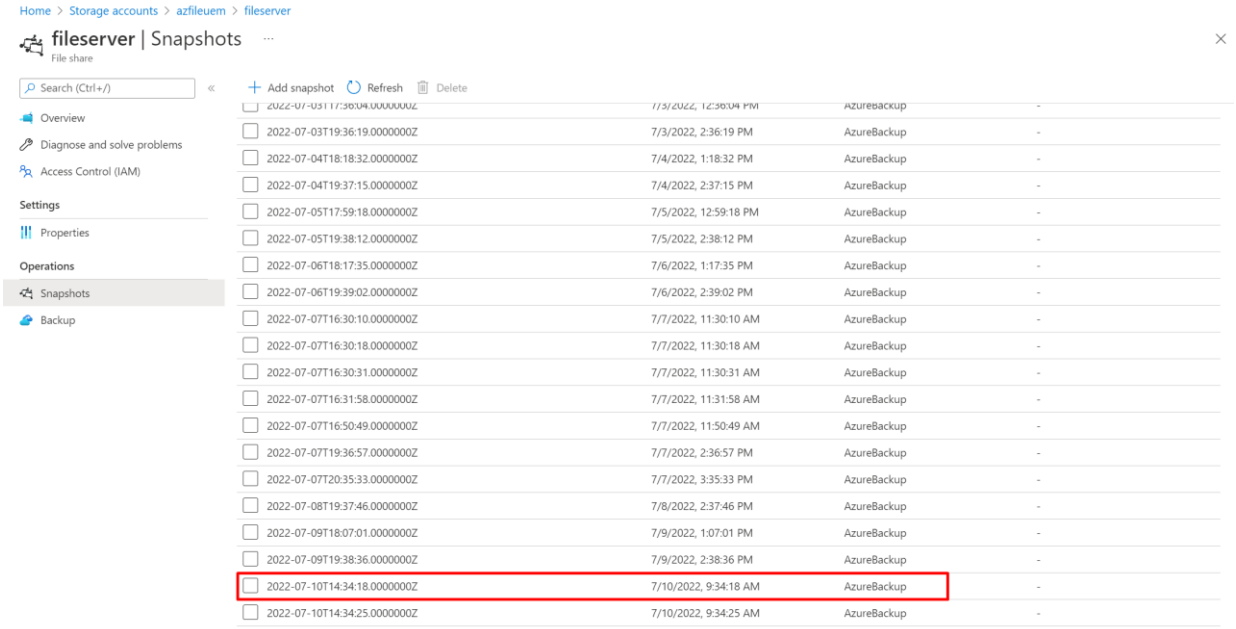

Figura 54 Generación de backup a partir de de detección de ransomware

5.4 Ejecución de malware

Esta cuarta prueba podremos observar cuando el ransomware se ha ejecutado en nuestro servidor, en tal, sentido vamos a ver como el comportamiento de la solución implementada.

1. El ransomware se ha ejecutado en nuestro servidor.

Figura 55 Ransomware ejecutado en nuestro servidor

2. Se puede visualizar en el servicio de Microsoft Defender for Cloud que se han generado varias alertas, esto debido que el ramsonware va ejecutando una serie de comandos de encriptamiento en cada parte del sistema operativo

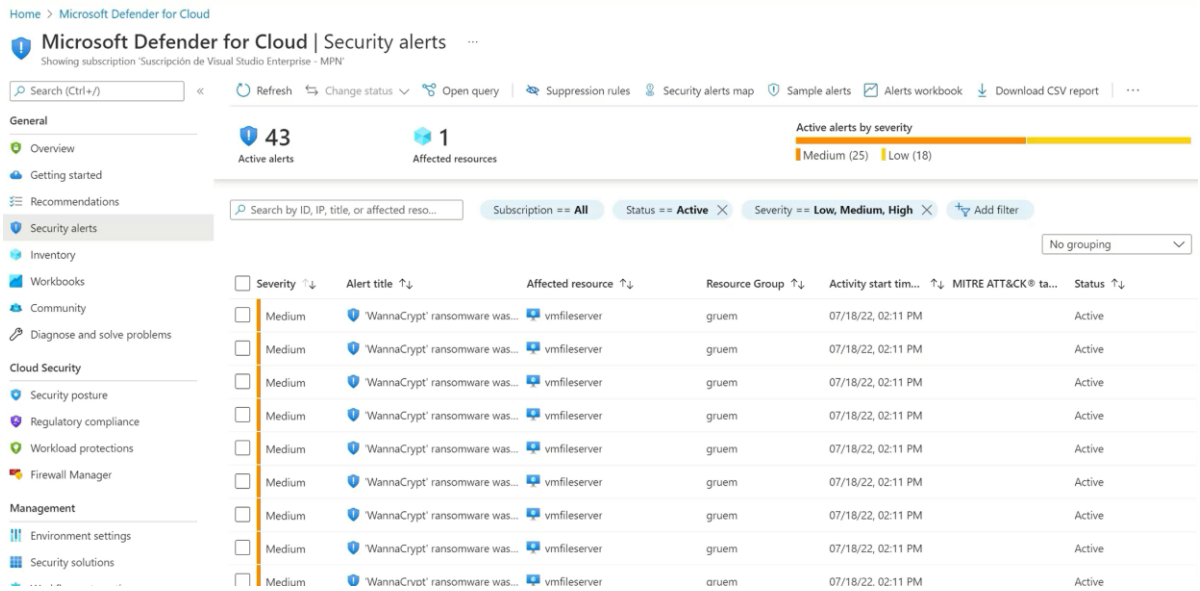

Figura 56 Detección de alertas en el servicio de Microsoft Defender for Cloud

3. El comportamiento del servicio de LogicApps será igual al servicio de Microsoft Defender for Cloud, pues como la herramienta Defender a detectado varias alertas en función a las ejecuciones efectuadas por el ransomware, pues este también generara varias alertas en el servicio en mención, tal como se puede ver en la imagen a continuación.

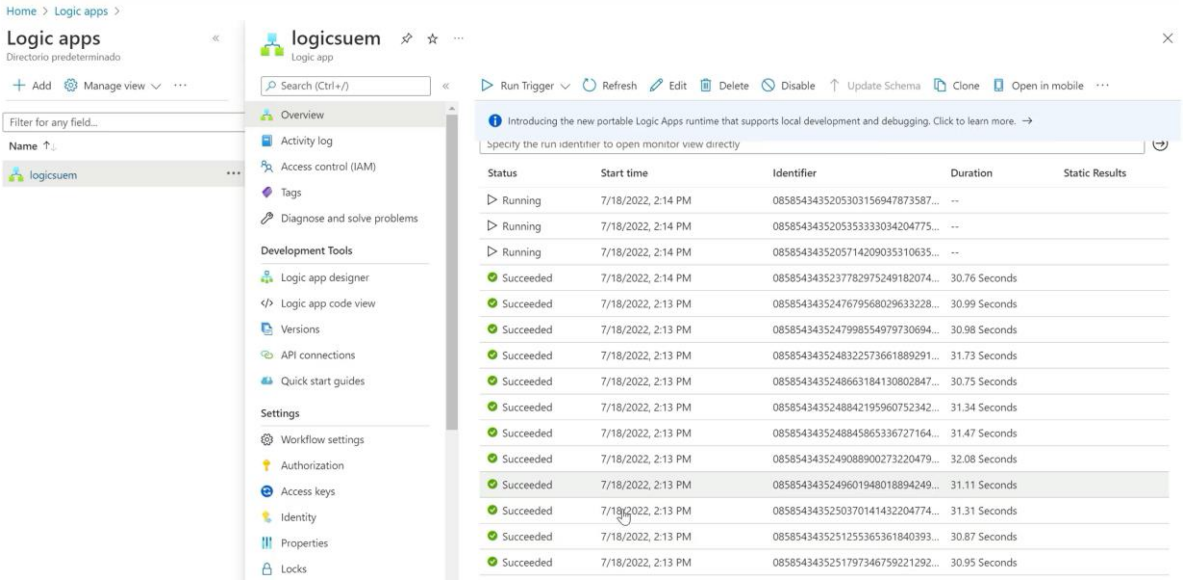

Figura 57 Generación de trigger en LogicApps

4. Bajo el mismo escenario que los servicios anteriores, las ejecuciones en el servicio de Azure Automation es igual, se ha ejecutado varias veces.

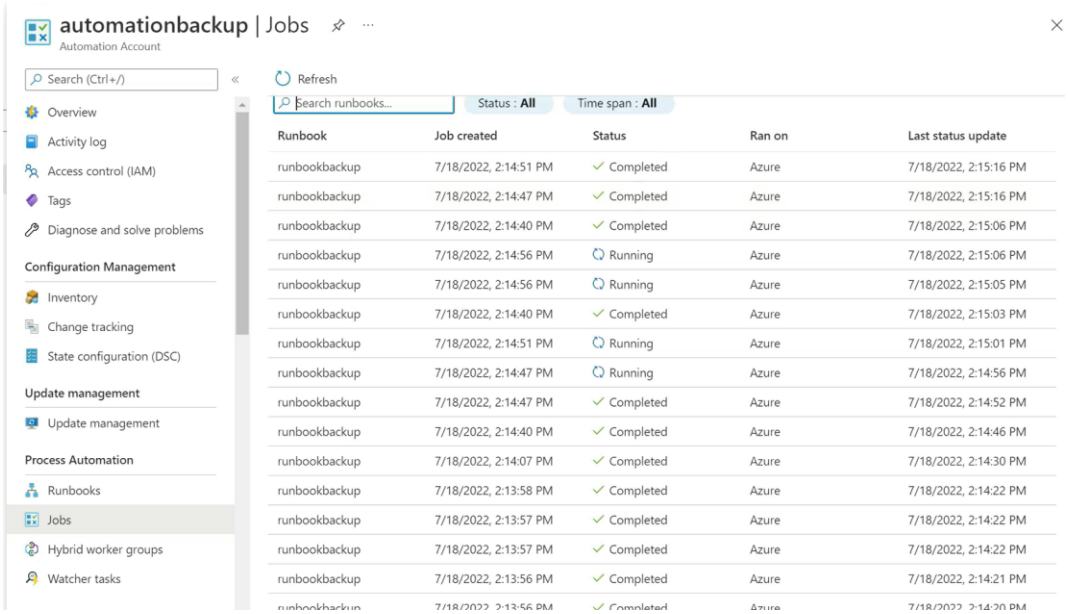

Figura 58 Ejecuciones de Azure Automation a partir de ejecución de ransomware

5. El último paso que podemos validar es la generación de todos los backups generados en función a las alertas detectadas por el Microsoft Defender a partir de cada actividad del ransomware que ejecutó en el sistema operativo.

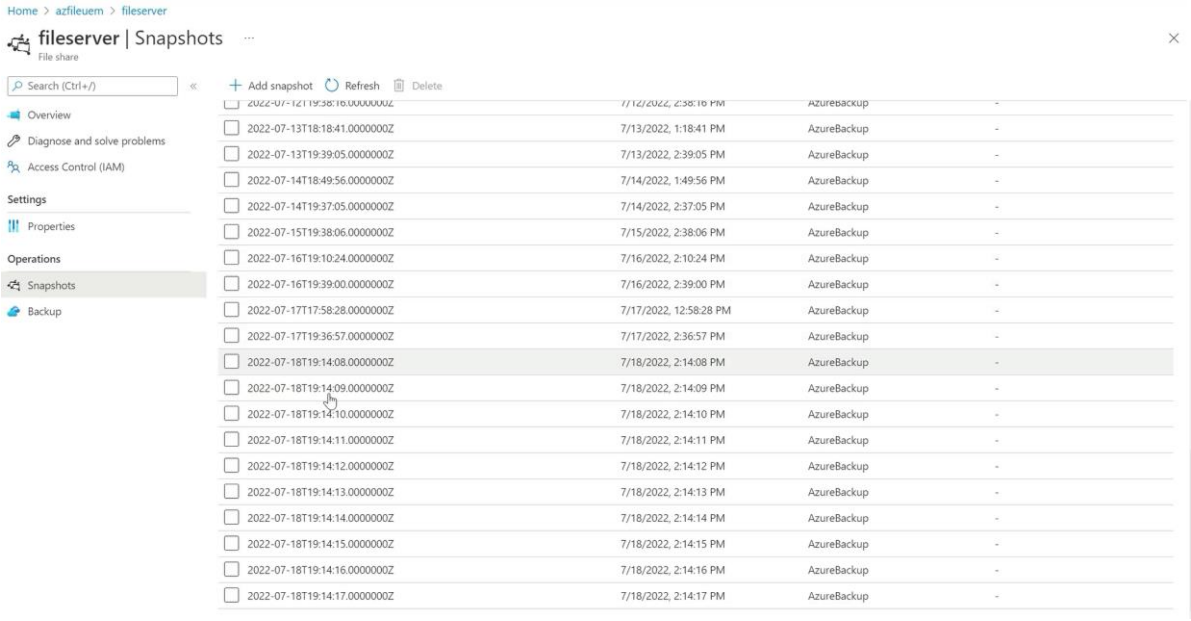

Figura 59 Generación de backups a partir del ransomware ejecutado

6. Sin embargo, se puede evidenciar que todos los backups generados cuentan con la extensión del ransomware por lo que impide generar ejecutar el proceso de restauración de archivo.

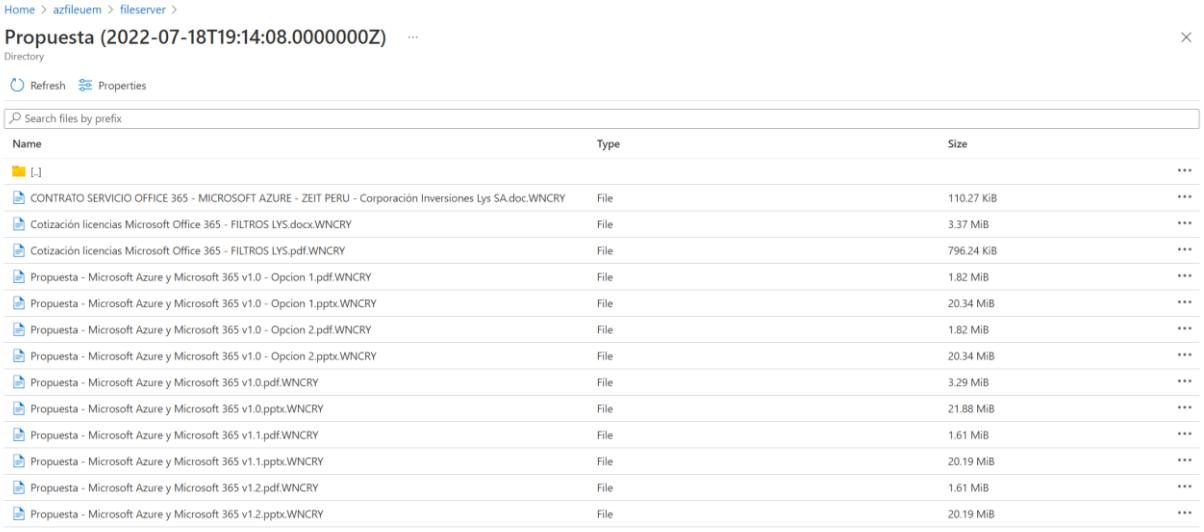

Figura 60 Revisión de un backup generado por la ejecución del ransomware

5.5 Restauración de un archivo

La última prueba que ejecutamos es la restauración de un archivo que se encuentra almacenado en un Backup generado de manera automática o en ataque preventivo.

1. Visualización de archivo que actualmente se encuentra afectado por el ransomware.

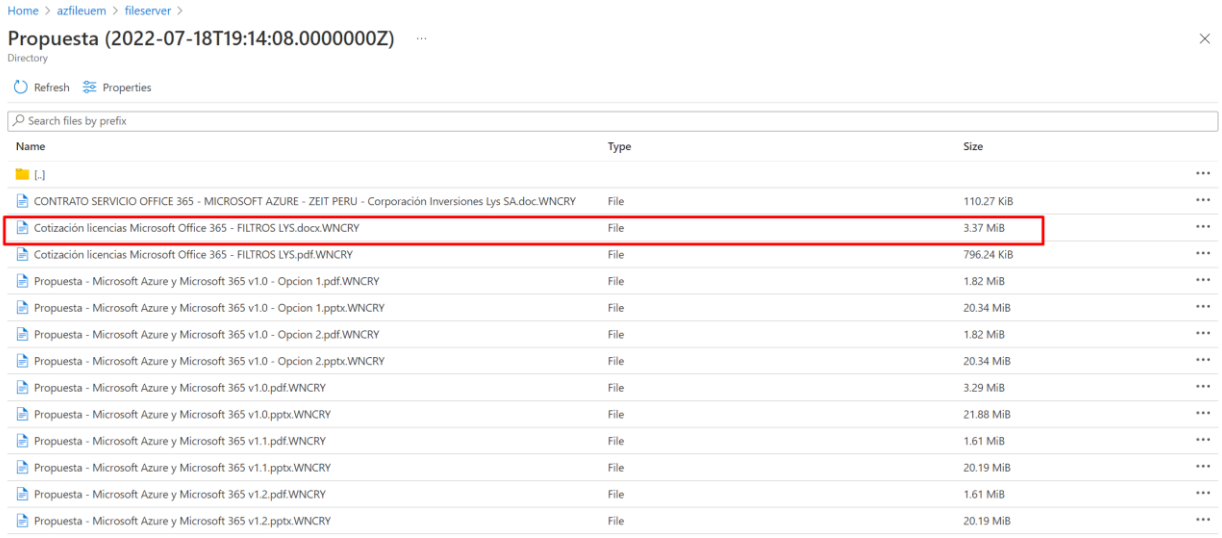

Figura 61Visualización de archivo afectado por el ransomware

2. Visualización de archivo en un Backup previo, vemos que no se encuentra afectado.

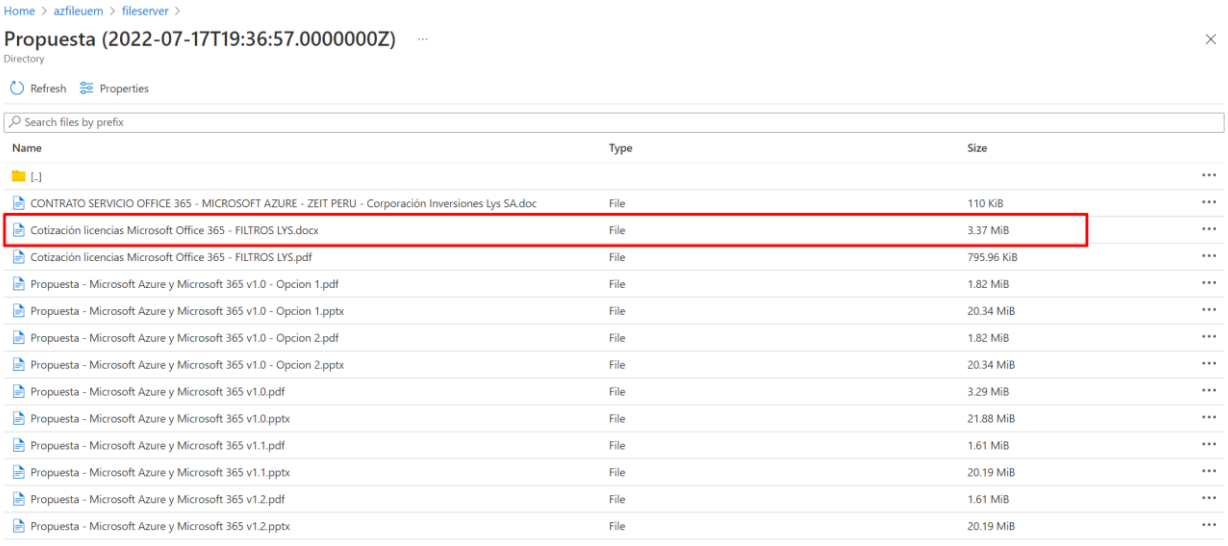

Figura 62 Visualización de un archivo de backup previo

3. El siguiente paso es seleccionar el archivo y darle clic en la opción restaurar.

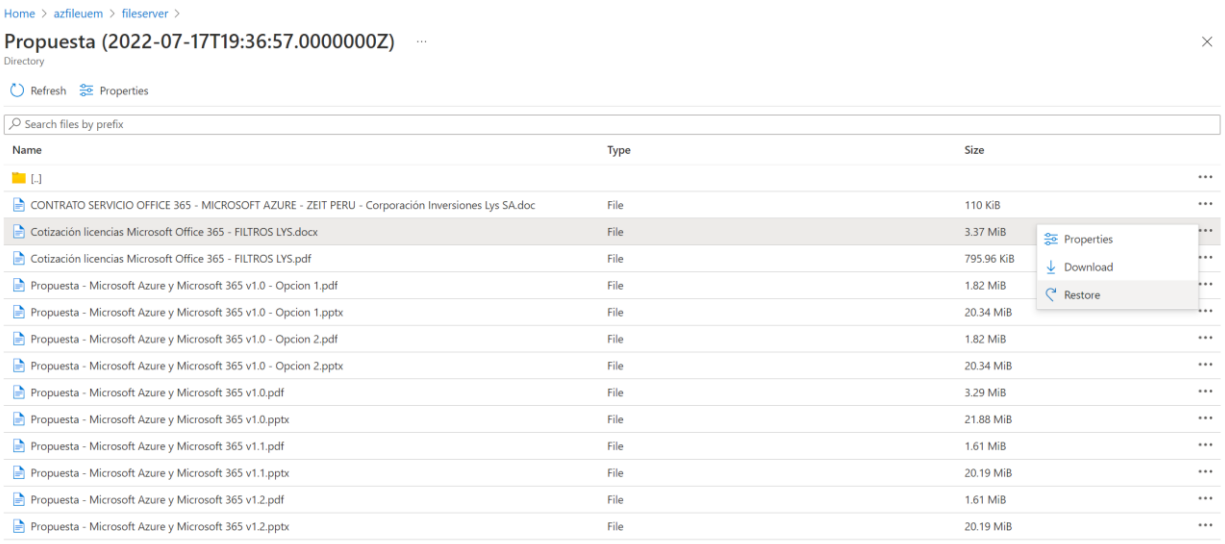

Figura 63 Opción de restauración de archivo

4. El siguiente paso es seleccionar la forma de restaurar el archivo, que puede ser crear uno nuevo o sobrescribir el actual, para este caso, vamos a seleccionar la opción sobrescribir.

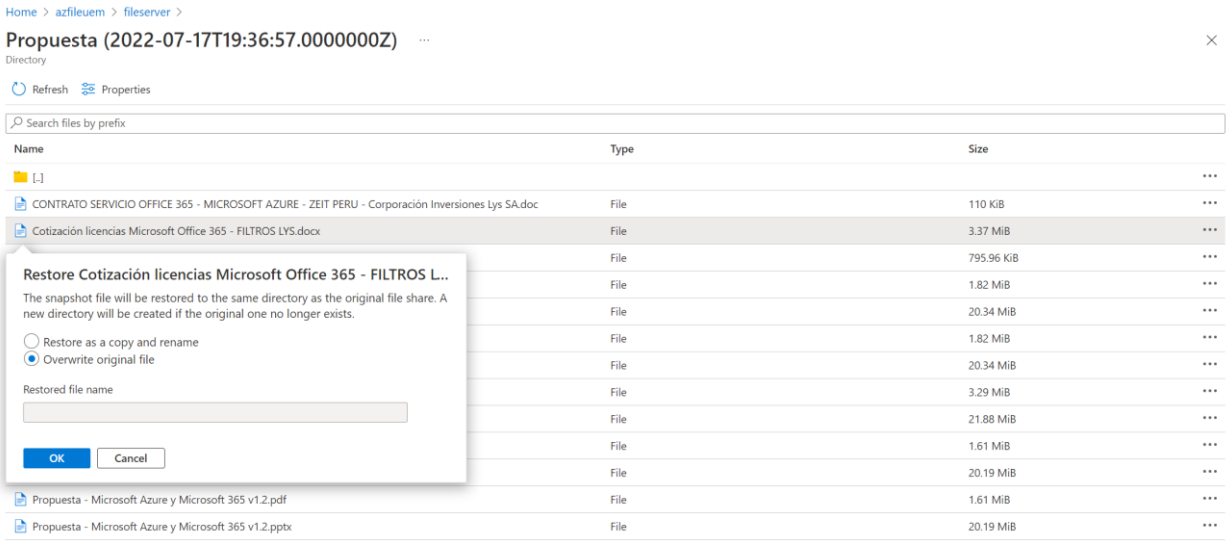

Figura 64 Opción sobrescribir de restauración de archivos

5. Finalmente, podemos ver el archivo restaurado y sobrescrito sobre el archivo afectado.

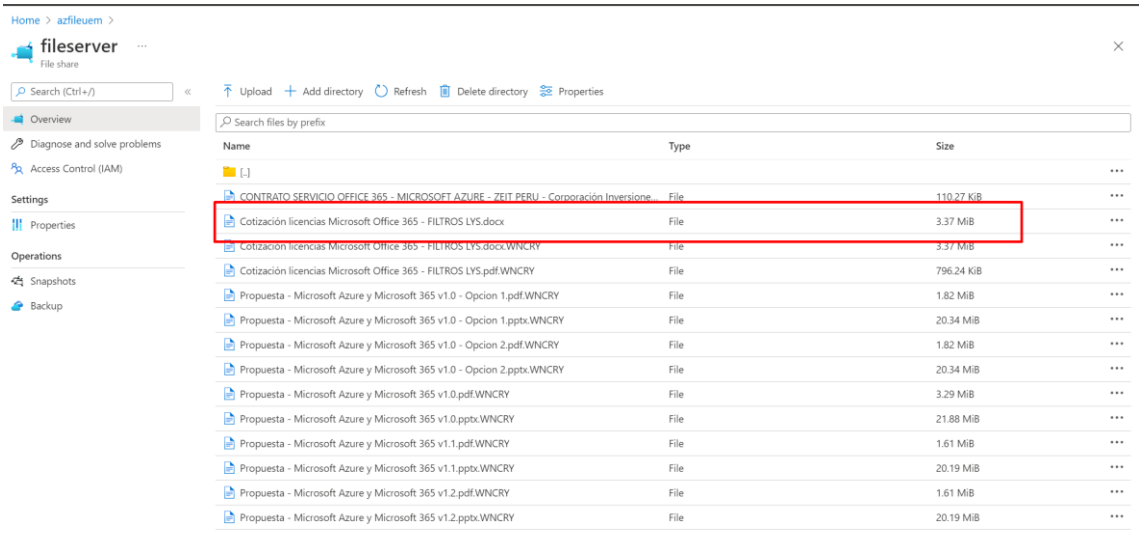

Figura 65 Archivo sobrescrito sobre el afectado

6. RESULTADOS

A continuación, se detalla los resultados ejecutados por cada objetivo general detallado en el punto 4.1.1 de este documento.

4.1 Objetivo General 01

El primer objetivo de este proyecto es elaborar un plan o guía de continuidad de negocio de un file server ante un ataque de malware en cloud. En tal sentido, se puede señalar que en todo el punto 4.4 de este documento se ha detallado la arquitectura, la creación de los servicios y la configuración de cada uno de ellos.

4.2 Objetivo General 02

El segundo objetivo de este proyecto es reducir el tiempo de recuperación (RTO) ante un ataque de malware de un file server. En tal sentido, primero partimos que en función a la experiencia en implementaciones del autor de este documento podemos señalar algunos tiempos identificados.

- Información muy crítica: 02 horas.
- Información crítica: 04 horas.
- Información mediamente crítica: 12 horas.
- Información poco crítica: 24 horas.

Dichos tiempos han sido estimados en función a las siguientes acciones a ejecutar, que cabe señalar, que puede variar en función a la realidad de cada organización.

- Restauración de snapshot.
- Asociación de una IP al nuevo servidor.
- Configurar la nueva ruta del file server en los dispositivos de los colaboradores.
- Asociar la nueva IP en aplicaciones que consuman dicha información.

Según las pruebas ejecutadas las cuales se han detallado en el punto 5 de este documento, se puede visualizar el procedimiento de restauración de la información y el tiempo estimado que tomó en restaurar un archivo a partir de un Backup generado, dicho tiempo aproximado fue de 30 segundos por archivo aproximadamente.

4.3 Objetivo General 03

El tercer objetivo de este proyecto es reducir el objetivo de punto de recuperación (RPO) ante un ataque de malware sobre un file server. En tal sentido, primero partimos que en función a la experiencia en implementaciones del autor de este documento podemos señalar algunos tiempos identificados.

- Información muy crítica: 01 backup x cada hora.
- Información crítica: 01 backup x cada 04 horas.
- Información mediamente crítica: 01 backup x cada 12 horas.
- Información poco crítica: 01 backup x cada 24 horas.

Según las pruebas ejecutadas las cuales se han detallado en el punto 5 de este documento, se puede evidenciar que el tiempo de generación de los backups que vendrían hacer los puntos de restauración, oscilan en el rango de 02 a 04 minutos. A continuación, se detalla los tiempos de cada una de las pruebas.

- Prueba 01: 03:05 minutos.
- Prueba 02: 04:00 minutos.
- Prueba 03: 02:50 minutos.

En este punto podemos señalar que los Backup solo se generan cuando detecta ataques preventivos, puesto que en caso el ransomware se ejecute los Backup generados también se encuentran encriptados, en tal sentido, los archivos no se podrán restaurar, por ende, debemos de tomar un Backup previo según el tiempo de antigüedad en el cual se generó.

4.4 Objetivo General 04

Implementar un plan de continuidad de negocio con los estándares más reconocidos de la industria.

El cuarto objetivo de este proyecto es alinear la guía a los estándares más reconocidos de la industria, por ende, como ya se ha señalado en secciones anteriores de este documento, los estándares utilizados son los siguientes:

- ISO 22301:2019.
- Cloud Security Alliance (CSA).
- Centro para la Internet Segura (CIS).

7. CONCLUSIONES

Podemos concluir que se ha podido evidenciar una reducción considerable (menos de un minuto por archivo) en cuanto al RTO bajo la solución propuesta, pues en un modelo tradicional toma mucho más tiempo en efectuar la restauración de los archivos, ya que primero se debe de buscar el Backup para luego restaurarlo en un sistema operativo nuevo que previamente se tendrá que desplegar; lo mencionado esta orientado al objetivo 02 de este documento, el cual por lo señalado se ha cumplido de manera satisfactoria.

Por otro lado, también se ha podido evidenciar que los puntos de restauración (RPO) se pueden generar al momento que la herramienta de Microsoft Defender detecte un posible ataque, pues de esa manera podemos tener un punto de restauración en un rango de 02 a 04 minutos, mientras que en modelo tradicional usualmente se maneja backup como mínimo de 01 hora, dicho punto nos ha permitido cumplir de manera satisfactoria el requerimiento 03. Sin embargo, es importante señalar que se ha podido evidenciar que en caso el ransomware llegue a ejecutarse en nuestro servidor, la herramienta igual generará backups pero estos no funcionarán al momento que deseamos restaurar pues los archivos ya que estos igual se encontrarán encriptados; pero como nosotros contamos con otros backups generados por la misma plataforma de manera automatizada como un plan de contingencia adicional a la estrategia ya mencionada durante todo el documento; estos pueden ser utilizados para la restauración de los archivos, pues al estar en una plataforma aislada del ambiente onpremises podemos señalar que los Backups generados no se verán afectados por el ransomware, por lo que podemos mencionar que dichos backups pueden tener una integridad del 100% de nuestros datos; además al ser un modelo de Plataforma como Servicio (PaaS) este no requiere contar con una máquina virtual por lo que se puede desplegar de manera inmediata.

Para el caso de los objetivos 01 y 04 propuestos en este documento se puede señalar que a lo largo del desglose de cada sección de este documento se ha podido detallar el procedimiento de ejecución de la solución propuesta, así como también los estándares más resaltantes que la industria tiene disponible a la fecha.

Finalmente, podemos señalar que para la implementación de esta solución se requiere contar con un consultor con conocimientos intermedios en la plataforma de Microsoft Azure, además la empresa debe de contar con una suscripción de Microsoft Azure adquirida, pues en ella se

desplegarán los servicios indicados en el documento; y para los servicios disponibles por la plataforma de Microsoft Azure se puede indicar que funcionan de manera correcta en cuanto a las pruebas ejecutadas de manera preventiva más no cuando el rasomware ya se ha ejecutado, para este caso los archivos igual se encriptan.

8. TRABAJOS FUTUROS

A continuación, se detalla los trabajos futuros a considerar a partir del presente trabajo de investigación.

- Se debe de considerar implementar el mismo alcance de la solución en otras nubes, como AWS y Google Cloud.
- Implementar un procedimiento de respuesta ante un incidente que se está tratando.
- Implementar un procedimiento y/o estrategia de forense del incidente que se está tratando, así como también para los servicios implementados.
- Hacer otro tipo de ataques preventivos para poder validar alguna amenaza no considerada.

9. REFERENCIAS

Acktib. (19 de Mayo de 2021). *En qué consiste un RTO y un RPO: qué considerar para definirlos*. Obtenido de https://acktib.com/en-que-consiste-un-rto-y-un-rpo-que-considerar-para-definirlos/#:~:text=En%20resumen%2C%20podemos%20decir%20que,de%20seguridad%20y%20el%20incidente.

AENOR. (2010). *AEN/CTN 157 - PROYECTOS*. Recuperado el 25 de abril de 2013, de Normas y Publicaciones: http://www.aenor.es/aenor/normas/ctn/fichactn.asp?codigonorm=AEN/CTN%20157

Alliance, C. S. (26 de Julio de 2017). *Guía de seguridad para áreas críticas de enfoque en Cloud Computing v4.0*. Obtenido de https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Amazon Web Services. (2022). *Centro de Cumplimiento*. Obtenido de https://aws.amazon.com/es/compliance/programs/

AV-TEST. (16 de Julio de 2019). *Security Report 2018/2019*. Obtenido de https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf

Bachmaier, C. (2006).

Centro Critológico, N. (2018). *Medidas de Seguridad contra Ransomware*. Obtenido de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

Crespo Martínez, I. S. (Setiembre de 2019). *Análisis de Criptografía usada por ransomware mediante instrumentación dinámica de binarios*. Obtenido de http://webdiis.unizar.es/~ricardo/files/TFMs/CriptografiaRansomwareDBI.pdf

IBM. (25 de Noviembre de 2020). *Adaptarse y responder a los riesgos con un plan de continuidad de negocio (BCP)*. Obtenido de https://www.ibm.com/es-es/services/business-continuity/plan

Info-lab. (2017). *Ransomware: Seguridad, investigación y tareas forenses*. Obtenido de http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1595/JAIIO%20SID%202017-2936-Ransomware-CR.pdf?sequence=1

ISO ORG. (2019). *Sistemas de gestión de la continuidad del negocio*. Obtenido de https://www.iso.org/standard/75106.html

Microsoft. (s.f.). *¿Qué es Azure?* Obtenido de https://azure.microsoft.com/es-es/overview/what-is-azure/

Microsoft. (Octubre de 2021). *Informe Anual de Ciberseguridad*. Obtenido de https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738

Microsoft. (10 de Mayo de 2022). *¿Qué es Azure Files?* Obtenido de https://docs.microsoft.com/es-es/azure/storage/files/storage-files-introduction

Microsoft. (09 de junio de 2022). *¿Que es el Ransomware según Microsoft?* Obtenido de ¿Que es el Ransomware según Microsoft?: https://docs.microsoft.com/es-es/security/compass/human-operated-ransomware

Microsoft. (21 de Abril de 2022). *¿Qué es Microsoft Defender for Cloud?* Obtenido de https://docs.microsoft.com/es-es/azure/defender-for-cloud/defender-for-cloud-introduction

Microsoft. (21 de Febrero de 2022). *¿Qué es PowerShell?* Obtenido de https://docs.microsoft.com/es-es/powershell/scripting/overview?view=powershell-7.2

Microsoft. (2022). *Centro de Cumplimiento*. Obtenido de https://docs.microsoft.com/es-es/azure/compliance/

Microsoft. (Junio de 2022). *Configuración de Sincronización Grupo de Sincronización.* Obtenido de https://docs.microsoft.com/es-es/azure/storage/file-sync/file-sync-server-endpoint-create?tabs=azure-portal.

Microsoft. (27 de Mayo de 2022). *Costos de Azure Automatización*. Obtenido de https://azure.microsoft.com/es-es/pricing/details/automation/

Microsoft. (Junio de 2022). *Costos de Azure Backup*. Obtenido de https://azure.microsoft.com/es-es/pricing/details/backup/

Microsoft. (27 de Mayo de 2022). *Costos de Azure FIles*. Obtenido de https://azure.microsoft.com/es-es/pricing/details/storage/files/

Microsoft. (Junio de 2022). *Costos de Log Analytics*. Obtenido de https://azure.microsoft.com/es-es/pricing/details/monitor/

Microsoft. (Junio de 2022). *Costos de Logic App*. Obtenido de https://azure.microsoft.com/es-es/pricing/details/logic-apps/

Microsoft. (24 de Mayo de 2022). *Costos de Microsoft Defender for Cloud*. Obtenido de https://azure.microsoft.com/es-es/pricing/details/defender-for-cloud/

Microsoft. (21 de Junio de 2022). *Detección de Anomalías de Microsoft Defender.* Obtenido de https://docs.microsoft.com/es-es/azure/defender-for-cloud/alerts-reference

Microsoft. (27 de Junio de 2022). *Ransomware-as-a-service.* Obtenido de https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Microsoft. (13 de Mayo de 2022). *Roles integrados de Azure*. Obtenido de https://docs.microsoft.com/es-es/azure/role-based-access-control/built-in-roles

Microsoft. (24 de Mayo de 2022). *Tipos de almacenamiento del servicio de Almacenamiento de Microsoft Azure*. Obtenido de https://docs.microsoft.com/es-es/azure/storage/common/storage-account-overview

Microsoft. (s.f.). *Oferta de Microsoft Azure*. Obtenido de https://azure.microsoft.com/es-es/support/legal/offer-details/

Microsoft. (s.f.). *Qué es IaaS*. Obtenido de https://azure.microsoft.com/es-es/overview/what-is-iaas/#overview

Microsoft. (s.f.). *Qué es PaaS*. Obtenido de https://azure.microsoft.com/es-es/overview/what-is-paas/

Microsoft. (s.f.). *Qué es SaaS*. Obtenido de https://azure.microsoft.com/es-es/overview/what-is-saas/

Miró Julià, J. (2010). *Recursos para aprender a escribir.* Recuperado el septiembre de 2012, de http://bioinfo.uib.es/~joemiro/RecEscr/manual.pdf

PcRisk. (15 de Junio de 2021). *Cibersecuestro Phobos*. Obtenido de https://www.pcrisk.es/guias-de-desinfeccion/9023-phobos-ransomware

PWC. (s.f.). *La nueva estructura de alto nivel ISO.* Recuperado el 07 de Junio de 2022, de La nueva estructura de alto nivel ISO: https://auditortraining.pwc.com.au/blog/2015/01/20/new-iso-high-level-structure-mean/#:~:text=The%20High%2DLevel%20Structure%20(HLS,between%20systems%20of%20different%20disciplines.

QuestionPro. (s.f.). *¿Qué es la metodología de la investigación?* Obtenido de https://www.questionpro.com/blog/es/metodologia-de-la-investigacion/

Rivera Guevara, R. (Setiembre de 2018). *Detección y Clasificación de Malware con el Sistema de Análisis de Malware Cuckoo*. Obtenido de https://reunir.unir.net/bitstream/handle/123456789/7444/RIVERA%20GUEVARA%2cRICHARD%20PAUL.pdf?sequence=1&isAllowed=y

Security, C. f. (Mayo de 2021). *CIS Critical Security Controls Version 8*. Obtenido de https://www.cisecurity.org/controls/v8

Significados. (s.f.). *Que es metodología de la investigación*. Obtenido de https://www.significados.com/metodologia-de-la-investigacion/

Sophos. (Abril de 2021). *The State of Ransomware 2021*. Obtenido de https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

UNE 157001. (2002). *Criterios generales para la elaboración de proyectos.* Recuperado el 25 de abril de 2013, de Escuela Universitaria de Ingeniería de Vitoria: http://www.coiib.es/coiib/documentos/DocumentosContenidos/Gu%C3%ADa%20de%20elaboraci%C3%B3n%20de%20proyectos/2-Electricidad/5_PNE_157701_Criterios.pdf

Villacís Onofa, K. V. (Julio de 2018). *Propuesta Metodológica para un plan de continuidad de negocio alineada a la norma ISO/IEC 22301 y recuperación ante desastres en Cloud*. Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/19638/1/CD-9041.pdf

Virtus Total. (Octubre de 2021). *Ransomware in a Global Conext*. Obtenido de https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf

VMWARE. (s.f.). *Recuperación ante desastres como servicio (DRaaS)*. Obtenido de Recuperación ante desastres como servicio (DRaaS): https://www.vmware.com/es/topics/glossary/content/disaster-recovery-service-draas.html