UNIVERSIDAD FINIS TERRAE
FACULTAD DE INGENIERÍA
INGENIERÍA CIVIL EN INFORMÁTICA Y TELECOMUNICACIONES

PROTOCOLO PARA CIBERSEGURIDAD UTILIZANDO LA APLICACIÓN “AZURE” DE MICROSOFT

JORGE LUIS HUENCHÚN LÓPEZ

Trabajo de título presentado a la Facultad de Ingeniería de la Universidad Finis Terrae, para optar al Título de Ingeniero Civil en Informática y Telecomunicaciones.

Profesor Guía: Angélica Urrutia Sepúlveda

Santiago, Chile

2024-2025

DEDICATORIA

El presente trabajo se lo quiero dedicar con profundo amor, cariño y gratitud a mis padres, María López y Jorge Huenchún. Sin su amor, su fortaleza y su apoyo incondicional, no sería la persona que soy hoy, ustedes dos son mi ejemplo que seguir a diario, su historia de superación diaria, me dejan una vara muy alta de superar. Cada logró que alcanzo es también suyo. Gracias por sostenerme incluso en mis momentos difíciles y enseñarme de ellos, los cuales fueron aprendizaje para ayudarme a creer en mí, me demuestran que, con esfuerzo y dedicación, se puede alcanzar hasta el cielo.

A mi hermano Héctor Huenchún, cuya sabiduría de hermano mayor, compañía, comprensión y aliento constante han sido un pilar fundamental en mi vida. Gracias por impulsarme siempre a ser mejor, por acompañarme en cada decisión y por darme la confianza para enfrentar nuevos desafíos.

Y a mi pareja, Esmeralda Arteaga, por su motivación diaria, por creer en mi potencial incluso cuando yo dudaba, siendo un apoyo emocional constante en mi día a día. Gracias por estar, por acompañarme en cada paso y por inspirarme a seguir creciendo.

AGRADECIMIENTOS

Quiero agradecer en primera instancia a mi profesora guía Angélica Urrutia, decana de la facultad de ingeniería de la Finis Terrae quien fue la primera persona en creer en este proyecto y que, a pesar de estar colmada de alumnos ella me aceptó de igual forma, su paciencia, guía fue fundamental para finalizar de buena forma este trabajo, sin ella no hubiera podido ser posible. Este trabajo, además de ser guiado por la profesora, contó con la colaboración de dos expertos que sacrificaron su tiempo en revisar el trabajo sin poner ningún tipo de problema, primero agradecer a Nicolás Espinoza, arquitecto de ciberseguridad quien en muy breve tiempo me entrego un feedback positivo y correctivo de ciertos elementos, también a Yenny Méndez, Directora de Carrera Computación e Informática y Data Science de la Universidad Mayor que gracias a ella también se pudo llevar a cabo con ayudar a la corrección de elementos en todo el proyecto.

No puedo dejar de lado a todos mis amigos que me apoyan constantemente. Amigos que tengo desde el colegio y que, a pesar del tiempo aún me siguen apoyando, que el mismo tiempo ha demostrado que son mis mejores amigos, sin duda la distancia y las responsabilidades que conlleva realizar un trabajo de título como este llevó a no verlos mucho tiempo, aun así, todo es igual que siempre, Gracias Francisco Castillo, Juan Pablo Castillo, Darlene Sobarzo, Alen Garces, Felipe Cifuentes, Andreas Marín y todos los que me apoyan incondicionalmente.

Mis amigos que conocí en esta aventura universitaria Matías Urbina, Oscar Maldonado, Matías Alarcón y Ariel Arteaga, un grupo que, juntos, pueden con todo y siempre han estado presentes, desde la vida universitaria, hasta la vida diaria y las celebraciones. Finalmente agradecer a todos los compañeros que siempre creyeron, confiaron durante todo este proceso, conocí gente fantástica.

A pesar de haber dedicado este trabajo a mi familia y mi pareja, no quiero dejar de lado agradecerles a ellos por estar siempre presentes y ser pilares fundamentales.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS E ILUSTRACIONES

RESUMEN

Este trabajo desarrolló un protocolo de ciberseguridad en la nube implementado en Microsoft Azure, con el propósito de establecer un marco adaptable y metódico que fortalezca la protección de datos en entornos propios de nube. La propuesta surgió ante la creciente acogida de los servicios en la nube y las dificultades observadas en la gestión de accesos, la clasificación de información, trazabilidad de incidentes y el cumplimiento normativo.

El protocolo se diseñó conforme a los estándares internacionales ISO/IEC 27001, NIST SP 800-53, GDPR y junto a la legislación chilena sobre la protección de datos personales. La estructura se modeló mediante BPMN, organizando el flujo en seis fases que integraron controles técnicos basados en herramientas nativas de Azure como Microsoft Entra ID, Key Vault, Defender for Cloud y Log Analytics.

Durante el desarrollo, se aplicó una metodología combinada entre Kanban y Lean que permitió gestionar las tareas de forma visual, eliminando redundancias y priorizando actividades de mayor valor. La implementación práctica se ejecutó utilizando una suscripción gratuita de Azure, lo que permitió validar la operatividad del modelo e identificar limitaciones asociadas a funciones avanzadas. Aun así, mostraron resultados de un 83% de cumplimiento respecto de las configuraciones planificadas, demostrando su factibilidad técnica dentro del entorno disponible.

En otras palabras, el protocolo demostró que es un modelo modular, replicable y alineado con buenas prácticas internacionales, capaz de fortalecer la postura de ciberseguridad de las organizaciones que operen en la nube y sentó bases claras para futuras ampliaciones bajo suscripciones empresariales completas.

ABSTRACT

This work developed a cloud cybersecurity protocol implemented on Microsoft Azure, with the purpose of establishing an adaptable and methodical framework to strengthen data protection in cloud environments. The proposal arose from the growing adoption of cloud services and the difficulties observed in access management, information classification, incident tracking, and regulatory compliance.

The protocol was designed in accordance with the international standards ISO/IEC 27001, NIST SP 800-53, GDPR, and Chilean legislation on the protection of personal data. The structure was modeled using BPMN, organizing the workflow into six phases that integrated technical controls based on native Azure tools such as Microsoft Entra ID, Key Vault, Defender for Cloud, and Log Analytics.

During development, a combined Kanban and Lean methodology was applied, allowing for visual task management, eliminating redundancies, and prioritizing higher-value activities. The practical implementation was executed using a free Azure subscription, which allowed for validation of the model's operability and the identification of limitations associated with advanced features. Even so, it showed 83% compliance with the planned configurations, demonstrating its technical feasibility within the available environment.

In other words, the protocol proved to be a modular, replicable model aligned with international best practices, capable of strengthening the cybersecurity posture of organizations operating in the cloud and establishing a clear foundation for future expansion under full enterprise subscriptions.

1. INTRODUCCIÓN.

El presente capítulo tiene el propósito de contextualizar el problema de investigación, destacando la relevancia que tiene la ciberseguridad en entornos corporativos altamente digitalizados. Por lo que se describen los principales desafíos asociados a la protección de datos sensibles, los riesgos derivados de incidentes de seguridad y la necesidad de implementar un protocolo que busque fortalecer las infraestructuras de seguridad tecnológica de la organización. Además, se justifica el estudio y se sientan las bases conceptuales que permiten comprender la importancia de diseñar un marco de seguridad en la nube alineado con estándares internacionales y bajo las leyes chilenas.

1.1 Situación del problema

En un entorno corporativo donde la digitalización es fundamental para el desarrollo de las operaciones, una empresa del sector financiero enfrenta un incidente de seguridad que compromete la confidencialidad y disponibilidad de su información. La organización detecta accesos no autorizados a su sistema de gestión de clientes, lo que sugiere una posible brecha de seguridad que pone en riesgo datos sensibles, incluyendo información bancaria y personal de los usuarios.

Ante esta situación, la implementación de ciberseguridad robusta y el uso de Azure desempeñan un papel crucial para mitigar el impacto del ataque y fortalecer las defensas de la empresa. La implementación de Defender for Cloud (ver Capítulo 3) permitirá evaluar la infraestructura de seguridad en tiempo real, identificando vulnerabilidades y proporcionando recomendaciones para reducir el riesgo de nuevas intrusiones. Microsoft Defender for Cloud brindará protección contra ataques avanzados mediante la detección temprana de amenazas y la respuesta automatizada para contener posibles daños. Dicho lo anteriormente IBM realiza un reporte anual que ha sido ampliamente citado, el cual detalla los principales vectores de ataque, las industrias más atacadas y tipos de malware. Esta información ayuda a contextualizar la necesidad de un protocolo de ciberseguridad, en la ilustración 1 se muestra el ranking de los principales ataques maliciosos según el archivo de origen.

Diversas instituciones confirman que pdf como formato es uno de los más utilizados a nivel empresarial, gubernamental y académico, explicando su presencia constante en flujos de trabajos críticos, esto según Adobe, quien lo define como “the world´s most widely used file format for delivering documents” (Adobe, s.f.). Según el informe de IBM los archivos PDF concentran el 45,2% de los intentos de ataques detectados, seguidos por archivos HTML y zip. Este dato evidencia la necesidad de políticas de clasificación y protección activa de datos según su tipo de formato (IBM, 2025).

La ilustración 2 que también proviene del informe de IBM, muestra la distribución de incidentes registrados en las distintas regiones del mundo, reflejando cómo la frecuencia y el tipo de ataque varían según el continente.

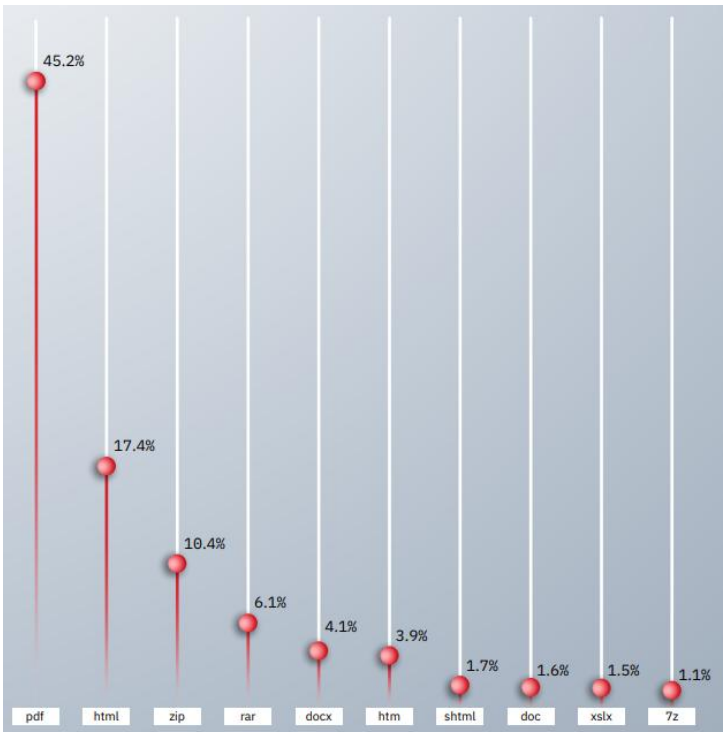

Ilustración 1: Tipo de archivos más vulnerables ante ciberataques Obtenida de: (IBM, 2025)..

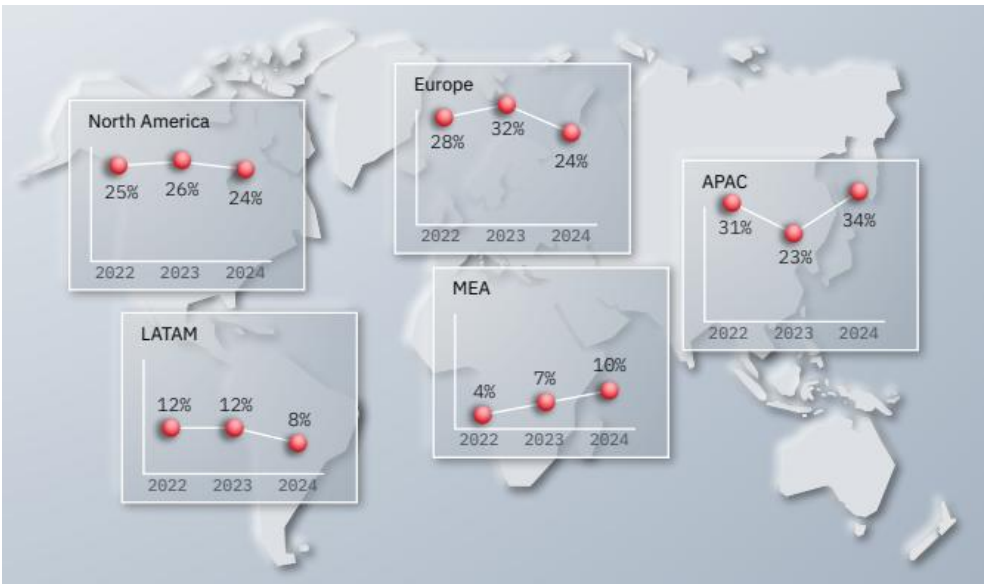

Ilustración 2: Distribución de incidentes de seguridad por continente. Obtenida de: (IBM, 2025).

En el contexto nacional, Entel realiza también un reporte anual de ciberseguridad, en este caso, publicando la 5ta edición del año 2025. En la ilustración 3 se muestra un aumento sostenido de ataques de ransomware en la región de Latinoamérica (Entel, 2025).

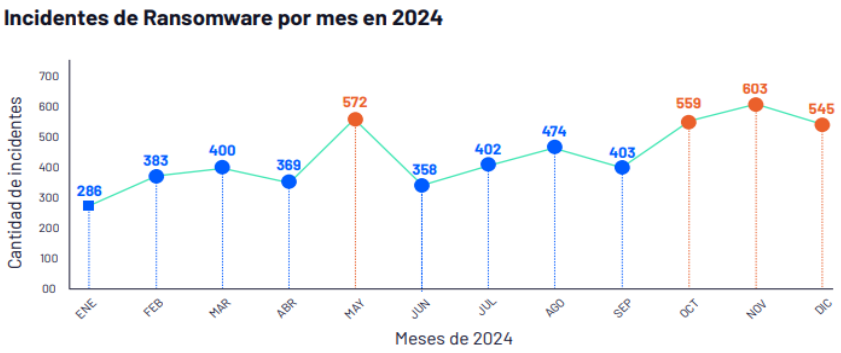

Ilustración 3: Incidentes de ransomware por mes en Latinoamerica (2024). Obtenida de: (Entel, 2025).

En la ilustración 3 se muestra el pico máximo en noviembre con más de 600 casos reportados en solo ese mes. Reflejando una amenaza constante y creciente que requiere un monitoreo y respuesta automatizada. En el caso de los incidentes de seguridad en la nube Entel también dice que el 61% de las organizaciones reporto haber experimentado incidentes de seguridad en la nube durante los últimos 12 meses, representando un aumento del 24% del año anterior. Además, para ayudar a contextualizar el panorama actual, la ilustración 4 menciona cinco tendencias dominantes en ataques a entornos Cloud y SaaS.

Ilustración 4: Tendencias más notables de amenaza en la nube y SaaS. Obtenida de: (Entel, 2025).

El escenario de la ilustración 4 obliga a reforzar controles de identidad y acceso, endurecer la superficie de ataque, monitorear y automatizar la respuesta y proteger los datos con cifrados. Adicionando cuantificación de riesgo con estadísticas recientes sobre ciberataques a infraestructuras en la nube o el costo promedio de una brecha de datos.

Es importante conocer la situación actual y los costos que puede implicar un ataque que genere que los datos se filtren dentro de una empresa, según un informe anual de IBM encuentra que una brecha de datos cuesta actualmente a las organizaciones estadounidenses un promedio de 10,22 millones de dólares, lo que representa un aumento del 9 % respecto al año anterior, expresando la variación del costo promedio (monto absoluto) entre dos periodos, no son magnitudes comparadas entre sí, si no tasa de cambio vs valor (Kapko, 2025). Además, otro reporte de IBM complementa este análisis al indicar que el coste medio mundial de una vulneración de datos alcanzó un promedio de 4,88 millones de dólares registrado el 2024 (IBM, 2025).

Luego de conocer el costo promedio de una brecha en los datos es importante conocer la gravedad de ciberataques en la nube, según SentinelOne “El mayor desafío para seguridad en la nube es una falta de capacitación y concientización sobre la seguridad cibernética en la gestión de soluciones de seguridad en la nube”. Adicionalmente se menciona “El 80% de las empresas ha encontrado un aumento en la frecuencia de los ataques en la nube, el 33% puede atribuirse a violaciones de datos en la nube, 27% a ataques de intrusión ambiental, el 23% a minería criptográfica y el 15% de los ataques comprenden auditorias fallidas”. Es importante que “Los servidores son los objetivos principales del 90% de las violaciones de datos, los servidores de aplicaciones web basados en la nube son los más afectados” (SentinelOne, 2025).

SentinelOne muestra que las configuraciones en la nube representan uno de los principales riesgos de seguridad en entornos públicos, ya que cerca del 23% de los incidentes están directamente relacionados con este problema y el 27% de las empresas han experimentado violaciones en su infraestructura por errores de configuración. La mayor parte de estas fallas que son el 82% se debe a errores humanos y no defectos de software, lo que evidencia la falta de visibilidad y control de la gestión de los recursos. Dentro de los problemas más comunes destacan las configuraciones inadecuadas de identidad y acceso, claves API inseguras, ausencias de monitoreo de seguridad y copias de respaldo mal implementadas (SentinelOne, 2025).

1.2 Planteamiento del problema

El análisis previo logra evidenciar un aumento constante de los incidentes de ciberseguridad y la falta de protocolos integrales que orienten la aplicación de herramientas de defensa en la nube. Por esto a continuación se ejemplifica una situación que refleja la problemática central de este estudio y las soluciones parciales disponibles actualmente.

Para controlar el acceso no autorizado, Microsoft Entra ID (ver Capítulo 3) se utilizará para reforzar la autenticación y centralizar la gestión de identidades, aplicando medidas como el acceso condicional y la autenticación multifactor. Adicionalmente, Privileged Identity Management (ver Capítulo 3) restringirá y auditará los accesos con privilegios elevados, evitando la exposición de credenciales comprometidas y minimizando la posibilidad de que los atacantes obtengan acceso a información crítica.

La protección de los datos será una prioridad en la respuesta a este incidente. Azure Key Vault (ver Capítulo 3) garantizará que las claves de cifrado y credenciales sean almacenadas de manera segura, evitando su exposición en caso de ataques. Azure Information Protection (ver Capítulo 3) permitirá la clasificación y protección de documentos sensibles, impidiendo su acceso por usuarios no autorizados y asegurando que los datos no sean filtrados. Además, Azure Purview (ver Capítulo 3) facilitará la identificación de información sensible dentro de la infraestructura, ayudando a evaluar el impacto del ataque y a reforzar las políticas de gobernanza de datos.

En la fase de monitoreo y respuesta ante el incidente, Azure Sentinel (ver Capítulo 3) desempeñará un papel clave al analizar registros de seguridad y detectar patrones anómalos que puedan indicar nuevas amenazas. Azure Monitor y Azure Log Analytics (ver Capítulo 3) permitirán supervisar el comportamiento de la infraestructura en tiempo real, generando alertas en caso de detectar actividades sospechosas. La implementación de Just-In-Time VM Access reducirá la exposición de las máquinas virtuales a ataques, asegurando que solo se otorgue acceso cuando sea estrictamente necesario.

Para garantizar la integridad de las comunicaciones y evitar futuros ataques similares, se adoptarán protocolos avanzados de seguridad. Transport Layer Security garantizará la protección de los datos en tránsito mediante cifrado avanzado, evitando la interceptación de información durante su transmisión. HTTP Strict Transport Security asegurará que todas las conexiones sean seguras, eliminando el riesgo de ataques de intermediarios que puedan comprometer la privacidad de los datos.

Gracias a la rápida identificación del incidente y la aplicación de las herramientas de seguridad de Azure, la empresa podrá contener la amenaza, mitigar el impacto en la información comprometida y fortalecer su infraestructura digital. La adopción de estas medidas permitirá que la organización continúe operando de manera segura y confiable, reduciendo la posibilidad de futuros ataques y asegurando la protección de los datos de sus clientes.

Expuesto todo lo anterior, el panorama evidencia que las organizaciones independientemente de su rubro enfrentan un escenario de creciente riesgo en la nube, siendo afectados con costos elevados de brechas de datos, incidentes asociados a configuraciones erróneas y carencia de procesos estandarizados para gestionar identidades y proteger la información. Aunque Microsoft Azure dispone de múltiples herramientas de seguridad, el problema central se concentra en una ausencia de un protocolo integral, el cual oriente su implementación de manera sistemática, la idea principal es reducir errores humanos, garantizando el cumplimiento normativo y fortaleciendo la resiliencia frente a ciberataques. Esta brecha justifica la necesidad de proponer un protocolo de ciberseguridad en la nube basado en BPMN y RBAC (ver Capítulo 3) que sea capaz de integrar prácticas técnicas y organizacionales en un modelo aplicable a diversos contextos corporativos. En síntesis, el problema que aborda esta investigación es la ausencia de un protocolo integral y sistemático que oriente la implementación de medidas de ciberseguridad en entornos de nube, permitiendo reducir errores humanos, fortalecer la resiliencia organizacional y garantizar el cumplimiento normativo.

1.3 Solución propuesta

Luego de conocer los problemas y la situación actual para realizar este proyecto, para abordar esta implementación en el entorno de la ciberseguridad en la nube, se propone diseñar un protocolo de seguridad y privacidad de los datos en Microsoft Azure.

Es necesario descubrir que herramientas teóricas se deben de manejar para este proyecto, en primera instancia es importante conocer la criptografía para la protección de datos de tránsito y en reposo, incluyendo el algoritmo de encriptación AES (Advanced Encryptation Estándar) y RSA (ver Capítulo 3) para asegurar la confidencialidad de los datos. En segundo lugar, realizar un modelo de control de acceso, el RBAC permite asignar funciones y autorizaciones en la infraestructura informática de una organización, en otras palabras, controla que usuarios pueden acceder, ver, realizar dentro del sistema TI (cloudflare, 2024). Por último, como se ha recalcado con anterioridad es importante conocer las normativas y regulaciones que se aplican en la protección de los datos para asegurar el cumplimiento de la ley, como se vio con anterioridad se propone visualizar las normas ISO y SSAE18/ISAE 3402 (ver Capítulo 3) que también son aplicables en el ecosistema de Microsoft Azure.

Considerando los estándares descritos en el marco teórico, se plantea diseñar un protocolo de ciberseguridad utilizando el NIST Cybersecurity Framework (NIST CSF) (ver Capítulo 3). Se compone de cinco funciones principales que operan de manera simultánea: Identificar, Proteger, Detectar, Responder y Recuperar.

Los resultados esperados de este proceso son que el modelo cumpla con todas las normativas previamente establecidas, garantizando así la privacidad de los datos de los usuarios. Se busca mejorar la seguridad de los datos, reduciendo los riesgos asociados con su posible filtración. Además, se espera aumentar la confianza de la empresa al implementar este modelo en su organización, permitiendo una respuesta proactiva ante cualquier incidente. La solución propuesta también debe transmitir transparencia a la organización, proporcionando claridad sobre lo que ocurre en su interior.

Con el transcurso de la investigación para utilizar Google BI, se encuentra la herramienta de Microsoft Azure, la cual representa una alternativa que demuestra ser más robusta que la primera herramienta mencionada, esto debido a su integración nativa con herramientas propias del ecosistema de Microsoft, facilitando un flujo de trabajo eficiente y sin fricciones de parte de algún programa. A su vez Azure ofrece servicios avanzados de inteligencia artificial y machine learning preparados para ser utilizados sin mucha dificultad, demostrando que su arquitectura está diseñada para escalar sin problemas desde proyectos pequeños hasta grandes proyectos, permitiendo una conectividad directa y segura con base de datos locales, en la nube y APIs, garantizando un control y flexibilidad de la información.

En consecuencia, la implementación de un protocolo de ciberseguridad basado en Microsoft Azure permitirá gestionar riesgos, detectar amenazas y aplicar medidas preventivas y correctivas que aseguren la confidencialidad, integridad y disponibilidad de la información dentro de la organización. Para ello, se utilizarán herramientas avanzadas que proporcionen una supervisión continua y una defensa eficaz contra posibles vulnerabilidades y ataques.

Defender for cloud será una pieza clave en este enfoque, ya que evaluará constantemente el estado de seguridad de la infraestructura y ofrecerá recomendaciones para mitigar riesgos. Junto con esto, Microsoft Defender for Cloud protegerá los entornos híbridos mediante inteligencia artificial y monitoreo en tiempo real, mientras que Azure Sentinel, como plataforma SIEM, facilitará la identificación y gestión de incidentes de seguridad a través del análisis de grandes volúmenes de datos.

La gestión del acceso a los sistemas será un componente esencial dentro del protocolo de ciberseguridad. Microsoft Entra ID centralizará la administración de identidades, garantizando autenticación multifactor y acceso condicional para evitar accesos no autorizados. Además, el uso de Privileged Identity Management permitirá restringir y auditar los accesos con privilegios elevados, minimizando el riesgo de compromisos de seguridad.

Para asegurar la protección de datos sensibles y el cumplimiento de normativas internacionales, se integrarán diversas soluciones. Azure Key Vault proporcionará un almacenamiento seguro para claves de cifrado, contraseñas y certificados, mientras que Azure Information Protection clasificará y protegerá la información confidencial para prevenir filtraciones. Asimismo, Azure Purview facilitará la identificación y gobernanza de los datos dentro de la organización, garantizando el manejo adecuado de la información.

El monitoreo y la respuesta ante incidentes serán aspectos fundamentales para reforzar la seguridad. Azure Monitor y Azure Log Analytics permitirán una supervisión en tiempo real, generando alertas en caso de detectar anomalías en la infraestructura. Adicionalmente, la implementación de Just-In-Time VM Access (ver Capítulo 3) controlará el acceso a máquinas virtuales, reduciendo la exposición a posibles ataques y asegurando que los accesos sean otorgados solo cuando sea necesario.

Como parte de las estrategias de protección, se aplicarán estándares avanzados de cifrado y seguridad en las comunicaciones. El uso de Transport Layer Security (ver Capítulo 3) garantizará la protección de los datos en tránsito mediante cifrado avanzado, mientras que HTTP Strict Transport Security (ver Capítulo 3) reforzará la seguridad en las conexiones, evitando ataques de intermediarios y asegurando la integridad de la información transmitida.

La implementación de este protocolo basado en Azure proporcionará a la organización una infraestructura tecnológica robusta, capaz de afrontar los desafíos de ciberseguridad actuales. Con estas medidas, se reducirá el riesgo de amenazas, se optimizará la gestión de accesos y se garantizará la continuidad operativa en un entorno digital seguro y confiable.

En este trabajo la solución propuesta consiste en el diseño de un protocolo de carácter general y modular de ciberseguridad en la nube implementado en la plataforma Microsoft Azure, modelando procesos con notación BPMN y con gestión de accesos basada en roles RBAC (ver Capítulo 3). Este protocolo posee herramientas nativas de Azure (Active Directory, Key Vault, Monitor, Sentinel, Backups, etc) y con los principios de seguridad internacionales y nacionales, logrando además una estandarización de la clasificación de datos, reforzando los controles de identidad, cifrados robustos, monitoreo continuo y garantizando respaldo y recuperación ante incidentes. De esta manera, se ofrece un marco conceptual adaptable diversas organizaciones que utilicen servicios en la nube, manteniendo su implementación práctica orientada al ecosistema de Microsoft Azure, este protocolo busca reducir errores de configuración, asegurando cumplimiento normativo y fortaleciendo la resiliencia frente a amenazas en entornos cloud.

1.4 Objetivos

Objetivo General

Proponer un protocolo de seguridad de los datos para la adecuada implementación de soluciones con la plataforma “Azure”.

Objetivos Específicos

1. Seleccionar distintos procesos y secuencias lógicas que permitan un ciclo eficiente en un protocolo de ciberseguridad en la nube.
2. Modelar el protocolo de seguridad de datos en Microsoft Azure utilizando notación BPMN y políticas de acceso.
3. Implementar y evaluar medidas técnicas del protocolo en un entorno controlado de Azure.
4. Depurar el protocolo, formulado en el objetivo 2, con evaluación de un experto de ciberseguridad, de acuerdo con los errores identificados en el objetivo 3.

1.5 Alcances y limitaciones

En una primera instancia, se había considerado la opción de trabajar este proyecto utilizando Google BI como herramienta principal, sin embargo, al analizar con mayor profundidad los objetivos del trabajo, se descartó esta alternativa ya que Google BI, por su naturaleza, está orientado principalmente al análisis y visualización de datos, sin ofrecer las capacidades necesarias para diseñar un protocolo completo de ciberseguridad. En otras palabras, su alcance se habría limitado a generar reportes o métricas de la información, pero no habría permitido implementar controles, políticas ni procedimientos técnicos orientados a proteger los datos sensibles de forma integral. Por este motivo se decidió optar por la plataforma Microsoft Azure, que ofrece un conjunto de servicios específicamente pensados para la gestión de identidad, acceso, cifrado, respaldo, monitoreo y cumplimiento normativo.

El proyecto se enfoca en diseñar e implementar un protocolo de ciberseguridad en la nube, utilizando herramientas nativas de Azure para cubrir de forma estructurada las distintas fases necesarias para resguardar la información. Su alcance considera la definición de políticas de acceso basadas en roles, el uso de autenticación multifactor, el cifrado de datos tanto en reposo como en tránsito, la configuración de respaldos cifrados, replicados y el desarrollo de mecanismos para la detección de fugas de datos y el monitoreo continuo de eventos de seguridad. Microsoft Azure resultó una plataforma que desplazó de inmediato a Google BI ya que logra cubrir controles de seguridad, por lo que la implementación se termina realizado en Microsoft Azure.

1.5.1 Alcances

El desarrollo de este protocolo tiene como alcance principalmente protocolo de seguridad de los datos para la adecuada implementación de soluciones con la plataforma “Azure”. La idea es poder construir un modelo integral que abarque desde la clasificación de datos hasta el respaldo y la recuperación ante desastres, pasando por controles de acceso, cifrado, monitoreo y cumplimiento, para así ofrecer una propuesta que pueda servir de base a quienes quieran reforzar su seguridad en entornos cloud.

Para lograr esto, se trabajó directamente en la plataforma de Azure, configurando servicios reales y probando su integración para validar la viabilidad de cada fase. Todo se realizó en un entorno de demostración, pensado para replicar lo más fielmente posible las condiciones que podría tener una empresa real, aunque sin aplicar el protocolo en producción ni con datos sensibles de una organización específica. Esto significa que el resultado final no es solo un documento teórico o una propuesta en papel, sino que existe una implementación técnica concreta que demuestra que el modelo será factible de aplicar.

El protocolo está estructurado para aprovechar las capacidades nativas de Azure, permitiendo construir por capas los diferentes controles de seguridad. Por ejemplo, se contempla el uso de herramientas para autenticar a los usuarios con múltiples factores, gestionar permisos con mayor granularidad, cifrar la información tanto en reposo como en tránsito, generar copias de seguridad automatizadas y configurarlas para que estén disponibles incluso si ocurre un desastre, además, se incluye la capacidad de monitorear y registrar eventos de seguridad, habilitar alertas tempranas y facilitar las revisiones periódicas para cumplir con normativas y buenas prácticas.

Una de las ventajas de plantear el protocolo de esta forma es que se evita la necesidad de invertir en infraestructura física local, ya que todos los servicios corren en la nube esto puede facilitar la adopción para empresas de distintos tamaños.

Es importante considerar que, si bien el protocolo está completamente implementado en un entorno de prueba y validado de forma técnica, para que pueda ser usado en una empresa real será necesario adaptarlo a las necesidades específicas de cada organización, sus datos y procesos. Será importante analizar cada caso particular, ajustar configuraciones, capacitar a los equipos involucrados y mantener las revisiones de forma constante para garantizar su eficacia en el tiempo.

1.5.2 Limitaciones

El desarrollo de este protocolo presenta diversas limitaciones que deben ser consideradas tanto en su aplicación práctica como en el contexto de este trabajo de título.

En primer lugar, al tratarse de un servicio de pago, se requiere obligatoriamente contar con una suscripción activa en Azure para poder habilitar todas las herramientas necesarias, en mi caso particular, esto significó una limitante importante puesto que se tuvo que migrar el desarrollo completo a otra cuenta con capacidad de pago, obligándome a rehacer la configuración desde cero para poder concretar el protocolo. Esto implicó un mayor consumo de tiempo y recursos, además de la necesidad de planificar cuidadosamente cada paso para evitar costos innecesarios.

El protocolo, además, ha sido diseñado de forma exclusiva para el ecosistema de Azure. Esto representa una dificultad relevante si se considera la posibilidad de migrar a otra nube o a infraestructura local en el futuro, ya que las herramientas, formatos y sistemas implementados dependen directamente de Azure, limitando la portabilidad y dificultando la interoperabilidad o la auditoría externa en otros entornos. Sin embargo, la estructura modular del protocolo permite adaptar sus principios generales de control, monitoreo y gestión de acceso a otras plataformas cloud en futuros desarrollos. También, lo que garantiza su eficiencia en este entorno, surge una interrogante clave ¿Cómo puede este protocolo ser implementado en organizaciones que utilizan otros ecosistemas de nube como AWS o Google Cloud? ¿cómo se garantiza la reducción de errores de configuración? En

este contexto sería importante adaptar ciertos componentes del protocolo, como las políticas para el acceso o el cifrado a otras plataformas sin comprometer su efectividad.

Asimismo, el acceso a los sistemas y servicios diseñados depende de la conectividad a Internet y de la disponibilidad de la nube de Azure. Esto puede ser un problema significativo para organizaciones que no cuenten con acceso estable o de alta calidad, y representa un riesgo adicional en caso de interrupciones masivas del servicio de Azure o del Internet en Chile, comprometiendo la disponibilidad de sistemas críticos y afectando la continuidad del negocio.

Otro aspecto importante es la complejidad técnica del propio protocolo. A pesar de que Azure ofrece herramientas muy completas y flexibles, su correcta implementación requiere de un profesional con experiencia avanzada en la plataforma. Configuraciones incorrectas pueden derivar en brechas de seguridad no intencionales o en el incumplimiento de requisitos legales, elevando el riesgo operacional.

Es importante mencionar también que existen consideraciones legales y establecidas relevantes. Microsoft, como proveedor de Azure, se encuentra principalmente bajo la jurisdicción de Estados Unidos, lo que puede dificultar o ralentizar la supervisión jurídica chilena en caso de disputas legales o incidentes de seguridad graves. Además, los acuerdos de servicio de Microsoft suelen incluir cláusulas que limitan su responsabilidad ante pérdidas económicas, legales o reputacionales del cliente en caso de un incidente de ciberseguridad, lo cual debe ser conocido y evaluado antes de adoptar completamente este protocolo.

2. ESTADO DEL ARTE.

Este capítulo recopila y analiza trabajos relacionados con la ciberseguridad en entornos de nube, en particular con la herramienta trabajada en este proyecto, en particular en Microsoft Azure. El objetivo es establecer una base comparativa y teórica que permita identificar limitaciones, avances o vacíos en el desarrollo de protocolos de seguridad que combinen marcos normativos, metodologías organizacionales y servicios nativos de los principales proveedores cloud.

Los trabajos revisados se presentan en orden temáticos y cronológico, iniciando con investigaciones centradas en la infraestructura de seguridad, continuando con análisis de auditorías técnicas y finalizando con estudios experimentales de respuesta ante incidentes. Posteriormente, se integra una comparación entre Azure, AWS, Google Cloud Plataform y Oracle Cloud, así como una síntesis de métricas de comparación y vacíos identificados.

2.1 Infraestructura de seguridad en la nube de Azure.

Este trabajo se centra en la seguridad en la nube de Microsoft Azure, se analiza la infraestructura de seguridad en Microsoft Azure y propone una herramienta automatizada para identificar y mitigar vulnerabilidades, analiza conceptos básicos de la nube, riesgos de seguridad, servicios de Azure y prácticas recomendadas de implementación. En esta memoria también se crea una herramienta portatil en PowerShell llamada “AzInfraSec” que sirve para auditar y asegurar entornos de Azure, incluyendo la automatización de tareas de seguridad y la generación de informes, el trabajo identifica una vulnerabilidad en los privilegios de lectura de Azure Active Directory de la UOC (Universidad Oberta de Catalunya). La investigación busca proporcionar una guía práctica y una herramienta para mejorar la postura de seguridad en la nube de Azure.

El autor menciona que en el trabajo realizado utiliza una metodología ágil, argumentando que de esta forma consigue mejoras incrementales en cada iteración dentro de todo el Sprint antes de la entrega final. Aunque este no es el único utilizado puesto que para realizar el seguimiento utiliza un Backlog con estilo Kanban que ofrece Azure DevOps, el cual permite visualizar las tareas a realizar con el debido peso y estado concreto de cada tarea, separándolas de 3 formas: Epics, Features y Tasks simples para completar el trabajo de forma ordenada.

Este trabajo detalla algunas limitaciones dentro de lo aplicado, una de estas es que a pesar de delegar la seguridad de la plataforma Azure, el cliente o la organización debe conocer en qué aspectos es responsable y capaz de proteger implicando así una limitación en la responsabilidad del proveedor y la necesidad de que el cliente asuma ciertas tareas y responsabilidades de seguridad. Una limitación importante surge al momento de migrar a la nube, puesto que esto trae tres dificultades, la primera es sobre migrar grandes bases de datos, que a pesar de tener herramientas ofrecidas por los proveedores cloud, puede igualmente ser una tarea difícil dependiendo de la cantidad y características de los datos; la gestión y cumplimiento normativo también plasma una limitación enlazada con la nube, puesto que por culpa de diversas leyes y normas de algunos sitios resulta ser una tarea sensible al no estar alojados en el cumplimiento normativo, por último la integridad de los datos al migrarlos deben de ser compatibles con los servicios o frameworks disponibles (López, 2023).

2.2 Análisis de ciberseguridad a una infraestructura de red implementada en Microsoft Azure.

Este estudio se realizó en la Fundación Universitaria Los Libertadores y presenta un análisis de ciberseguridad que esta realizado a una infraestructura de red con Microsoft Azure usando técnicas de hacking éticos, buscando identificar vulnerabilidades en la red, conocer los componentes y configuraciones para determinar el nivel de seguridad que tiene la infraestructura en la nube. Las herramientas utilizadas son NMAP y NESSUS para realizar escaneos externos e internos, revelando diversas vulnerabilidades y la exposición de información incluyendo también las herramientas de seguridad propias de Microsoft Azure.

El análisis se basa en una metodología cuantitativa, la cual tiene como objetivo explicar mediante una investigación sistemática los fenómenos que se van observando, la cual implica la recopilación y análisis de datos cuantificables, que en este caso es la ciberseguridad en la infraestructura de red en la plataforma Azure. El autor menciona que para el proceso se escanea con un plan de auditoría que puede ser viable como guía metodológica, identificando amenazas, riesgos y acciones de mejora.

Al final el trabajo se determina que tiene varias limitaciones, para comenzar menciona el alcance limitado a un modelo IaaS en Azure, esto significa que las conclusiones y vulnerabilidades identificadas pueden no ser directamente aplicables a otros modelos de servicios en la nube tales como PaaS o SaaS, ni a otras plataformas de nube como de Cloud de Google o AWS de Amazon. La segunda limitación es la dependencia de herramientas, ya que el análisis fue realizado principalmente con las herramientas de hacking ético NMAP y NESSUS a pesar de que son herramientas robustas son limitadas con cierto tipo de vulnerabilidades. Finalmente, al estar enfocado principalmente en vulnerabilidades técnicas, esto supone un limitante principal en la identificación de vulnerabilidades técnicas en la infraestructura y sus componentes, el análisis en si no profundiza en estas áreas, ni en aspectos como la seguridad a nivel de aplicaciones o la gestión de identidades y accesos de manera exhaustiva (Gallego, 2023).

2.3 Incident Response to Brute-Force Attack: A Study of Azure and Traditional Approaches.

Esta tesis se realizó en LAB University of Applied Sciences, Finlandia, la cual examina la respuesta a ataques de fuerza bruta, comparando enfoques en Azure y sistemas tradicionales de código abierto. El estudio evalúa dos entornos de prueba aislados, uno integrado con servicios de Azure y otro utilizando la aplicación Fail2Ban que, mediante simulaciones con Hydra, logra comparar los tiempos de detección de respuesta, así también comparando el uso de recurso y precisión de los dos sistemas.

En el trabajo se utilizaron dos metodologías, experimental y comparativa, con el fin de poder implementar y evaluar el rendimiento de dos entornos de sandbox aislados en respuesta a ataques de fuerza bruta simulados dividiéndolo en cuatro etapas para asegurar pruebas seguras de aplicación sin afectar los sistemas de producción, las etapas son las siguientes, Entorno de prueba, Simulación de ataque de fuerza bruta, respuesta al ataque de fuerza bruta y recolección de datos, análisis y evaluación.Este proceso no está exento de limitantes y dificultades, de hecho, se detallan seis

importantes, donde el enfoque se centró únicamente en ataques de fuerza brutas simulados, restringiendo la aplicación de los resultados ante otras amenazas, entornos los cuales, si bien son seguros, no logran reproducir con precisión la complejidad de un sistema real. También se evidencia variabilidad en los tiempos de respuesta del sistema auto hospedado, posiblemente por cambios en la carga o condiciones que pueda tener la red de la empresa. Además, la investigación al estar limitada con Azure y el sistema auto hospedado, no considera otras aplicaciones, plataformas o configuraciones hibridas. Por último, a pesar de realizar múltiples pruebas, se sugiere usar conjunto de datos más amplios que puedan fortalecer una mejor generación de los hallazgos (Phung, 2024).

2.4 Contribuciones identificados en la literatura.

Los trabajos revisados en este capítulo resultaron valiosos como punto de partida, ya que permitieron identificar tanto las herramientas más utilizadas en entornos Azure como NMAP, NESSUS o la automatización mediante PowerShell. Las metodologías de análisis y respuesta ante incidentes que han sido aplicadas en los distintos trabajos analizados, estos estudios aportaron lineamientos prácticos para la evaluación de vulnerabilidades, la importancia del monitoreo continuo y la necesidad de contar con marcos organizacionales que acompañen la dimensión técnica.

2.5 Enfoques organizacionales y metodológicos en la gestión de ciberseguridad.

Las herramientas técnicas ofrecen las distintas plataformas en la nube, también existen enfoques metodológicos y organizacionales que buscan mejorar la gestión de la ciberseguridad dentro de las empresas, los enfoques permiten integrar la parte técnica con gestión de procesos, logrando que la seguridad no dependa solo de las herramientas, sino también de la forma que se administran, modelan y ejecutan las políticas internas.

Dentro de los trabajos relevantes en este ámbito de las metodología es un trabajo realizado por la Universidad de Ingenieria y Tecnología de Pakistán en el año 2020, quienes proponen una extensión del modelo BPMN 2.0.2 para incorporar dentro de los diagramas de procesos los requisitos de seguridad necesarios durante el desarrollo de sistemas de información, Con esta propuesta se logra representar visualmente las actividades que se deben cumplir para los controles de seguridad, como validaciones de acceso, cifrado o respuesta ante incidentes, logrando que un BPMN se transforme en una herramienta útil no solo para modelar procesos de negocios sino también para procesos de seguridad (Zareen, 2020).

Por otra parte, en el ámbito de la gestión operativa, han surgido metodologías Lean IT y KanBan aplicadas en los equipos de ciberseguridad, pero este artículo ayuda a visualizar mejor las tareas críticas estableciendo prioridades bajo las tareas pendientes, estableciendo prioridad los incidentes y reducir los tiempos de respuesta ante amenazas. Además, facilitan la colaboración entre los equipos de monitore y respuesta, esto permite ver de manera clara los cuellos de botella y las tareas en progreso, promoviendo una mejora continua en la gestión de incidentes (Lark Editorial Team, 2024).

2.6 Comparación entre proveedores de nube.

Para este estudio es necesario conocer como están trabajando otro tipo de plataformas en el entorno Cloud que tienen como objetivo solucionar problemas de ciberseguridad, por lo que a

continuación se realiza un resumen de cómo trabajan estas herramientas con el propósito de comparar Microsoft Azure con estas mismas:

- **Google Cloud Platform (GCP):** Tiene su fuerte es la analítica e inteligencia artificial aplicada a seguridad con herramientas como Chronicle SIEM y Security Command Center.
- **Amazon Web Services (AWS):** Destaca por la madurez y amplitud de servicios como Security Hub, Shield y GuardDuty que están enfocados en la detección de amenazas y la automatización de respuesta.
- **Oracle Cloud Infrastructure (OCI):** Este se orienta principalmente a la protección de datos críticos y cumplimiento normativo con Data Safe y Cloud Guard.

Sin embargo, estas herramientas presentan en la literatura un protocolo metodológico integral que combine BPMN, RBAC y marcos normativos como el NIST o ISO/IEC 27001. A partir de esto el presente trabajo se diferencia precisamente al proponer un modelo híbrido que articula la tecnología con procesos organizacionales y de gobernanza.

2.7 Vacíos identificados en los trabajos previos.

Si bien los trabajos logran aportan antecedentes relevantes y valiosos sobre diagnósticos y herramientas de seguridad en los entornos cloud, aún presentan limitaciones que son relevantes a considerar. Uno de los principales vacíos identificados toma presencia con la ausencia de métricas e indicadores concretos y visibles que permiten medir la efectividad de la seguridad implementada. Con este proyecto, este punto se aborda mediante las funciones del NIST Cybersecurity Framework (identificación, protección, detección, respuesta y recuperación) además métricas de evaluación basadas en el nivel de cumplimiento de estas funciones y en reducción porcentual de incidentes detectados durante la fase práctica del protocolo propuesto dentro de la plataforma de Microsoft Azure.

Otro punto importante para considerar es la desconexión entre los marcos normativos internacionales y nacionales (respecto del país de estudio). La mayoría de los trabajos se concentran en tener configuraciones o vulnerabilidades sin articular las normas NIST o ISO/IEC 27001. En cambio, el presente estudio vincula explícitamente ambos niveles, asegurando trazabilidad entre las políticas organizaciones y las medidas técnicas aplicadas y esto sin considerar que también este estudio considera tener cumplimiento con la ley chilena.

Los estudios existentes se enfocan en casos o sectores específicos como instituciones educativas o redes cerradas, sin la opción de ofrecer un modelo que pueda ser replicado en distintos rubros. Este trabajo propone un protocolo modular adaptable a diversos tipos de organizaciones que operen en entornos cloud. Finalmente, los vacíos identificados justician el desarrollo de este protocolo de ciberseguridad en la nube basado en BPMN y RBAC, el cual integra marcos normativos, métricas de evaluación y validación práctica en un modelo universal aplicable a distintos contextos corporativos.

3. MARCO TEÓRICO.

En este capítulo se presentan los fundamentos teóricos y técnicos que sustentan el desarrollo del protocolo de ciberseguridad en la nube, se abordan los principales protocolos de comunicación de seguridad, los marcos normativos y legales aplicables y las herramientas tecnológicas de Microsoft Azure que permiten implementar las fases del modelo propuesto. El gran propósito de este apartado establecer una base conceptual sólida que respalde las decisiones técnicas y metodológicas del proyecto, asegurando la coherencia entre los estándares internacionales, la legislación nacional y las capacidades de la plataforma a utilizar.

3.1 Fundamentos de comunicación y seguridad.

Protocolo TCP/IP, que por sus siglas Control de Transmisión/Protocolo de Internet (TCP/IP) es un conjunto de normas que permite la comunicación entre dos equipos a través de Internet. Este protocolo asegura la exactitud de la información al dividir los datos en paquetes individuales, que son enviados y luego ensamblados nuevamente en su destino para reconstruir la información completa. Al dividir los datos en paquetes pequeños, se facilita mantener la precisión de la información en comparación con enviarlos todos de una vez, garantizando así que cada comunicación llegue intacta a su destino deseado (Chavez, 2024).

Protocolo HTTPS (Hypertext Transfer Protocol Secure), es una versión segura del protocolo HTTP, esto porque agrega cifrado, autenticación e integridad, HTTPS que utiliza SSL/TLS para el cifrado y la autenticación, permitiendo a los usuarios transmitir datos confidenciales con completa seguridad, permitiendo acciones importantes para grandes empresas ya que sin preocupaciones se pueden ingresar información bancaria, números de tarjetas de crédito y/o credenciales de inicio de sesión, de manera segura a través de Internet. Por esto, HTTPS se está estableciendo rápidamente como el protocolo estándar para todos los sitios web, independientemente si se intercambian datos confidenciales con los usuarios o no (SSL, 2025).

Protocolo de Transferencia de Archivos (FTP), determinado estándar para transferir archivos entre dos computadores, usualmente se utilizan servidores y clientes o computadores y servidores. Este protocolo, basado en un modelo cliente-servidor, implica que un programa servidor se ejecuta y espera conexiones de los clientes, quienes envían archivos al servidor a través de una conexión TCP (Chica, 2025).

Protocolo Secure Shell (SSH), permite conectarse a un computador de forma remota y ejecutar programas en él. Funciona parecido al inicio de sesión remoto usando una red privada virtual (VPN). A diferencia de otros protocolos SSH ofrece una conexión de red cifrada que se utiliza ampliamente para la transmisión segura de datos entre computadores. Este protocolo es muy versátil permite acceder una variedad de dispositivos, incluidos servidores web, almacenamientos en red, routers, WiFiS, entre otros. SSH puede utilizarse tanto para transferir archivos como para proporcionar inicios de sesión seguros y ejecución remota, siendo más seguro que otros protocolos como SFTP y FTP (Chica, 2025).

Protocolo (DNS), que significa Sistema de Nombres de Dominio, permite a los usuarios de Internet naveguen utilizando nombres de host en lugar de direcciones IP numéricas. Este protocolo facilita que los navegadores encuentren sitios web específicos. Una serie de funciones traducen la solicitud

de un cliente DNS de un nombre de host, como www.ejemplo.com, en la dirección IP adecuada, ya sea IPv4 o IPv6. Este proceso no solo autentica las direcciones IP, sino que también hace que Internet sea más accesible al convertir nombres de dominio personalizados en complejas direcciones numéricas (Quiroz-Vásquez, 2024).

Protocolo Transport Layer Security (TLS), es un protocolo criptográfico diseñado para proporcionar comunicaciones seguras por una red de computadoras, sus funciones principales en primer lugar encriptación ya que oculta los datos transferidos a por la red a un tercero, la autenticación logra garantizar que las partes intercambien información real, asegurando que los mensajes no se alteren.

Strict Transport Security (HSTS), Mecanismo de seguridad de política de seguridad para las páginas web diseñado para proteger las páginas webs HTTPS contra los ataques de degradación y secuestros de cookies. En resumen, este protocolo garantiza que los usuarios puedan acceder a la web a través de conexiones seguras, mejorando esta seguridad y reduciendo la posibilidad de ataques de terceros de forma maliciosa (ciberseguridad).

3.2 Modelos y marcos normativos.

C**iberseguridad,** es una colección de herramientas, conceptos de seguridad, enfoque de manejo de riesgos y tecnologías que son usadas para proteger el entorno y organizaciones del ciberespacio y a los usuarios activos (Unión Internacional de Telecomunicaciones, 2015).

Modelo Zero Trust, se basa en un paradigma "Nunca confíes, siempre verifica", ya sea con usuario, dispositivos o servicios, eliminando así el poder gozar de la confianza implícita, incluso dentro del perímetro organizacional. Este modelo propone una arquitectura centrada en autenticaciones continuas, segmentaciones estrictas y monitoreos continuos. Microsoft promueve este modelo sobre tres principios fundamentales: verificar explícitamente cada solicitud, aplicar el mínimo privilegio necesario y asumir que una brecha puede ocurrir en cualquier momento (Im, 2024). Su importancia es proteger a las aplicaciones web contra fugas de datos y otros ataques por el estilo, es común ver este estándar que protege a HTTPS en los sitios web (Cloudfire, 2024).

NIST, se basa en estándares, pautas y mejores prácticas que ayuden a las organizaciones a poder mejorar la gestión que pueden tener con los riesgos de ciberseguridad, este diseño tiene una flexibilidad que logra integrarse con los procesos actuales de seguridad dentro de cualquier empresa (IBM).

ISO/IEC 27001, Norma que se utiliza para establecer, implementar y mejorar un sistema de gestión de seguridad de la información, garantizando las buenas prácticas de seguridad de la información, esta norma permite que los datos suministrados sean confiables, íntegros, disponibles y legales para protegerlos de los riesgos que se puedan presentar (Pirani, s.f.).

Reglamento general de protección de Datos (GDPR), es una ley europea que entró en vigencia en el año 2018, que se encarga de la protección de la privacidad y los datos personales de los ciudadanos de la Unión Europea. Esta ley afecta a todas las empresas y organizaciones que procesan datos personales (University of miami health system, s.f.).

Ley 19.799, habla sobre Documentos Electrónicos, Firma Electrónica y servicios de certificación de firma, esta ley busca regular el uso tanto de los documentos y las firmas electrónicos en Chile, consiguiendo que estas tengan validez legal, consiguiendo que tenga la misma validez que los documentos en papel (Loyola, 2024).

Ley 19.628, menciona soy la protección de la vida privada y regula el tratamiento el tratamiento de datos personales, logrando establecer normas para la recolección, almacenamiento, procesamiento y uso de datos personales, buscando proteger la privacidad de las personas (Loyola, 2024).

Ley 21.459, establece normas sobre los delitos informáticos en Chile, derogando la ley 19.223 la cual tipificaba las figuras penales relativas a la informática que fue promulgada en el año 1993 ajustándola a la legalidad del convenio de Budapest (Loyola, 2024).

Ley 21.663, resguarda el marco de ciberseguridad y tiene por objetivo regular la normativa general aplicable a las acciones de ciberseguridad de los organismos del estado, establece los requisitos mínimos para enfrentar incidentes de ciberseguridad, las obligaciones y las atribuciones del estado, los deberes de las instituciones determinadas en la ley, como los mecanismos de control, supervisión y responsabilidad frente a infracciones (Loyola, 2024).

3.3 Notaciones y metodologías organizacionales.

Notación Business Process and Notation (BPMN), es un estándar que permite modelar procesos de negocio mediante diagrama de flujo tanto para el personal técnico y administrativo, esta notación facilita la documentación, el análisis y la mejora continua de los procesos para los negocios mediante los diagramas (Standards Development Organization, 2010).

Metodología Lean, se trata de un enfoque de gestión que busca optimizar procesos mediante la eliminación de tareas que no generan valor, reduciendo tiempos y recursos, la idea principal es mantener solo las actividades esenciales (Lean Enterprise Institute, s.f.).

Metodología Kanban, este enfoque se baja en un sistema visual de gestión del trabajo basado en tableros que muestran flujos de tareas desde su inicio hasta su finalización. Su propósito es optimizar el progreso de manera continua, logrando evitar sobrecargas en trabajos y lograr asegurar la trazabilidad de las actividades (businessmap, s.f.).

3.4 Gestión de acceso y protección de datos.

Modelo Role-Based Access Control (RBAC), es un método de control de acceso donde los permisos se asignan en función del rol del usuario dentro de una organización, el propósito de este modelo reduce errores humanos y evita accesos indebidos al aplicar el principio de mínimo privilegio (NIST, 2020).

Autenticación Multifactor (MFA), se trata de un mecanismo de seguridad que requiere dos o más factores de verificación para acceder a un sistema o recurso. Por lo general combinan algo que el usuario sabe de contraseñas con algo que posea con dispositivos y algo que puede ser biometría (Microsoft, s.f.).

Prevención de pérdida de datos (DLP), conjunto de políticas que permiten detectar, bloquear o alertar ante movimientos no autorizados de información sensible (Microsoft, s.f.).

Application Programming Interface (API), es un conjunto de reglas y protocolos que permiten la comunicación e integración entre aplicaciones los servicios. Estos se utilizan para automatizar configuraciones, recopilar datos y facilitar la interoperabilidad entre los distintos módulos del entorno (Goodwin, s.f.).

Customer-Managed Keys (CMK), son claves de cifrado administradas por el cliente dentro de Azure Key Vault, estas permiten a las organizaciones mantener control total sobre el cifrado de sus datos, cumpliendo con normativas de privacidad y auditoria avanzada (Microsoft, s.f.).

3.5 Servicios de Microsoft Azure.

Azure, es un ecosistema enorme, el cual posee múltiples herramientas para distintas áreas de la informática. Cada una de ellas tiene un propósito, desde computación, almacenamiento, hasta inteligencia artificial y seguridad, las cuales se detallarán solo las necesarias para este proyecto.

Microsoft Entra ID (Azure Active Directory), Brinda un servicio de identidad y gestión de accesos en la nube que permite autenticar usuarios y servicios. Dentro del protocolo es clave para implementar **Autenticación Multifactor (MFA)** acceso condicional y gestión de roles (RBAC), reduciendo el riesgo de accesos no autorizados y suplantación de identidad (LogicMonitor, 2024).

Azure Key Vault, permite entregar soluciones centralizadas para almacenar y gestionar secretos, claves y certificados de forma segura. Permite cifrar datos en reposo utilizando claves gestionadas por el cliente (CMK) y aplicar políticas de acceso granular mediante Azure RBAC, garantizando confidencialidad y trazabilidad de objetos sensibles (Microsoft, 2025).

Azure Blob Storage, es un servicio de almacenamiento de objetos que soporta cifrado automático con AES-256 en reposo y transporte seguro con TLS. En el protocolo se emplea para almacenar datos clasificados, respaldos cifrados y logs de auditoría, asegurando disponibilidad y resistencia a fallos (Microsoft, s.f.).

Azure Virtual Network (VNet), crea redes privadas lógicas dentro de Azure, segregando recursos críticos mediante subredes y reglas de acceso. Soporta la implementación de túneles cifrados (VPN Gateway, ExpressRoute, Virtual Network Encryption) para proteger el tráfico en tránsito y prevenir ataques (Microsoft, 2025).

Azure Backup, servicio de copias de seguridad automatizadas y cifradas. Utiliza cifrado AES-256 para proteger datos en reposo y permite replicación geográfica (Geo-Redundant Storage) para garantizar continuidad operativa ante desastres. Además, se integra con Azure Key Vault para la gestión de claves personalizadas (Microsoft, 2025).

Azure Monitor, es una plataforma de supervisión centralizando métricas, logs de actividad y diagnósticos de servicios en Azure. Permite registrar accesos, cambios de configuración y uso de recursos, habilitando el análisis forense y la trazabilidad para auditorías (Microsoft, 2025).

Microsoft Defender for Cloud, herramienta de administración de postura de seguridad (CSPM) y una protección contra amenazas para cargas de trabajo en entornos multiclouds e híbridos. Presta ayuda con evaluar continuamente la seguridad, detectar vulnerabilidades y responder a amenazas en tiempo real (Microsoft, 2025).

Microsoft Sentinel, es una solución basada en la nube, la cual recolecta datos de todos los servicios, los correlaciona y ejecuta respuestas automáticas ante amenazas mediante alerta y playbooks en el protocolo ayuda a detectar anomalías y actuar frente a incidentes de seguridad al ser una solución SIEM (Security Information and Event Management) y SOAR (Security Orchestration Automated Response) (Microsoft, 2025).

Microsoft Purview, plataforma de protección de datos que permite aplicar políticas de etiquetado automático, ayuda a prevenir la fuga de datos (DLP) cumpliendo con normativas y gestión de privacidad (Microsoft, 2025).

Application Security Groups (ASG), es un grupo de seguridad de aplicaciones en Azure, el cual permite agrupar recursos en la red de manera lógica y aplicando reglas de seguridad a grupos de máquinas virtuales en lugar de direcciones IP específicas. En la práctica en este protocolo se utiliza para reforzar la seguridad perimetral controlando el tráfico entre subredes de forma granular (Microsoft, 2025).

Azure Private Link, herramienta propia de Azure que permite el acceso privado a servicios de Azure a través de una conexión dentro de la red virtual del cliente, logrando evitar la exposición a internet públicas (Microsoft, 2025).

Azure Bastion, servicio que permite el acceso de forma segura a máquinas virtuales directamente desde el portal de Azure, utilizando conexiones sin necesidad de exponer la dirección IP pública. En el protocolo permite reforzar la administración de recursos críticos (Microsoft, 2025).

Azure Virtual Network Encryption (DTLS), es una funcionalidad interna que crea túneles Datagram TLS entre VMs o VNets, cifrando el tráfico de forma automática dentro de Azure. Siendo importante para tener un cifrado del tráfico VM-to-VM o a través de VNets emparejadas (peering). Dando valor en el protocolo con añadir una capa de protección en el nivel de red para comunicaciones internas.

4. METODOLOGÍA.

Para comenzar con el trabajo del presente proyecto, se considera inicialmente la metodología "prototipo", debido a su carácter iterativo y flexible ya que se puede adaptar mejor a los desafíos dinámicos que puedan surgir de un proyecto de ciberseguridad, asegurando una implementación más eficaz y ajustada a las necesidades del proyecto. No obstante, esta metodología fue descartada, puesto que su uso es más apropiado cuando existe un cliente activo que revisa versiones tempranas del producto y retroalimenta continuamente en el desarrollo. Bajo lo anteriormente mencionado el contexto de este trabajo y su dinámica, no era viable adoptar esta metodología, además de presentar desventajas como una alta dependencia de retroalimentación externa, un mayor consumo de tiempo y la necesidad de revisar múltiples iteraciones el mismo entregable.

Al momento de descartar "prototipo" y ver sus limitaciones, se opta por utilizar la metodología Kanban, la cual permite trabajar de una forma personalizada a las necesidades del proyecto, permitiendo organizar las actividades en un flujo visual y flexible, priorizando tareas según su criticidad y asegurando su avance progresivo mediante las columnas "Por hacer", "En proceso", "Hecho" y "Aprobado". Su uso permitió gestionar el trabajo de manera ordenada, identificando bloqueos tempranos y manteniendo la trazabilidad completa de las actividad pendientes y realizadas semanalmente.

De forma complementaria, se integra el enfoque Lean, cuyo aporte principal consiste en eliminar información, pasos o actividades que no generan algún tipo de valor para el proyecto, con la intención de concentrar todos los esfuerzos únicamente en los elementos esenciales para el diseño del protocolo. En particular, Lean resulta fundamental para poder depurar información durante la elaboración del estado del arte, marco teórico y la redacción de los capítulos técnicos. Aplicando por ejemplo en la eliminación de información redundante durante la elaboración del marco teórico y la simplificación de las secciones técnicas que no fueron directamente útiles para los objetivos del proyecto.

La metodología Kanban/Lean se selecciona y se justifica especialmente en proyectos de ciberseguridad, donde la dinámica de amenaza requiere enfoques ágiles y adaptativos. Por un lado, Kanban facilita la visualización del flujo de trabajo en tiempo real, controla el avance con límites de trabajó en progreso y detecta en cada paso si ocurre un acontecimiento que pueda retrasar la implementación, prioriza tareas críticas y evita sobrecargas en las actividades. De este modo, cada fase del protocolo se desarrolla de manera ordenada y trazable. Por otra parte, Lean aporta el criterio de concentrarse únicamente en actividades de valor, que elimina pasos redundantes en la documentación y asegura la eficiencia en la construcción del modelo. En el contexto de este proyecto, su aplicación permite priorizar la información esencial y garantiza la eficiencia en la construcción del protocolo.

4.1 Investigación y planificación.

Para esta fase inicial se define como tarea fundamental recopilar toda la información necesaria para dar forma al protocolo. En "Por hacer" se identificaron fuentes normativas como la Ley 19.628, GDPR, ISO/IEC 27001 y las mejores prácticas de seguridad recomendadas por Azure.

Durante en “Progreso” se organizan estas fuentes, se revisan guías oficiales de Azure, documentación técnica y referencias académicas, filtrando lo esencial gracias al enfoque Lean para evitar información redundante o poco relevante.

Al pasar a “Realizado” se consolida un marco claro de requisitos, objetivos y alcance, que sirve como base estructurada para el desarrollo de todas las fases siguientes del protocolo.

4.2 Desarrollo del protocolo.

Esta etapa se plantea como el desarrollo central del trabajo, donde se abordan todas las fases necesarias para construir el protocolo de seguridad en la nube. Cada subfase se incorpora como tarea en la columna “Por hacer”, la cual avanza a “En Progreso” conforme se desarrolla su contenido técnico y conceptual y se mueve a “Realizado” tras revisiones que aseguran su consistencia, claridad y valor real para el objetivo del proyecto. Gracias a la metodología Kanban se prioriza y se adapta cada fase según el avance y los hallazgos semanales, mientras que el enfoque Lean permite eliminar pasos y concentrarse en los elementos esenciales del protocolo.

Durante la fase de diseño y planificación, la metodología Kanban permite organizar las tareas iniciales del proyecto en categorías visuales que facilitan el seguimiento y la priorización donde cada uno correspondiente a un momento crítico del desarrollo.

- Diseño y planificación.
- Desarrollo del protocolo.
- Implementación y validación.

Estos tableros permiten evidenciar el flujo de trabajo y demuestran cómo se cumplió el Objetivo 1, ya que muestran una secuencia clara, ordenada y verificable de las operaciones del protocolo, posteriormente representadas en el diagrama BPMN.

Por Hacer	**En Proceso**	**Hecho**	**Aprobado**
(Fase inicial destinada a definir tareas)	—	—	• **Objetivos del proyecto.** • **Investigación de contexto.** • **Investigar políticas de acceso.** • **Investigar tipos de cifrado.** • **Definir clasificaciones de datos.** • **Definir operaciones eficientes en un protocolo.** • **Modelar diagrama BPMN.** • **Diseño de rúbricas.**

Tabla 1: Diseño y planificación en Kanban

La tabla 1 permitió organizar la investigación preliminar, filtrar información relevante mediante Lean y establecer la base conceptual que sostiene el desarrollo del protocolo.

Adicional a la ilustración 5, se realiza otro tablero con el propósito de desarrollar el protocolo de forma ordenada y meticulosa, ayudando a visualizar el progreso de forma progresiva solamente de los puntos en los cuales se avanza como se muestra en la ilustración 6.

Por Hacer	En Proceso	Hecho	Aprobado
(Subfases del protocolo planificadas)	—	• **Reordenar desarrollo completo (pulir redacción y orden).** • **Rehacer el diagrama BPMN.** • **Resumir rúbricas.** • **Realizar punto 5.3.**	• **Realizar punto 5.2.1.** • **Realizar punto 5.2.2.** • **Realizar punto 5.2.3.** • **Realizar punto 5.2.4.** • **Realizar punto 5.2.5.** • **Realizar punto 5.2.6.**

Tabla 2: Implementación y validación en Kanban

Esta tabla 2 evidencia cómo se avanzó en la construcción estructural y depuración del protocolo, permitiendo desarrollar y depurar cada fase de forma organizada y verificable.

Por Hacer	En Proceso	Hecho	Aprobado
— (Planificación de configuraciones a implementar en Azure)	—	• **Mejorar aspectos formales del documento.** • **Ordenar documento final.**	• **Configurar Azure Active Directory (RBAC).** • **Configurar Azure Key Vault y gestión de claves.** • **Implementar cifrado AES-256 y TLS 1.2.** • **Crear etiquetas y políticas DLP en Microsoft Purview.** • **Configurar Azure Monitor y Log Analytics.** • **Activar Microsoft Defender for Cloud.** • **Configurar Sentinel y alertas automáticas.** • **Implementar Azure Backups y Site Recovery.** • **Validar cumplimiento del protocolo con experto**

Tabla 3: Desarrollo del protocolo en Kanban

Finalmente, la tabla 3 permitió gestionar la fase práctica del protocolo, verificando avances técnicos y estableciendo controles de cumplimiento que posteriormente fueron evaluados por especialistas, cumpliendo así el Objetivo 4.

El uso de estos tableros permitió mantener una visión clara del avance durante cada etapa del desarrollo, facilitó la priorización de tareas críticas y aseguró que cada fase del protocolo fuera diseñada, ejecutada y depurada de manera controlada. Gracias a esta estructura visual y metodológica, se garantizó que todas las operaciones estuvieran correctamente alineadas con los objetivos del proyecto y, posteriormente, con la representación secuencial del diagrama BPMN.

Siguiendo este desarrollo metodológico, se busca cumplir con el objetivo 1, puesto que cada fase y subtarea quedó claramente definida en el tablero Kanban y representado en el futuro diagrama BPMN asegurando el flujo secuencial, ordenado y verificable.

4.2.1 Diseñar diagrama BPMN del protocolo.

Esta subfase inicial consiste en modelar gráficamente el flujo completo del protocolo utilizando la notación BPMN. Este paso resulta fundamental, ya que permite definir desde el inicio la secuencia lógica del proceso, identificar dependencias y detectar posibles inconsistencias. Todo esto se realiza antes de avanzar hacia las etapas de mayor complejidad técnica. El diagrama funciona como una guía estructural del protocolo asegurando que las fases posteriores se desarrollen bajo un orden claro y verificable.

Siguiendo la metodología Kanban, la tarea comenzó en la columna "Por hacer", donde se definió la necesidad de representar visualmente cada fase del protocolo, sus conexiones y los puntos de decisión. En la etapa "en proceso" se trabajó en la selección de la herramienta de modelado, el diseño de las fases principales, la identificación de las actividades internas y la construcción de los flujos que articulan todo el proceso, el objetivo de esta etapa fue garantizar que el modelo reflejará de manera precisa cada operación descrita en el desarrollo metodológico.

Luego al mover la actividad a "Realizado", se validó la consistencia entre el diagrama y la estructura textual del protocolo, ajustando nombres, secuencias y relaciones para lograr coherencia total entre ambos, con esto, el BPMN quedó consolidado como un recurso central para la comprensión del proceso, funcionando como la representación formal y visual del flujo completo del protocolo de ciberseguridad.

4.2.2 Clasificación y evaluación de datos.

La siguiente tarea consiste en definir y detallar las tareas de clasificación de información, así como el análisis de riesgos asociados a su manejo. La correcta ejecución es fundamental para poder establecer los niveles de sensibilidad y los controles de seguridad aplicables en fases posteriores, siguiendo el flujo Kanban, la actividad comenzó en "Por hacer", incorporando las tareas necesarias para asegurar que los datos ingresarán por canales controlados. En etapa "En proceso" se desarrollaron las siguientes acciones.

- A. Envió desde el canal autorizado.
- B. Captura y registro de datos recibidos.
- C. Clasificación de datos.
- D. Aplicar políticas de seguridad según clasificación.
- E. Etiquetado automático con Microsoft Purview.
- F. Evaluar cumplimiento de políticas y riesgos.
- G. Ajustar políticas de seguridad.

Al momento de completar y revisar las subtareas, la actividad pasó a la columna "Realizado", quedando la fase lista para avanzar al diseño de políticas de acceso.

4.2.3 Gestión de identidad y acceso.

Superada la subfase de clasificación, el propósito de esto está enfocado en estructurar las políticas de control de acceso que permitirán asegurar que cada usuario y servicio actúe bajo el principio de mínimo privilegio. Comienza en “Por hacer”, incorporando las subtareas necesarias para la definición de accesos y controles de identidad. Durante la fase “En proceso”, se desarrollaron las siguientes acciones.

- A. Definir requisitos de acceso.
- B. Evaluar cumplimiento de requisitos.
- C. Solicitud de acceso.
- D. Solicitud de privilegio temporal vía PIM.
- E. Asignación de permisos.
- F. Registro de denegación de acceso.
- G. Aplicación de RBAC.
- H. Auditoria de cumplimiento.
- I. Autenticación de servicios con identidades administradas.

Tras la verificación final, todas las tareas fueron marcadas como “Realizado” para cerrar la fase y dejando configurado un sistema de identidad y acceso coherente con las mejores prácticas de seguridad en la nube.

4.2.4 Cifrado, protección y prevención de fuga de datos.

Esta subfase implementa los controles destinados a proteger la información tanto en tránsito como en reposo, a la vez que refuerza la seguridad perimetral y prevenir la fuga de datos. Avanzando desde “Por hacer” hasta “Realizado” conforme se complementaban las subtareas. Durante la fase “En proceso”, se desarrollaron las siguientes acciones.

- A. Cifrado de datos.
- B. Seguridad perimetral.
- C. Activación de políticas DLP.
- D. Gestión de claves.
- E. Restricción de envió de datos sensibles.
- F. Supervisión de fugas y comportamientos anómalos.
- G. Evaluación de amenazas.

Al completarse todas las subtareas, la fase fue movida a la columna “Realizado”.

4.2.5 Monitoreo, Detección y Respuesta ante incidentes.

En esta subfase se habilita la vigilancia continua, la detección temprana y preparación ante incidentes de seguridad dentro del protocolo. Su ejecución siguió el flujo Kanban. Durante la etapa “En proceso”, se desarrollaron las siguientes subtareas.

- A. Supervisión activa.
- B. Escaneo con Defender for Cloud.
- C. Consulta de logs mediante Azure Log Analytics (KQL).

- D. Revisión y respuesta a incidentes.

Al completar estas subtareas y con posterior validación, se avanzó a la columna “Realizado” para pasar a la siguiente subfase.

4.2.6 Respaldo y Recuperación.

Una vez completadas las capacidades de monitoreo, detección y respuesta ante incidentes, para entrar a trabajar en establecer medidas necesarias para asegurar la continuidad operativa del entorno, manteniendo copias válidas de los datos y posibilitando la recuperación ante incidentes o desastres.

- A. Activar respaldo y recuperación.
- B. Validar backup exitoso.
- C. Restaurar sistema.

Completadas y verificadas todas las actividades, se marca la subfase completa como “Realizado”.

4.2.7 Supervisión, Cumplimiento y Auditoría.

Para finalizar el desarrollo del protocolo, se trabajó en integrar los controles de revisión periódica, cumplimiento normativo y auditoria, asegurando que el protocolo pueda mantenerse en el tiempo y alinearse con estándares internacionales. Las actividades ejecutadas fueron las siguientes.

- A. Centralización de logs.
- B. Revisión trimestral.
- C. Asignación de tareas de corrección.
- D. Registro de evidencia,

El cierre de esta subfase, permitió consolidar el protocolo con alineamiento tanto a normas internacionales como a requisitos nacionales de ciberseguridad, además consagra el objetivo 2, puesto que en este punto las fases no solo se documentaron si no que se estructuraron en un modelo integral, aplicable y alineado a normas internacionales como nacionales. Un entorno que pueden ser llevado a la práctica en entorno real de la nube.

4.3 Implementación del protocolo.

Al marcar como “Realizado” todo el desarrollo previo del protocolo, se da paso a la fase de implementación efectiva en el entorno de Microsoft Azure. El objetivo de esta etapa es convertir todas las políticas, controles y buenas prácticas definidas, asegurando que la solución no solo quede documentada, sino que se mantenga funcional en un entorno real. Para ello, se sigue una estrategia estructurada dividida en fases consecutivas que permiten avanzar paso a paso en la construcción de un entorno seguro, consistente y auditado. Este punto está orientado a dar respuesta al objetivo 3 (ver 4.1). Esto se logra mediante la configuración de grupos de recursos, roles de acceso, monitoreo y respaldo de Azure, buscando que el protocolo este en un entorno real y se verifique la viabilidad de este mismo, dejando registro las limitaciones encontradas y de las funcionalidades que si lograron ejecutarse de forma correcta.

4.3.1 Fase 1. Clasificación y evaluación de datos (5.2.1)

La primera tarea consiste en la implementación técnica con la creación de la estructura base para la clasificación de la información, realizando las siguientes acciones.

- Definir de niveles de sensibilidad (confidencial, interno y público).
- Creación de los grupos de recursos para cada nivel de sensibilidad.
- Configurar políticas mediante Azure Policy, incluyendo Auditoria del uso de disco administrado, bloqueo del uso de direcciones IP públicas y exigencia de etiquetas obligatorias en todos los recursos.

Estas tareas se aplican de forma diferenciada según el nivel de sensibilidad. Una vez configuradas, se trasladan a la columna "Hecho" de la metodología Kanban.

4.3.2 Fase 2. Control de Identidad y Acceso (5.2.2)

Tras clasificar y proteger los recursos, se avanzó a la tarea de definir el control de acceso y gestión de identidades.

- Asignar de roles mediante IAM aplicando el principio de mínimo privilegio.
- Para datos confidenciales se autorizan únicamente usuarios específicos definidos con anterioridad.
- Configurar roles predeterminados y personalizados, siendo estos Lectores para usuarios con permisos de solo consultas, Colaborador para el equipo TI y Colaborador de supervisión para las auditorias.

Cada asignación al ser documentadas y configuradas pasa a la columna "Hecho".

4.3.3 Fase 3. Cifrado, vigilancia y prevención de fuga de datos (5.2.3).

Una vez definido el control de acceso, se trabaja en la tarea de habilitar la supervisión y protección de la información.

- Crear un Área de trabajo de Log Analytics asociada al grupo completo de ciberseguridad para centralizar log.
- Establecer la máquina virtual, integrando controles como Secure Boot y vTPM.
- Configurar una Regla de Recopilación de Datos (DCR) para definir qué métricas y eventos recopilar.
- Instalar el Azure Monitor Agent (AMA).

Al momento de tener lista estas acciones, se garantiza la base de monitoreo activa y consistente, la fase queda lista para pasar a la columna "Hecho" del modelo Kanban.

4.3.4 Fase 4. Monitoreo, Detección y Respuesta ante Incidentes de Seguridad (5.2.4).

Con el monitoreo habilitado, se procede a la tarea de habilitar la detección de amenazas y respuestas ante de incidentes.

- Activar Microsoft Defender for Cloud en la suscripción, habilitando evaluaciones continuas.
- Revisar las recomendaciones generadas por Defender, aplicando mejoras en configuración.
- Validar la generación de alertas básicas como el uso de puertos abiertos, configuraciones incompletas, falta de extensiones de seguridad y recomendaciones de cumplimiento.

Esta fase permitió comprobar la capacidad del entorno para detectar las vulnerabilidades, al estar configurados todos los puntos, se procede a desplazar a la columna “Hecho”.

4.3.5 Fase 5. Respaldo y Recuperación (5.2.5).

Completada la detección activa, se avanza a la tarea de garantizar la continuidad operativa.

- Crear un Recovery Services Vault dentro del grupo GR-Ciberseguridad.
- Configurar la copia de seguridad de la VM utilizando la política EnhancedPolicy con la retención de 30 días y la restauración instantánea habilitada.
- Verificar la presencia de la Máquina virtual como un “elemento protegido”, para evidenciar que la copia de seguridad funcione correctamente.

Al momento de configurar los 3 puntos anteriores se procede a pasar a la siguiente fase, donde esta pasa a la columna “Hecho”.

4.3.6 Fase 6. Supervisión, Cumplimiento y Auditoría (5.2.6).

Finalmente, se trabaja en la tarea de validar la configuración de retención de datos en Log Analytics, con el propósito de configurar la trazabilidad y el cumplimiento normativo.

- Validar la configuración de retención de 30 días en Log Analytics, requisito esencial para auditoría y análisis forense.
- Revisar controles de cumplimiento considerando las normativas chilenas, ISO/IEC 27001, NIST SP 800-53.

Esta fase final permite dar cumplimiento normativo, integrando la revisión técnica, retroalimentación profesional y validación de la implementación, Al igual que las fases anteriores pasa a la columna “Hecho” al momento de terminar su configuración.

4.4 Validación del experto.

Una vez implementadas todas las fases técnicas del protocolo en el entorno de Microsoft Azure, se procede a establecer la etapa de validación externa con especialistas en ciberseguridad. El propósito de esta instancia es verificar la coherencia, pertinencia y solidez técnica del modelo propuesto, además de confirmar que cada una de las tareas desarrolladas en las fases previas cumpliera con el estándar profesionalmente aceptados en un entorno de ciberseguridad.

En términos metodológicos esta validación funcionó como un paso adicional en el flujo Kanban, puesto que la implementación de la fase anterior quedó todas en la columna “Hecho”. Solo tras recibir la revisión y aprobación del experto, cada ítem avanzo a la columna “Aprobado”, solo de esta manera se afirmaba el cumplimiento definitivo. Este proceso permitió garantizó que el protocolo no solo

estuviera implementado técnicamente, sino también evaluado externamente conforme a criterios profesionales. Los expertos revisaron aspectos claves también, como.

- Estructura secuencial del protocolo.
- Alineación entre teoría, BPMN e implementación real.
- Coherencia entre cifrado, monitoreo y auditoría.
- Trazabilidad de los logs y copias de seguridad.
- Consistencia del modelo frente a normas internacionales (ISO/IEC 27001, NIST SP 800-53) y legislación nacional.

Con esta etapa se entrega cumplimiento al objetivo 4 (ver 1.4) del proyecto, dado que la validación externa aseguró que el protocolo resultante fuera coherente, aplicable y sustentado profesionalmente. Permitió confirmar la transición formal del diseño e implementación hacia un protocolo integral aprobado, con potencial de ser adoptado en entornos reales de ciberseguridad en la nube.

5. DESARROLLO.

En una primera instancia se consideró la posibilidad de estructurar el protocolo de ciberseguridad utilizando Google Business Intelligence (BI) como plataforma de apoyo, dado que entrega un marco de trabajo inicial para organizar información y visualizar procesos. Sin embargo, se identificaron limitaciones significativas. Esta herramienta está diseñada principalmente para el análisis y la presentación de datos, lo que restringe su capacidad para implementar controles de seguridad, políticas de acceso o mecanismos de protección en un entorno de nube. En consecuencia, no es una herramienta adecuada para cubrir los requerimientos técnicos y normativos que el proyecto demanda.

Frente a las limitaciones, se decidió optar por Microsoft Azure, lo que permitió construir un protocolo más robusto y completo, capaz de abordar todas las fases del ciclo de vida de la seguridad de los datos en la nube. Se logró implementar controles de acceso basados en roles, autenticación multifactor, cifrado en reposo y en tránsito, copias de seguridad automatizadas y replicadas, así como herramientas de monitoreo y detección de incidentes en tiempo real. Este cambio permitió desarrollar un modelo más integral y adaptado a los objetivos del proyecto, dejando como resultado un protocolo de ciberseguridad en la nube que puede servir como base para organizaciones que necesiten fortalecer su seguridad de manera estructurada y alineada con estándares internacionales.

5.1 Planificación de operaciones del protocolo.

Una gran empresa o una pequeña empresa que maneje información almacenada en una base de datos en la nube necesita establecer un protocolo de ciberseguridad que no solo detecte amenazas, sino que también permita responder de manera eficiente y estructurada ante posibles incidentes. Si bien la presente propuesta es teórica y se implementará mediante una simulación en un entorno controlado a través de una máquina virtual en Microsoft Azure, su diseño se ajusta a estándares reales de seguridad empresarial en la nube.

La secuencia propuesta se basa en las recomendaciones de Microsoft para arquitecturas seguras, en conjunto con lineamientos de seguridad internacionales como el estándar NIST SP 800-53, que establece controles de seguridad organizados, como control de accesos, respuesta a incidentes, y monitoreo continuo (Force, 2020). Microsoft también propone un enfoque estructurado de seguridad a través de su iniciativa Zero Trust, que se basa en "verificar explícitamente, usar el mínimo privilegio y asumir que hay una brecha" (BrendaCarter, 2025).

Con el fin de garantizar una protección integral en entornos de nube, se propone una secuencia estructurada de acciones que responda a buenas prácticas y estándares reconocidos a nivel internacional. Esta secuencia tiene como objetivo establecer un protocolo claro y eficiente, capaz de anticipar, detectar y responder ante incidentes de seguridad. A continuación, se detallan las etapas clave que componen dicho protocolo, orientadas a optimizar la ciberseguridad desde la prevención hasta la evaluación post-incidente. A continuación, se detalla los componentes operativos esenciales del protocolo, organizados por etapas secuenciales que reflejan la lógica de implementación recomendada por Microsoft y los estándares internacionales.

A. Definición de políticas de acceso.

Se implementan políticas de acceso mínimo, esto se puede llevar a cabo con herramientas específicas de Azure, la cual se llama “Azure Role-Based Access Control” (RBAC) recurso el cual garantiza que la nube solo pueda acceder el personal autorizado puedan acceder a los recursos que se le establezcan. Según Microsoft, "la administración de acceso basada en roles ayuda a garantizar que los usuarios tengan solo los permisos que necesitan para realizar sus tareas" (Microsoft, Azure security best practices and patterns, 2024). Además, puede ayudar a limitar el famoso “trabajador despechado”, problema el cual se basa en el despido de un trabajador y por su descontento altera los datos sensibles de la empresa.

Si bien, utilizar “Azure Role-Based Access Control” (RBAC) garantiza que solo el personal autorizado tenga acceso a los recursos, también es importante tener en consideración la gestión del error humano, esto porque un alto porcentaje de incidentes de seguridad provienen de una mala categorización de datos o de errores en la asignación de roles. Para mitigar este riesgo, se implementan políticas de acceso mínimo y autenticación multifactor (MFA), que busque reducir la posibilidad de accesos indebidos. Siguiendo la línea de mitigar el error humano, más adelante se aplica el uso de la auditorias periódicas y revisiones de acceso, para así tener siempre alineadas las necesidades reales de los usuarios y que no existan privilegios innecesarios o erróneos. Este conjunto de prácticas buscan ayudar a minimizar los riesgos derivados de la intervención humana en la gestión de accesos y roles.

B. Implementación de reglas de recopilación de datos.

Estas reglas se denominan “Data Collection Rules (DCR)” configuran para recolectar métricas y logs de seguridad relevantes en tiempo real desde la máquina virtual y otros recursos. Esta información se envía a un área de trabajo de Log Analytics, donde será procesada y almacenada para su análisis posterior.

C. Monitoreo continuo con Azure Monitor y Log Analytics

A través de Azure Monitor, se realiza una supervisión continua de los recursos, permitiendo identificar patrones inusuales o actividades no autorizadas. El análisis de logs y métricas en Log Analytics Workspace es clave para obtener visibilidad del comportamiento de los sistemas. Como lo señala Microsoft, “el monitoreo continuo permite a las organizaciones identificar amenazas en tiempo real y reducir el tiempo de respuesta” (Microsoft, Azure security best practices and patterns, 2024).

D. Activación de alertas automáticas

Se configuran alertas inteligentes en Azure Monitor ante eventos críticos, como intentos fallidos de autenticación o cambios en configuraciones sensibles. Estas alertas pueden integrarse con Azure Sentinel para iniciar flujos automatizados de respuesta.

E. Respuesta automatizada ante incidentes

Con Azure Sentinel se implementan playbooks automáticos mediante Logic Apps que permiten aislar máquinas virtuales, bloquear IPs sospechosas o notificar inmediatamente al equipo de seguridad. Según Microsoft, "el uso de SOAR (Security Orchestration, Automation, and Response) en Sentinel permite una reacción más rápida y consistente a los incidentes" (Microsoft, Automate Yhreat reponse with playbooks in Microsoft Sentinel, 2024).

F. Evaluación post-incidente

Finalmente, se realiza una evaluación continua de los eventos que son registrados y de la efectividad de las respuestas aplicadas. Se aplica el control AU-6 del NIST SP 800-53 ya que este recomienda la revisión y análisis de registro para poder detectar problemas y así mejorar el sistema de seguridad periódicamente.

5.2 Diseño del protocolo de seguridad en Azure.

Para el diseño del protocolo se realizó en la ilustración 5 el diagrama completo del protocolo, integrando todas las fases y actividades en una sola vista. Este esquema permite observar de manera clara y continua el funcionamiento total del proceso. Proporcionando una visión global sin necesidad de fragmentarlo en diagramas desglosados.

Luego de presentar la ilustración 5, se presenta otro modelo BPMN, que corresponde a la ilustración 6 en la cual está el protocolo desplegado por completo, con el objetivo de comprender de forma más rápida las fases del diagrama, permitiendo un análisis más detallado de las actividades involucradas.

Aunque Azure no establece un protocolo único y obligatorio el cual seguir, pero si entrega un marco robusto de seguridad basado en buenas prácticas internacionales, herramientas nativas de Microsoft y principios como modelo de Zero Trust. Como se mencionó anteriormente el marco esta alineado con estándares reconocidos internacionalmente como ISO/IEC 27001, NIST SP 800-53 y GDPR. A continuación, se presenta un resumen de las principales herramientas nativas de Azure y rúbricas de elaboración propia, organizadas según los dominios clave abordados en el proyecto.

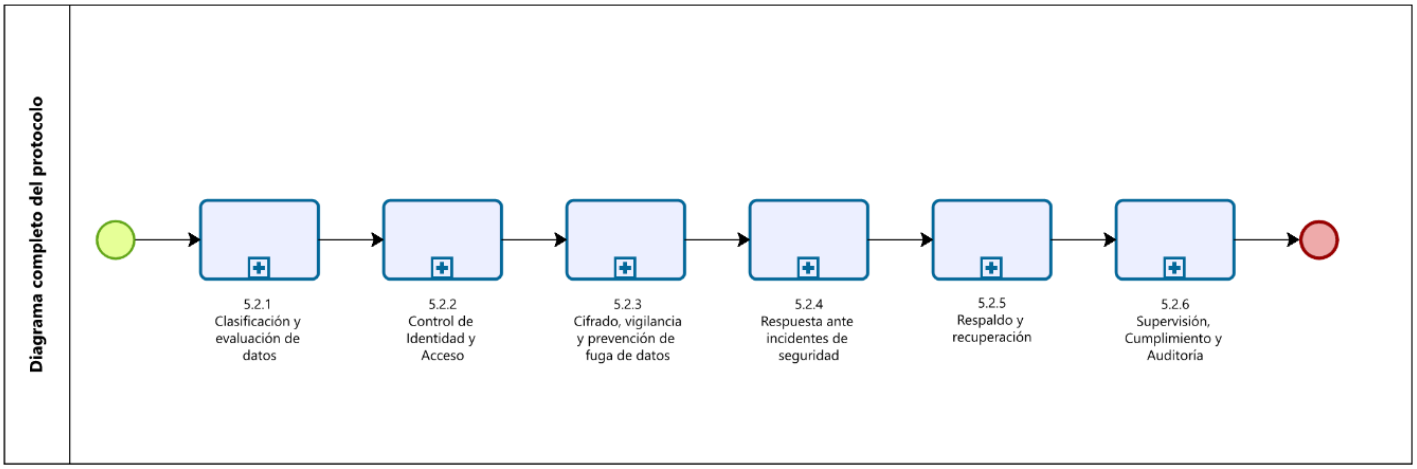

Ilustración 5: Diagrama BPMN del protocolo resumido.

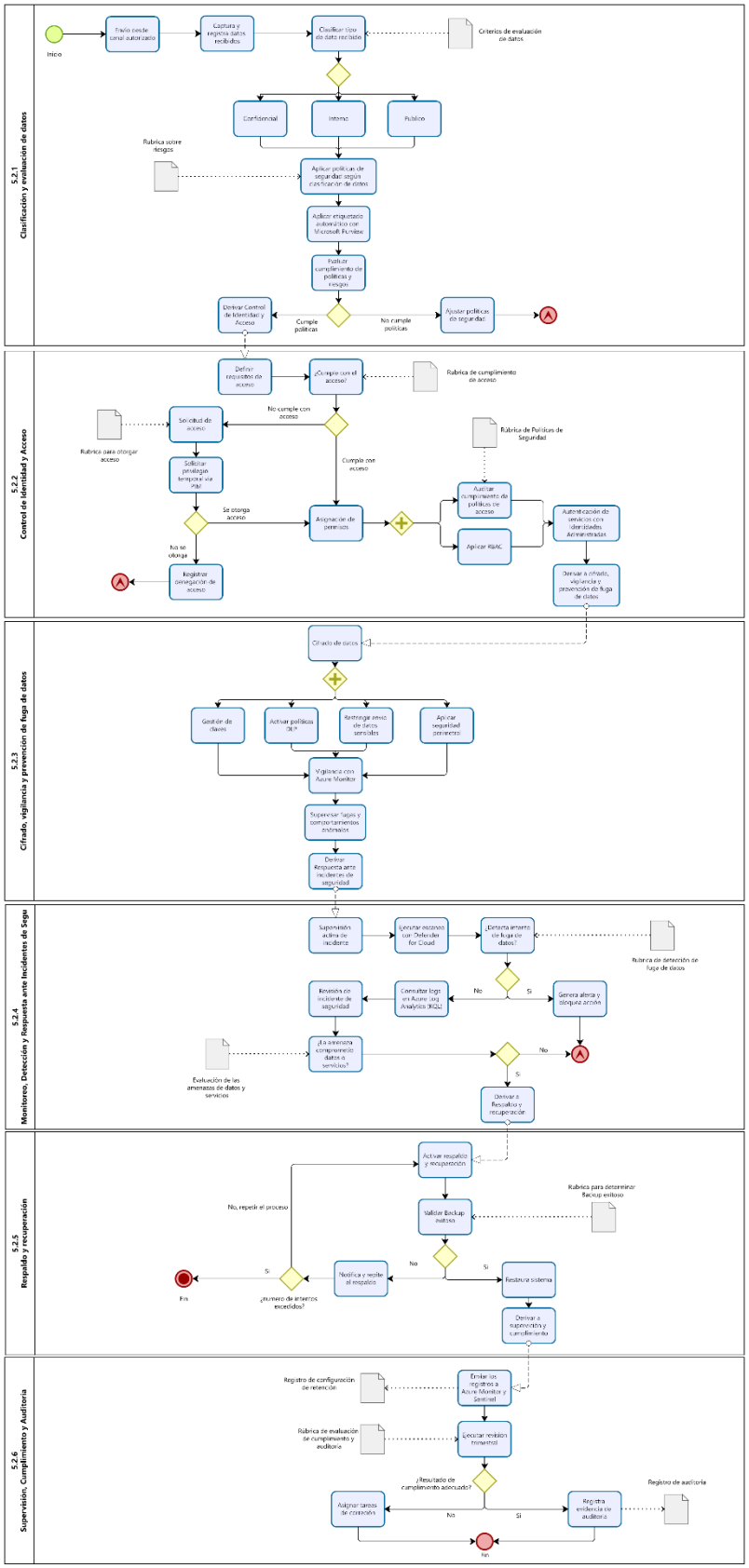

Ilustración 6: Diagrama BPMN del protocolo completo.

A. Clasificación y Evaluación de Datos.

Herramientas utilizadas:

- Microsoft Purview: Etiquetado automático de datos y políticas de clasificación.
- Matriz de riesgo semicuantitativa: Evaluación de amenazas e impacto.
- Canales de entrada autorizados: Filtrado inicial de información.

B. Control de Identidad y Acceso.

Herramientas utilizadas:

- Microsoft Entra ID: Autenticación centralizada.
- MFA (Multifactor Authentication): Acceso reforzado.
- RBAC (Role-Based Access Control): Asignación de permisos mínimos.
- Microsoft Entra ID Protection: Protección de identidades.
- PIM (Privileged Identity Management): Asignación temporal de privilegios.
- Managed Identities: Autenticación de servicios internos.
- Revisión periódica de accesos: Con Access Reviews en AAD Identity Governance.

C. Cifrado, Protección y Prevención de Fugas de Datos.

Herramientas utilizadas:

- Azure Key Vault: Gestión de claves cifradas (CMK).
- Cifrado AES-256: En reposo.
- TLS 1.2 / VPN Gateway / ExpressRoute / Azure VNet Encryption: En tránsito.
- Microsoft Purview DLP: Políticas de prevención de fuga de datos.
- Azure Monitor / Azure Sentinel / Log Analytics: Monitoreo y análisis de incidentes.
- Azure Bastion, ASG, Private Link: Seguridad perimetral y segmentación de red.

D. Monitoreo, Detección y Respuesta ante Incidentes.

Herramientas utilizadas:

- Microsoft Defender for Cloud: Evaluación continua, escaneo y alertas.
- Azure Monitor y Log Analytics (KQL): Recolección y análisis de logs.
- Microsoft Sentinel: Correlación de eventos y playbooks automatizados.
- Pruebas de penetración: Semestrales.
- Update Management: Aplicación automatizada de parches.

- Matriz de evaluación de amenazas: Riesgo de impacto y vulnerabilidad.

E. Respaldo y Recuperación.

Herramientas utilizadas:

- Azure Backup: Respaldos automáticos con cifrado AES-256.
- Azure Key Vault: Claves de respaldo (CMK).
- Rúbrica de Backup Exitoso: Evaluación estructurada.
- Azure Site Recovery (ASR): Restauración automática, failover y pruebas.

F. Respaldo y Recuperación.

Herramientas utilizadas:

- Azure Backup: Respaldos automáticos con cifrado AES-256.
- Azure Key Vault: Claves de respaldo (CMK).
- Rúbrica de Backup Exitoso: Evaluación estructurada.
- Azure Site Recovery (ASR): Restauración automática, failover y pruebas.

Para garantizar que el protocolo tenga una correcta alineación con las mejores prácticas internacionales, los dominios definidos con anterioridad se han mapeado con los controles establecidos en el Microsoft Cloud Security Benchmark (MCSB), Este marco permite evaluar niveles de cumplimiento del protocolo respecto de los estándares de seguridad establecidos para arquitecturas en la nube. Con el fin de sintetizar esta relación, la ilustración 7 se muestra un esquema general que conecta las normativas internacionales, con servicios nativos de Azure y las fases técnicas del protocolo. Esta representación facilita comprender cómo cada componente del diseño se sustenta un dominio específico del MCSB, asegurando coherencia entre la propuesta teórica y su implementación práctica.

Incorporar esta comparación estructurada también aporta una base objetiva para futuras evaluaciones de auditorías o evaluaciones de cumplimiento y revisiones de seguridad a una mayor escala. Podrá ayudar a identificar brechas y priorizar mejoras, en pocas palabras, este análisis actúa como un puente entre teoría y práctica, asegurando que la construcción del protocolo no solo sea funcional, sino también normativamente sólida. A continuación, se detalla en la tabla 4 la correspondencia directa entre cada fase del protocolo y los dominios del MCSB, explicando de qué manera se cumplen los lineamientos establecidos por este estándar.

Fase del Protocolo	Dominio MCSB	Descripción de la Relación
Clasificación y Evaluación de Datos (Ver 5.2.1)	IM – Identity Management	Incluye controles de etiquetado automático, clasificación y evaluación de riesgos que permiten establecer políticas de acceso alineadas con el dominio IM del MCSB.
Gestión de Identidad y Acceso (Ver 5.2.2)	IM – Identity Management	Incorpora Azure AD, MFA, RBAC, PIM e identidades administradas, conforme a los lineamientos de IM del MCSB para administración segura y verificada de accesos e identidades.
Cifrado, Protección y Prevención de Fuga de Datos (Ver 5.2.3)	DP – Data Protection	Considera cifrado en reposo y en tránsito, gestión de claves (PMK y CMK con Key Vault) y políticas DLP mediante Purview, alineado con DP del MCSB.
Cifrado, Protección y Prevención de Fuga de Datos (Ver 5.2.3)	NS – Network Security	Incluye medidas de segmentación y seguridad perimetral como ASG, Private Link, Azure Bastion, entre otras, en concordancia con el dominio NS del MCSB.
Monitoreo, Detección y Respuesta ante Incidentes (Ver 5.2.4)	LT – Logging & Threat Detection	Abarca Defender for Cloud, Microsoft Sentinel, Azure Monitor y gestión de vulnerabilidades, cumpliendo los criterios de supervisión del dominio LT del MCSB.
Respaldo y Recuperación (Ver 5.2.5)	BR – Backup & Recovery	Utiliza Azure Backup, Site Recovery, replicación geográfica y pruebas de restauración, tal como se establece en el dominio BR del MCSB.
Supervisión, Cumplimiento y Auditoría (Ver 5.2.6)	GS – Governance & Strategy	Se relaciona con el uso de Compliance Manager, auditorías, retención de logs y revisión trimestral, alineado con el dominio GS del MCSB.

Tabla 4: Relación del protocolo con prácticas internacionales.

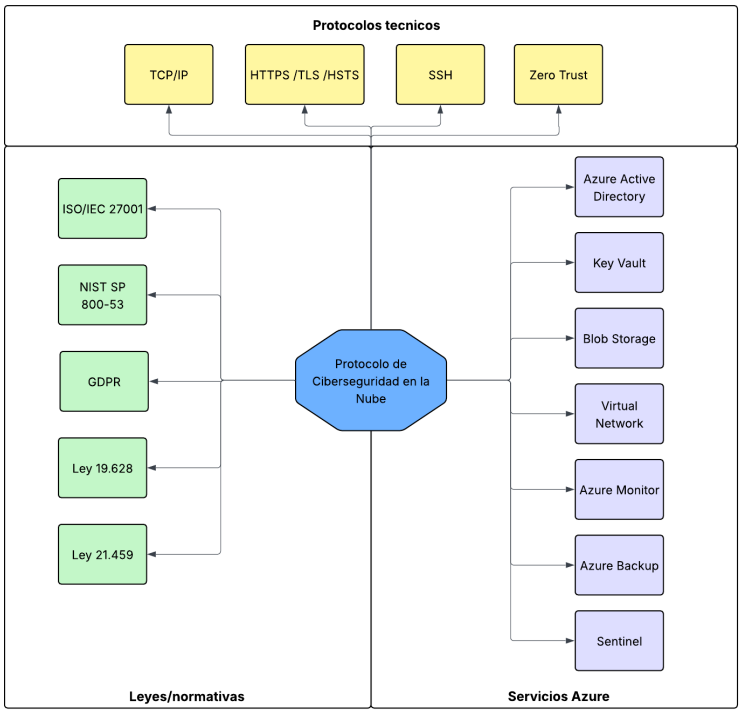

Ilustración 7: Diagrama relación con servicios, leyes y protocolos.

5.2.1. Clasificación y Evaluación de Datos

La primera fase del protocolo tiene como objetivo la clasificación y evaluación de datos, proceso esencial para poder garantizar que la información recibida tenga el nivel adecuado de protección según su sensibilidad. Esta etapa permite establecer las bases para aplicar medidas de seguridad que sean coherentes a los riesgos que pueden estar asociados a cada tipo de dato. En la ilustración 8, se representa el flujo detallado de esta fase, la cual abarca desde el ingreso de los datos hasta la evaluación de riesgos y a la derivación de control de acceso pertinente. Cada una de estas actividades está definida como una tarea clave dentro del protocolo que contiene decisiones automatizadas y revisiones según las políticas de seguridad establecidas.

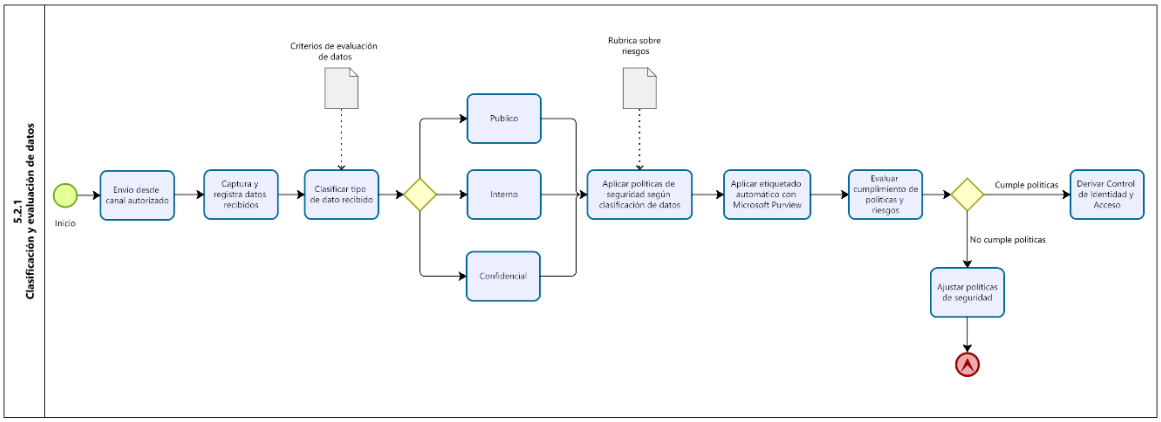

Ilustración 8: Diagrama BPMN 5.2.1.

Gracias a la ilustración 8, se evidencia que el protocolo tiene una base estructurada y documentada que establece el tratamiento diferencial de los datos según su sensibilidad, asegurando una gestión alineada con principios de confidencialidad, trazabilidad y cumplimiento normativo. A partir de este punto, se describe detalladamente cada una de sus fases, sus herramientas y como debe de proceder el protocolo en cada situación.

A. Envió desde canal autorizado.

Para identificar el **origen, tipo y almacenamiento de la información**, los datos son clasificados según su nivel de sensibilidad se continua con la identificación precisa del origen, tipo y mecanismo de almacenamiento de la información. Es por lo que se deben revisar cada paso para tener la información bien estructurada.

Origen de la información: El origen se refiere a la fuente de generación o recepción del dato y se debe capturar como metadato obligatorio, dentro de las fuentes se incluyen los sistemas internos (ERP, CRM, intranet), formularios webs, aplicaciones móviles, transferencias automatizadas desde sistemas externos o filiales, dispositivos IOT o sistemas de monitoreos, proveedores o entidades externas autorizadas.

B. Captura y registro de datos recibidos.

Tipo de información: Este apartado complementa el proceso de clasificación y dirige el tratamiento técnico que deben recibir los datos dentro de este protocolo. Cada tipo de información recibida es evaluada según la rúbrica establecida, permitiendo asignar un nivel de sensibilidad y aplicar controles diferenciados según su riesgo. Esta clasificación es fundamental para determinar qué medidas de protección corresponden a cada dato, siguiendo las recomendaciones del propio Azure Well-Architected Framework (Microsoft, 2023).

C. Clasificación de datos.

En el punto para **identificación y Categorización** para clasificar los datos en niveles de sensibilidad, al momento de la recepción de datos es necesario desde ese punto establecer una clasificación directa para poder establecer como manejar cada dato, aunque el protocolo se inicia con la clasificación de datos, no se limita a la naturaleza de esta información ya que además considera los requisitos de accesos asociados. Es decir, no solo importa qué tipo de dato ingresa, también quien puede acceder a él y en qué condiciones. Mencionando lo anterior se procede a establecer como se define las categorías de los datos.

Confidencial: Los datos confidenciales se consideran dentro de este protocolo y en general el nivel más alto de protección dentro de la clasificación de datos debido a su alto impacto en caso de filtración o acceso indebido. Estos incluyen información personal identificable o numerosa información sensible como Rut, tarjetas de crédito, registros médicos, contratos legales o información financiera, su divulgación conlleva riesgos legales, financieros, etc (Smith, 2025). Es por lo que las entidades que manejan este tipo de datos están sujetas a marcos regulatorios, los cuales exigen cifrados, controles de acceso y auditorias continuas. Según las buenas prácticas de Azure los datos etiquetados como confidenciales deben protegerse en todas las fases, reposo, tránsito y uso (Microsoft, 2023).

Interno: Estos datos no contienen información tan delicada como los datos confidenciales, pero aun así es necesaria la protección y control, ya que su exposición podría afectar el buen funcionamiento

de la organización interna o la estrategia de negocio. Estos datos son utilizados por equipos y sistemas internos, pero no pueden ser divulgados sin autorización, según la clasificación de Palo Alto Networks a estos datos se le denominan "Internal Use Only" englobando así nominas, planes de proyecto, etc (paloalto, s.f.). Aunque no provocan algún tipo de problema legal inmediato si se filtran, pueden generar pérdidas de eficiencia, impacto en la reputación de la organización, pérdidas monetarias o desventajas competitivas ante otra entidad. Dentro de las principales acciones para manejar estos datos es el control de acceso mediante RBAC, estableciendo empleados con roles específicos.

Público: Estos datos representan el nivel más bajo de sensibilidad en la clasificación, ya que están destinados a ser accesibles a cualquier persona sin restricciones y su divulgación no representa riesgos significativos ni para la organización o una persona individual. Esto incluye informes de investigación que hayan sido publicados y base de datos abierta. Los controles que se pueden aplicar para estos datos se centran en asegurar que sean verídicos, su disponibilidad inmediata y que no sufran modificación sin dejar registro.

Criterio clave	Confidencial	Interno	Público
¿Contiene datos personales o regulados?	Sí	No	No
¿Genera impacto legal, financiero o reputacional?	Sí	Parcial	No
¿Sujeto a normativas específicas?	Sí	No	No
¿Requiere control de acceso (RBAC)?	Sí	Sí	No
¿De uso exclusivamente interno?	Restringido	General	No
¿Contiene información de gestión u operación interna?	Sí	Sí	No
¿Es apto para publicación o difusión abierta?	No	No	Sí
¿Afecta la disponibilidad del sistema si se pierde?	Sí	Sí	No
¿Requiere integridad más que confidencialidad?	No	Sí	Sí

Tabla 5: Clasificación de Datos según nivel de sensibilidad.

Mencionado lo anterior, se presenta la Tabla 5, la cual resume los criterios claves a utilizar para clasificar los datos según su nivel de sensibilidad (Confidencial, interno y público) junto con la descripción de cada criterio. Mostrando de manera comparativa las diferencias entre cada categoría y controles asociados a ellas.

D. Aplicar políticas de seguridad según clasificación de datos.

Almacenamiento de la información: Estableciendo el origen y el tipo de información. Los datos se deben almacenar en los mismos servicios de Microsoft Azure, utilizando las herramientas más apropiadas para su protección, disponibilidad y cumplimiento de las normativas.

A continuación, se visualiza la Tabla 6, la cual busca clasificar según los datos y servicios de Azure recomendados junto a los controles de seguridad que se deben aplicar a cada uno.

Clasificación del dato	Servicio de Azure recomendado	Controles de seguridad aplicados
Confidencial	Azure SQL Database / Blob Storage / Key Vault	Cifrado en reposo y en tránsito, RBAC, etiquetas de sensibilidad
Interno	Azure Files / Cosmos DB	Cifrado en tránsito, control de acceso, auditoría moderada
Público	Azure Blob Storage / Web-hosted Repositories	Control de integridad, acceso abierto, monitoreo básico de disponibilidad

Tabla 6: Clasificación del dato y servicio de Azure recomendado.

Todo almacenamiento se realiza bajo el principio de mínimo privilegio con registro de accesos y operaciones mediante Azure Monitor incluyendo Log Analytics, asegurando trazabilidad y control total de la información (Microsoft, 2025).

E. Aplicar etiquetado automático con Microsoft Purview.

Para el **etiquetado automático**: Al estar los datos clasificados y almacenado se establece el uso de "Microsoft Purview Information Protection" para aplicar el etiquetado automático sobre los datos como mecanismo central de protección y trazabilidad. La elección de esta herramienta logra identificar, clasificar y proteger datos confidenciales en toda la organización, utilizando etiquetas de sensibilidad que se pueden aplicar automática o manualmente según estén predefinidas las reglas. El funcionamiento del etiquetado automático puede analizar archivos, correos electrónicos o bases de datos buscando los patrones preconfigurados, que pueden ser RUT, datos bancarios o financieros, contratos, palabras claves, etc. Al momento de detectar alguno de estos elementos la herramienta aplica una etiqueta que puede activar políticas como cifrado automático, restricción de acceso, marcas visuales, auditorias detalladas.

Clasificación	Etiqueta de sensibilidad sugerida	Acciones automáticas
Confidencial	"Confidential - Restricted"	Cifrado, acceso limitado, marca visual, bloqueo de reenvío
Interno	"Internal - Use Only"	Solo usuarios autenticados, sin distribución externa
Público	"Public - No Restrictions"	Sin restricción (monitoreo opcional)

Tabla 7: Clasificación y etiqueta de sensibilidad sugerida.

La Tabla 7, la cual permite mostrar que por la clasificación de los datos se genera una etiqueta de sensibilidad y la acción automática que debe de tomar el protocolo ante los datos mostrados. Esta tabla busca garantizar que las políticas de protección acompañen a los datos, sin importar su ubicación, incluso cuando se comparte por correo, se descarga o se sincroniza en dispositivos. Además, permiten cumplir con normativas como GDPR, ISO/IEC 27001 y la Ley 19.628 de Protección de Datos en Chile.

Lograr la categorización de los datos y la evaluación de riesgos es tarea clave dentro del protocolo, generalmente esta tarea es realizada por el equipo de seguridad de la información o por herramientas automatizadas como Microsoft Purview. Sin embargo, dado que la correcta clasificación es crucial para el éxito del protocolo, validar la categoriza se lleva a cabo mediante auditorias periódicas y revisiones por parte de expertos de ciberseguridad. Adicional la matriz de riesgo semicuantitativa es utilizada para evaluar las amenazas y su impacto se valida mediante simulaciones de incidentes y pruebas de penetración, buscando asegurar la clasificación y las respuestas sean apropiadas.

F. Evaluar cumplimiento de políticas y riesgos.

El objetivo de esta etapa es analizar los impactos que pueden tener la exposición de los datos sensibles, el análisis debe guiar la priorización de controles y tener medidas adaptadas al contexto del protocolo en Azure para saber que se debe analizar.

En la identificación de amenazas y vulnerabilidades, estas incluyen accesos no autorizados, brechas ocasionadas por phishing, exfiltraciones de datos, fallos de cifrado, vulnerabilidades del sistema o errores humanos. Pero, por otro lado, las vulnerabilidades pueden estar asociadas a configuraciones incorrectas, ausencia de MFA, papel de acceso excesivo en RBAC o a la falta de cifrado en tránsito o reposo.

Para determinar probabilidad y exposición potencial, se evalúa la probabilidad de que la amenaza ocurra ya sea por un ataque exitoso o un error humano, se debe tener en consideración el factor de exposición que compromete los datos, estimando así el porcentaje de daño al activo o a una pérdida asociada. Para la evaluación de impacto se consideran cuatro dimensiones claves para este punto.

- **Financiero**: Costos directos de remediación, multas por incumplimiento.
- **Operativo**: Interrupción de procesos, pérdida de productividad.
- **Reputación**: Pérdida de confianza de clientes o socios.
- **Regulatorio**: Sanciones por incumplimiento de normas como GDPR, HIPAA o ley 19.628 de protección de datos.

Cuantificación del riesgo: El nivel de exposición de la organización permite medir objetivamente este nivel ante la posible materialización de una amenaza sobre datos sensibles. A partir de esta evaluación, se establecen prioridades de mitigación y se definen los controles de seguridad apropiado.

Formula base

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Probabilidad: Que tan factible es que ocurra el evento.

Impacto: Consecuencias que tendría ese evento sobre la organización si se materializa.

Al ser necesario el evaluar la probabilidad de ocurrencia de un riesgo se utiliza una escala de cinco niveles que considera desde eventos improbables a inevitables, en la Tabla 8 se presenta la escala incluyendo una descripción de cada nivel de la probabilidad asociada al incidente de seguridad de la información. De manera paralela se aplica la Tabla 9 para estimar el impacto que tendría la materialización de un riesgo sobre la organización, detalla los niveles de impacto con 5 niveles como la Tabla 8, abarcando desde efectos insignificante hasta consecuencias que pueden ser críticas y graves que podrían afectar a la continuidad operativa o reputación de la entidad.

Con base a los valores de probabilidad e impacto, existe una matriz de riesgo que permite visualizar gráficamente el nivel de exposición frente a distintos eventos, la Ilustración 9 muestra la matriz de riesgo, donde el eje vertical representando la probabilidad y el eje horizontal el impacto, facilitando así la priorización de los riesgos identificados.

Nivel	Valor	Descripción
Muy baja	1	Extremadamente improbable, requeriría múltiples fallos simultáneos.
Baja	2	Poco probable, solo ocurriría bajo condiciones particulares.
Media	3	Factible; ha ocurrido ocasionalmente en la industria.
Alta	4	Alta probabilidad según historial o contexto organizacional.
Muy alta	5	Virtualmente inevitable si no se aplican controles.

Tabla 8: Escala de probabilidad.

Nivel	Valor	Descripción
Muy bajo	1	Sin efectos apreciables, no afecta continuidad.
Bajo	2	Impacto interno menor, sin implicancias externas.
Medio	3	Afecta operaciones o imagen de forma puntual.
Alto	4	Implica pérdida financiera o interrupción de servicios.
Crítico	5	Provoca daño legal, financiero o reputacional grave.

Tabla 9: Escala de Impacto.

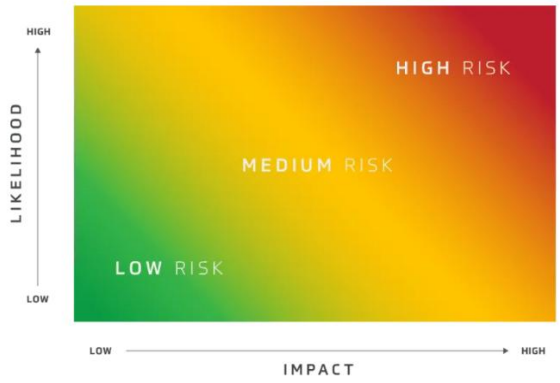

Ilustración 9: Matriz de riesgo. Obtenida de: (McGill, s.f.).

Riesgo Total (P × I)	Nivel de Riesgo	Acción Requerida
1 – 5	Bajo	Mantener controles actuales.
6 – 10	Moderado	Evaluar refuerzo de controles o revisión periódica.
11 – 15	Alto	Aplicar mejoras urgentes y seguimiento constante.
16 – 25	Crítico	Intervención inmediata; rediseñar proceso.

Tabla 10: Interpretación de resultados de evaluación de riesgo.

Al momento de ser evaluados los eventos con las escalas anteriores, se utiliza la formula base para obtener una puntuación total entre 1 y 25, interpretando este cálculo con la Tabla 10, la cual establece cuatro niveles de riesgos, cada nivel tiene diferentes rangos y por cada rango tiene las acciones correspondientes que deben ser implementadas.

G. Ajustar políticas de seguridad.

Las auditorias con esta herramienta aseguran la integridad, disponibilidad y conformidad con políticas internas y normativas como ISO 27001, GDPR y la Ley 19.628. La auditoría realiza un registro de logs que se habilita con Azure Diagnostic Settings en cuentas de Storage para capturar operaciones como lecturas, escrituras, eliminaciones y configuraciones. Luego de activar la herramienta anterior se realiza un almacenamiento seguro de logs para guardar los registros en una cuenta de almacenamiento cifrada o enviarlos a Azure Monitor, garantizando su retención y protección.

Al tener todo lo anterior listo se realizan rotación de claves ante la regeneración de claves de acceso, los logs deben estar frecuentemente actualizándose para poder seguir capturando los eventos correctamente, de la mano se debe de ir realizando los logs de forma mensual o idealmente después de un incidente para identificar accesos anómalos o configuraciones inseguras (Microsoft, 2025).

En el protocolo es vital la gestión de acceso, esta debe de formalizarse según las categorías de datos identificadas por lo que es importante definir políticas de acceso según clasificación (Confidencial, interno, publico).

- **Roles**: Se deben de asignar roles por categorías, por ejemplo “Encargado de recursos humanos”.
- **Alcances específicos**: Los permisos se deben aplicar por grupo de recursos, recursos individuales, alguna suscripción, con el fin de poder limitar su alcance.
- **Revisión periódica de acceso**: Revisar cada cierto periodo de tiempo los roles y personas que poseen estos mismos, ajustando accesos según cambios en funciones o equipos.
- **MFA y Zero Trust**: Se debe implementar y exigir autenticación multifactor para acceder a datos sensibles, siguiendo un enfoque de Zero Trust.

5.2.2 Control de Identidad y Acceso

La gestión de identidades y acceso es de los pilares más críticos en un entorno de seguridad en la nube. Esta fase define cómo se validan las credenciales del usuario y los servicios, en este punto se otorgan permisos basado en roles y se auditan su cumplimiento. Para esta fase se presenta en la ilustración 10, el diagrama que modela el flujo completo del proceso, desde la definición de requisitos hasta la derivación hacia las fases posteriores del protocolo.

Luego de visualizar el diagrama y ya comprendido los mecanismos fundamentales para el control de acceso seguro, se asegura que solo los usuarios o servicios autorizados puedan interactuar con los recursos críticos, sentando una base sólida para aplicar posteriormente las medidas de protección de datos, vigilancia y prevención de fuga de la información.

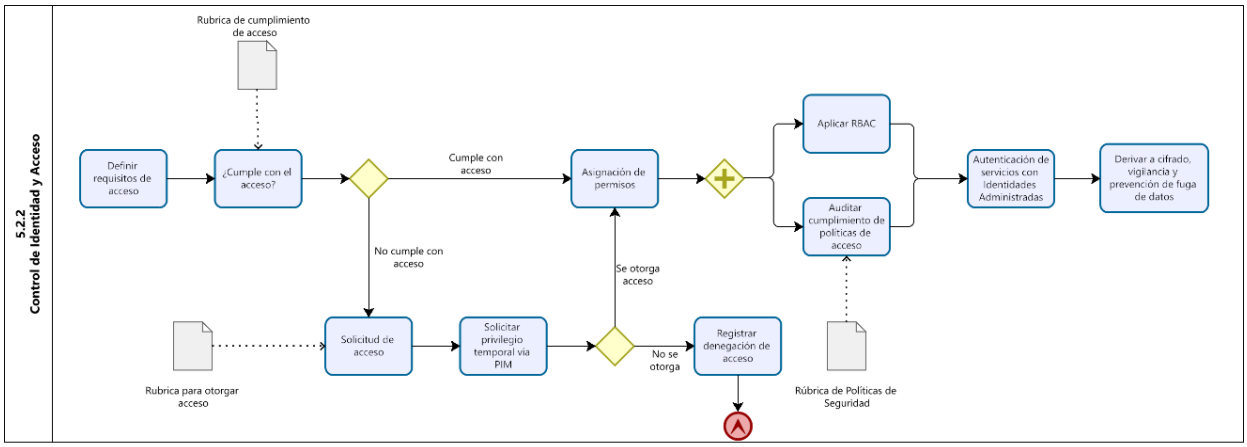

Ilustración 10: Diagrama BPMN 5.2.2.

A. Definir requisitos de acceso.

En primera instancia en este punto se deben hacer la **Autenticación y Gestión de Identidades**, la autenticación Multifactor (MFA) obligatoria mediante Azure Active Directory (AAD) representa un control critico que mejora la redundancia en seguridad, cumplimiento y reducción significativa de riesgos de accesos no autorizados. Agregando una capa adicional de verificación que contribuye a proteger las credenciales de los usuarios frente a ataques comunes. Un estudio de Microsoft en 2023 revelo que MFA bloquea más del 99% de los intentos de compromiso de cuentas (Microsoft, 2025). Para habilitar MFA a nivel organizacional, es necesario contar con una suscripción que incluya Azure AD Premium P1 o P2. Esto permite utilizar políticas de acceso condicional para aplicar MFA de forma granular.

Los métodos de autenticación recomendados incluyen.

- Microsoft Authenticator (opción preferida, con notificaciones push, códigos y opciones sin contraseña).
- Llaves de seguridad FIDO2.
- Códigos de verificación TOTP o SMS como alternativas adicionales.

Se debe configurar una política en Microsoft Entra ID que crea una política de acceso condicional.

- Aplique MFA a todos los usuarios (exceptuando únicamente cuentas de emergencia o de servicio).
- Se active para todas las aplicaciones y recursos críticos (por ejemplo, Azure Portal, Microsoft 365, recursos RBAC).
- Requiera autenticación multifactor como condición para conceder el acceso.

Durante la implementación, se recomienda iniciar con la política en modo de “solo informe” para evaluar su impacto y corregir posibles excepciones antes de activarla completamente.

Finalmente es importante tener la gestión de excepciones controladas, de esta forma las cuentas de emergencia (break-glass) puedan protegerse con autenticación fuerte y resistente a phishing, un ejemplo es FIDO2 que se mantienen documentadas, pero con acceso restringido. Para las cuentas no

humanas como scripts, automatizaciones o identidades de servicio, se deben usar identidades administradas o certificados, ya que la MFA no aplica a estos escenarios (Jaakkonen, 2025).

B. ¿Cumple con el acceso?

La **Aplicación del modelo de mínimos privilegios**, se necesita del principio del mínimo privilegio, el cual establecen los usuarios y recursos, donde solo deben tener los permisos estrictamente necesarios para realizar sus funciones, reduciendo así riesgos tales como la superficie de ataque. A continuación, se presenta la Tabla 11 que corresponde a una rubrica de cumplimiento de acceso diseñada para evaluar solicitudes según los criterios en las claves de seguridad, La rúbrica busca permitir categorizar las decisiones de acceso en tres niveles: Aprobado, Condicional o Denegado, de acuerdo con el elemento como la justificación del acceso, la clasificación del dato solicitado, el perfil del rol, las condiciones del dispositivo, el uso de MFA, la duración y alcance del acceso.

Criterio	Aprobado	Condicional	Denegado
Justificación	Clara y vinculada a funciones críticas.	Genérica o incompleta, requiere validación.	No justificada o fuera del rol.
Nivel de Sensibilidad del Dato	Corresponde al rol y está permitido.	Excede lo requerido, requiere revisión.	Dato confidencial sin respaldo adecuado.
Evaluación del Rol	Rol validado, funciones relevantes al acceso.	Rol temporal o ambiguo.	Rol sin relación, existe riesgo o conflicto.
Estado del Dispositivo	Dispositivo corporativo seguro (ej. Intune, certificado).	Dispositivo personal o no gestionado.	Dispositivo inseguro o no controlado.
MFA	Habilitado con método robusto (ej. FIDO2).	Habilitado, pero débil o incompleto.	No habilitado o incumple requisitos.
Alcance y Duración del Acceso	Temporal y justificado según necesidad.	Sin duración clara o con alcance amplio.	Indefinido, sin restricciones, representa riesgo.

Tabla 11: Rúbrica de Evaluación de Solicitudes de Acceso.

C. Solicitud de acceso.

En las **Políticas de acceso condicional en AAD (restricción por ubicación y dispositivo)**, Microsoft Entra ID permite reforzar la seguridad, controlando el acceso en función de indicadores como ubicación geográfica y estado del dispositivo.

Para realizarlo se definen ubicaciones seguras a través de rangos IP o países aprobados (“Named Locations”), generando un bloqueo por IP. Luego, se crea una política que bloquea o restringe acceso fuera de estas zonas, reduciendo el riesgo de acceso no autorizado desde ubicaciones externas, desconocidas o ajenas al perímetro definido. Por ejemplo: Solo las sedes corporativas autorizadas

pueden acceder a recursos críticos. Se excluyen cuentas de emergencia ("break-glass") para evitar bloqueos accidentales (Microsoft, 2025).

El filtrado por dispositivo se implementa con una política que requieren los dispositivos, asegurando que solo los gestionados y confiables puedan acceder a los datos sensibles. Deben estar registrados o unidos a Microsoft Entra ID, además tiene que cumplir con requerimientos de seguridad (por ejemplo, certificados, cumplimiento de Intune). Además, también pueden ser excluidos o incluidos según atributos definidos como extensiones específicas (Microsoft, 2025).

D. Solicitar privilegio temporal vía PIM.

Adicionalmente, se evalúan las solicitudes individuales de acceso, siendo fundamental auditar regularmente la implementación general de las políticas de seguridad adoptadas, Uno de los riesgos más críticos corresponde al uso de cuentas con privilegios permanentes, conocido como **Privileged Identify Management (PIM)** ya que estas representan un objetivo atractivo para atacantes y en caso de ser comprometidas, pueden derivar en accesos no autorizados a recursos sensibles. Para la problemática anterior Azure tiene a disposición la herramienta Privileged Identify Management (PIM), la cual implementa un modelo de manera de accesos que se denomina "Just-in-Time" que permite asignar privilegios administrativos de manera temporal (Microsoft, 2025). El funcionamiento de PIM permite a los usuarios con roles privilegiados no mantener esos permisos de forma continua, si no que deben de solicitarlos únicamente cuando los requieran y por un tiempo limitado, obligando a que cada elevación de privilegios pase por un proceso de aprobación, reduciendo de esta manera significativamente la exposición a amenazas asociadas a credenciales de alto nivel comprometidas. Además, PIM permite fortalecer el cumplimiento de normativas como ISO/IEC 27001 y también con NIST SP 800-53. Entre las ventajas más relevantes de PIM se encuentran:

- Reducción del riesgo de ataques por abuso de privilegios permanentes.
- Mayor trazabilidad y auditoria, esto porque cada uso de roles administrativos queda documentado y puede revisarse posteriormente.
- Integración con Zero Trust al eliminar la confianza implícita en los usuarios y exigir verificación explicita cada vez que se requieren permisos elevados.

E. Asignación de permisos.

Luego se debe **asignar permisos mínimos necesarios por usuario o servicio**, aunque esto ya está implícito en el modelo de mínimos privilegios, aquí se formaliza como una regla operativa:

- Análisis por perfil revisa las tareas reales de cada usuario o servicio y asignar únicamente los permisos estrictamente indispensables.
- Crear roles personalizados con permisos acotados.
- Documentar esta asignación como parte del proceso de alta o cambio de perfil.
- Revisar accesos trimestralmente para garantizar cumplimiento de seguridad.

F. Registro denegación de acceso.

Si ocurre que no se otorga el acceso, el sistema debe registrar adecuadamente la denegación, incluyendo la razón, la rúbrica de evaluación y la trazabilidad del evento para futura auditoria.

G. Aplicar RBAC.

Ya implementado en la sección de políticas de acceso por clasificación, **Implementar Control de Acceso Basado en Roles (RBAC)** sigue siendo la base del control de accesos en Azure:

- Uso de roles específicos y granulares según tareas definidas, evitando roles globales innecesarios.
- Configuración de alcances preciso (recurso, grupo o suscripción).

Usuarios y servicios deben recibir el mínimo privilegio necesario, como ya se describió en secciones anteriores.

H. Auditar cumplimiento de políticas de acceso.

Para garantizar que el permiso de privilegios sea coherente, seguro y justificado, se establece la siguiente rúbrica para otorgar acceso, siendo aplicable en procesos, cambios de perfil o asignación de nuevos permisos. Esto se debe revisar periódicamente para obtener los siguientes permisos:

- Ejecutar access reviews en Microsoft Entra ID (Identity Governance / PIM).
- Identificar acumulación de privilegios, accesos de usuarios inactivos o que ya no requieren permiso.
- Eliminar o ajustar accesos innecesarios encontrados.

Criterio	Cumplimiento Alto	Cumplimiento Medio	Cumplimiento Bajo
MFA activa y robusta	Obligatoria con Authenticator o FIDO2. Solo excepciones documentadas.	Solo algunos usuarios o recursos. Excepciones poco claras.	Deshabilitada o sin cobertura.
Políticas de acceso condicional	Por ubicación y dispositivos. Bloqueo fuera de zonas permitidas.	Aplicadas por grupo/usuario sin condiciones adicionales.	Inexistentes o ineficaces.
Mínimo privilegio aplicado	Roles específicos, revisiones periódicas, sin privilegios innecesarios.	Algunos roles revisados, sin control constante.	Roles amplios sin evaluación.
Uso de RBAC	Granular, documentado y revisado.	Parcial, sin personalización ni control preciso.	No implementado o mal configurado.
Gestión de cuentas especiales	Break-glass protegidas y documentadas. Identidades administradas.	Cuentas con protección débil o sin trazabilidad clara.	Genéricas, sin protección ni control.
Revisión periódica de accesos	Trimestral, con herramientas como Azure AD Access Reviews.	Esporádica y sin documentación.	No se realiza revisión de accesos.

Tabla 12: Rúbrica de Cumplimiento de Control de Acceso.

I. Autenticación de servicios con identidades administradas.

En la nube un aspecto critico se encuentra en la **administración de identidades** ya que es la forma en que los servicios y aplicaciones acceden a otros recursos. Tradicionalmente, este proceso requería almacenar credenciales de forma estáticas (contraseñas o claves de API) dentro del código o en archivos de configuración, lo cual incrementa el riesgo de exposición accidental y posibles brechas de seguridad. Para abordar esta problemática, Azure introduce las Identidades Administradas, un mecanismo que permite a los recursos de la plataforma como máquinas virtuales o aplicaciones en App Services autenticarse de manera automática en otros servicios de Azure sin la necesidad de tener que estar manejando credenciales de forma explícita. Aportando varias ventajas en términos de seguridad y cumplimiento. Al igual que el punto anterior refuerza el cumplimiento normativo de ISO/IEC 27001 y NIST SP 800-53 al garantizar que la autenticación sea gestionada de forma segura y centralizada, además también realiza el lineamiento con el modelo Zero Trust al restringir el acceso únicamente a los recursos autorizados y bajo control de las políticas del RBAC. Por último, elimina el riesgo de filtraciones de credenciales puesto que no existirán claves almacenadas en repositorios de código o archivos locales (Microsoft, 2025).

5.2.3. Cifrado, vigilancia y prevención de fuga de datos.

Aplicar mecanismos de protección para resguardar la confidencialidad e integridad de los datos es fundamental, es por lo que esta fase no se puede pasar por alto. Se consideran herramientas nativas de Azure que permiten el cifrado, la gestión segura de claves, implementación de políticas DLP y monitoreo de posibles fugas de información, la ilustración 11, presenta el diagrama a detalle, con todas las tareas que son pertinentes.

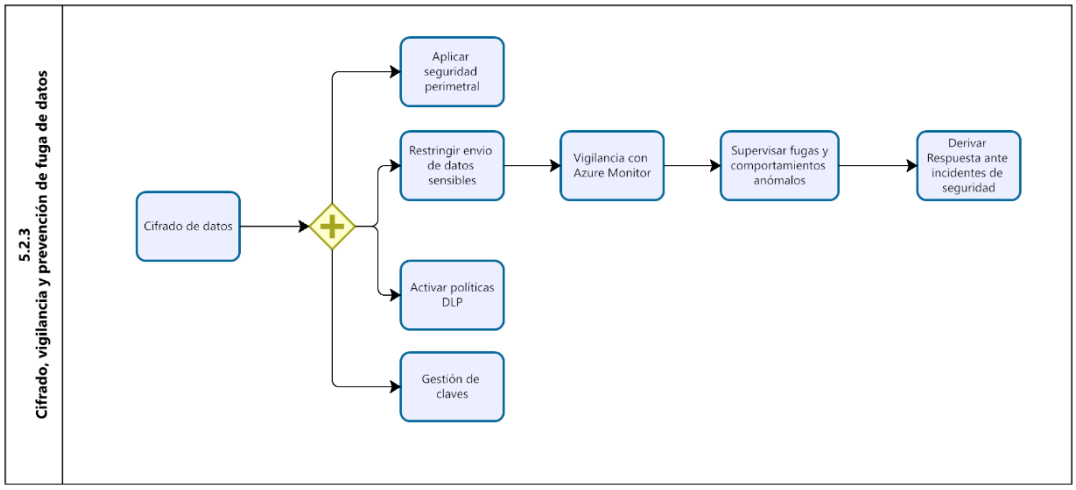

Ilustración 11: Diagrama BPMN 5.2.3.

Desde esta fase, el protocolo ya establece controles técnicos enfocados directamente a la protección activa de la información durante su ciclo de vida, fortaleciendo el perímetro de seguridad, supervisando comportamientos anómalos y asegurando el cumplimiento de políticas de prevención de fuga de datos. En esta fase las tareas implementadas permiten una detección oportuna de amenazas y la activación de respuestas automáticas para poder mitigar al máximo los riesgos antes de su materialización y no sea tarde para solucionar un posible problema.

A. Cifrado de datos.

El primer cifrado que se describe es el **cifrado de datos en reposo,** consiste en codificar la información almacenada en medios físicos o virtuales, como discos duros, bases de datos o backups, evitando que pueda ser leído por usuarios no autorizados, incluso si logran acceder al medio de almacenamientos pasando las barreras anteriormente establecidas. Es importante cifrar los datos en reposo para prevenir brechas de seguridad física o lógica, además esto cumple con diversos marcos regulatorios que exigen el cifrado en reposo siendo estos el reglamento general de protección de datos de estados unidos (GDPR), ISO/IEC 27001 y la Ley 19.628 de protección de la vida privada en Chile.

Realizar este cifrado permite reducir el impacto de filtraciones, incluso si los datos actúan como última línea de defensa. Según Microsoft cifrar los datos en reposo reduce significativamente el riesgo residual asociado a ataques físicos o internos (Microsoft, 2024). Es por lo que para cumplir lo anteriormente mencionado para tener un cifrado en reposo se aplica el cifrado automático con AES-256 para todos los datos en almacenamiento. Se implementa esta medida utilizando los mecanismos nativos de Microsoft Azure, que aplican automáticamente cifrado del lado del servidos con el algoritmo AES-256, sin necesidad de configuración manual por parte del usuario.

El algoritmo AES-256 (Advanced Encryption Standard de 256 bits) es uno de los estándares más robustos y reconocidos a nivel internacional. Y cumple con certificaciones FIPS 140-2. En Azure, este cifrado está activado por defecto para todos los datos en reposo, lo que garantiza su aplicación inmediata y continua durante todo el ciclo de vida que tiene la información. Además, el sistema admite distintos esquemas de gestión de claves:

- **Claves administradas por Microsoft (predeterminada)**: Al momento de utilizar Azure, automáticamente se encarga de crear claves, almacenarlas y rotarlas.
- **Claves administradas por cliente**: El usuario puede controlar el ciclo de vida de las claves con la herramienta Azure Key Vault, permitiendo un mayor control.
- **Clave proporcionada por el cliente**: Esta opción es la menos frecuente, se trata de que el cliente entregue la clave dinámicamente en cada operación de acceso a los datos.

Es importante a su vez tener configurado el **cifrado en tránsito**, este cifrado busca proteger la información mientras se encuentra en movimiento a través de la red, evitando que sea interceptarle, leída, alterada o suplantada durante su transferencia entre dispositivos, servicios o ubicaciones. La importancia de tener este cifrado es que previene ataques denominados como Man-in-the Middle (MITM) el cual garantiza confidencialidad e integridad durante la transmisión, cumpliendo el cifrado con las normas de seguridad GDPR, ISO 27001, PCI-DSS y recomendaciones de Azure Well-Architected Framework (Microsoft, 2024). Por lo tanto, para asegurar que todo el tráfico se mantenga cifrado durante su tránsito. El protocoló exige lo siguiente.

Implementar TLS 1.2, Vnet, VPN, ExpressRoute y Azure Virtual Network Encryption (Ver capítulo 3) resulta fundamental para asegurar el cifrado de datos en tránsito dentro de este protocolo. Para clasificar el rol de la estructura en el cifrado se realiza una comparación entre los túneles en la Tabla 13, la cual menciona el método, su respectivo alcance, la capa OSI que pertenece y la habilitación de usuario.

Método	Alcance	Capa OSI	Habilitación de Usuario
VPN Gateway (IPsec/IKE)	Local ↔ Azure, VNet-to-VNet	Red (3)	Configuración manual
ExpressRoute + MACsec	Tráfico físico dedicado	Enlace (2)	Activa MACsec en ExpressRoute Direct
Azure Virtual Network Encryption	VM ↔ VM, VNet peering	Transport (DTLS)	Activación por VM/NIC

Tabla 13: Comparación entre los túneles de cifrado en Azure.

A pesar de la implementación de cifrado en reposo y en tránsito, es fundamental contar con mecanismos que permitan detectar intentos de fuga, exfiltración o mal uso de la información sensible. Estos controles permiten anticiparse a incidentes de seguridad y activar respuestas tempranas. La siguiente rúbrica de detección de fuga de datos establece los criterios para evaluar la efectividad de estos mecanismos. La Tabla 14 establece criterios técnicos para evaluar el grado de cumplimiento de mecanismos, monitoreos y prevención de pérdidas de datos, integrando soluciones como Microsoft Sentinel, Azure Information Protection y Microsoft Purview. Esta evaluación permite auditar la capacidad del sistema para reaccionar ante incidentes y reforzar la protección del entorno cloud.

Criterio	Cumplimiento Alto	Cumplimiento Medio	Cumplimiento Bajo
Monitoreo de tráfico anómalo	Sentinel con alertas y respuestas automáticas.	Monitoreo sin alertas personalizadas.	Sin monitoreo o solo reactivo.
Políticas DLP activas	Configuradas en Microsoft 365 y Azure, con control por tipo de dato.	Generales, sin segmentación por usuario o contenido.	No existen o están desactivadas.
Detección de comportamiento anómalo	Azure Defender for Identity y UEBA habilitados.	Seguimiento parcial o sin herramientas específicas.	No se analiza el comportamiento del usuario.
Auditoría de accesos a datos	Logs activos y revisión periódica en Azure Monitor.	Logs activos sin revisión formal o centralización.	Sin registros o no se revisan.
Etiquetado de sensibilidad	Etiquetas automáticas con Microsoft Purview y protección activa.	Etiquetas manuales sin automatización ni control.	Sin clasificación ni etiquetas activas.
Respuesta ante incidentes	Playbooks activos e integrados en Sentinel.	Procedimiento manual sin estructura clara.	No existe un plan de respuesta.

Tabla 14: Rúbrica de detección de fuga de datos.

B. Seguridad perimetral.

Dentro del dominio de seguridad perimetral en Azure es la utilización de **Application Security Groups (ASG)**, el cual constituye un mecanismo lógico para agrupar máquinas virtuales (VMs) de acuerdo con su función o rol dentro de una aplicación. Este enfoque logra permite que los encargados puedan gestionar políticas de seguridad de red de manera centralizada y simplificada, sin la necesidad de asignar reglas específicas a direcciones IP individuales, dentro de la práctica, los ASG actúan como etiquetas lógicas que pueden asociarse a interfaces de redes de múltiples máquinas virtuales, logrando facilitar la aplicación de reglas coherentes en los Network Security Groups (NSG) (Microsoft, 2025).

En la ilustración 15 se muestra un ejemplo de implementación de ASG en una red virtual Azure, donde se observa la segmentación entre servidores web de lógica y base de datos y como se aplican las reglas de comunicación a nivel de grupos en lugares de direcciones IP específicas.

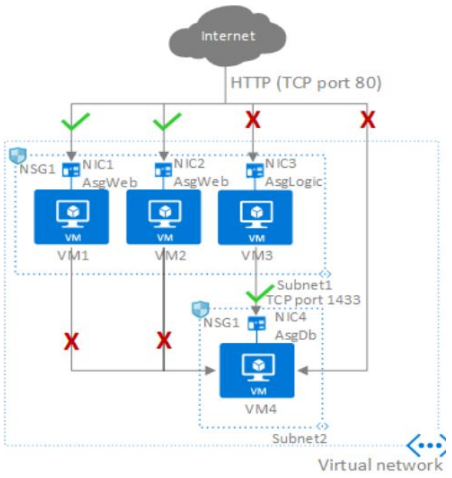

Ilustración 12: Diagrama de Application Security Groups (ASG). Obtenida de: (Microsoft, 2025).

De las principales ventajas del ASG ofrece escalabilidad y flexibilidad en entornos donde la infraestructura virtual está en constante crecimiento o modificaciones, esto porque la pertenencia de una VM a un grupo que se puede alterar manualmente las reglas de seguridad. Por otro lado, también favorece la consistencia de las políticas de acceso, pues permite definir reglas de comunicación entre las capas lógicas, que por ejemplo pueden ser front-end, lógica de negocio y bases de datos. En lugar de mantener reglas específicas para cada dirección IP, finalmente contribuyen a una administración más eficientes y segura, ya que reduce la complejidad y las probabilidades de errores humanos al configurar manualmente los NSG (kodekloud, s.f.).

Por último, es importante conocer la manera práctica de esta herramienta, que consiste en crear un ASG “Web” para los servidores de presentación, un ASG “Logic” para la capa de negocio y un ASG “Database” para el almacenamiento, luego las reglas en los NSG permiten únicamente tráfico HTTP/HTTPS desde Web hacia Logic y trafico SQL desde Logic hacia Database, logrando una segmentación interna por roles que simplifica la administración y refuerza la seguridad del entorno.

Usar **Azure Private Link,** logra ayudar a permitir el acceso a servicios PaaS de Microsoft (Azure SQL Database, Azure Storage o Key Vault) y también a servicios propios o terceros, esto a través de endpoints privados dentro de una red virtual. Este mecanismo elimina la exposición de dichos

servicios a la internet pública, porque todo el tráfico se mueve de manera interna y cifrada en la infraestructura propia de Microsoft, reduciendo de esta forma la superficie de ataque y los riesgos asociados a accesos no autorizados (Microsoft, 2025).

Este servicio muestra tres buenas ventajas, en primer lugar, garantiza una mayor seguridad y aislamiento al evitar exposición de recursos sensibles por internet. Por otra parte, aporta con simplicidad de configuración, puesto que al ser un servicio que fluye por la red de Microsoft no es necesario configuraciones complejas de firewall o VPN, finalmente favorece el cumplimiento normativo, ya que ayuda a las organizaciones a cumplir con el marco de seguridad y regulaciones de ISO/IEC 27001, NIST SP 800-53 y GDPR de la Unión Europea.

Es aquí donde aparece **Azure Bastion**, **e**ste servicio permite administrar las máquinas virtuales de manera remota a través del propio portal de Azure, sin la necesidad de exponer puertos de conexión como Remote Desktop Protocol (RDP) o Secure Shell (SSH) a la red pública, es así como Azure Bastion actúa como un puente seguro que establece sesiones cifradas directamente en el navegador, eliminando la dependencia de direcciones IP públicas y reduciendo de manera significativa la superficie de ataque de las máquinas virtuales (Microsoft, 2025). Es importante destacar que es un servicio que aporta en simplicidad operativa, ya que al trabajar solo en Azure se reduce la dificultad de estar en IPs públicas y aplicar reglas extras en los firewalls proporcionando una experiencia al usuario optimizada, permitiendo conexiones rápidas y seguras a través de navegadores estándar.

C. Activar Políticas DLP.

Las **soluciones de DLP** en la nube buscan identificar información sensible como datos financieros. PII o propiedad intelectual basadas en patrones que tengan coincidencia exacta o machine learning (zscaler, s.f.). Al momento de detectar intentos de divulgación no autorizada el sistema alerta al usuario, bloqueando la acción o mantiene la información en cuarentena, esto se implementa mediante políticas automatizadas, aplicándose sobre contenido en uso, en reposo y en tránsito con criterios específicos para cada canal. Además, el uso de **Microsoft Purview DLP** para políticas de bloqueo de transferencia de datos sensibles, esta herramienta permite implementar políticas automatizadas que detectaría y bloquea la transferencia de información confidencial hacia canales no autorizados, sean estos correos electrónicos, sitios webs externos, dispositivos extraíbles o servicios en la nube no aprobados. Esto trabaja bajo los datos clasificados inicialmente del protocolo, los confidenciales. Al momento de ser configuradas las políticas se procede a realizar las siguientes acciones.

- Bloquear la acción.
- Advertir al usuario mediante notificaciones.
- Registrar eventos detallados.

Estas acciones se aplican tanto en los entornos de Microsoft 365 (Outlook, OneDrive, SharePoint) en dispositivos de Windows 10/11 conectados con la organización y también en servicios de Azure.

D. Gestión de claves Cifrado.

Para la **Gestión de claves Cifrado**, el uso de Azure Key Vault para la gestión de claves criptográficas es crucial dentro del protocolo, ya que ofrece un almacenamiento centralizado y seguro de objetos sensibles. Según la documentación oficial, Azure Key Vault permite a las aplicaciones y los usuarios de Microsoft Azure almacenar y usar varios tipos de datos de secretos y claves" (Microsoft, 2025). Este servicio facilita el control de acceso a tokens, contraseñas, certificados y

claves criptográficas mediante Azure RBAC, lo que permite limitar el acceso de forma granular, auditar operaciones y rotar claves según políticas de seguridad. Su integración con los principios de Zero Trust.

La herramienta Key Vault considera dos modalidades importantes para la administración de claves criptográficas utilizadas en el cifrado de datos, en primer lugar, Platform-Managed Keys (PMK) en este caso Microsoft quien se encargue de generar, proteger y rotar de manera automática las claves empleadas por los distintos servicios de Azure, lo que simplifica la gestión operativa para las organizaciones. Por otro lado, Customer-Managed Keys (CMK), otorgan a las empresas la capacidad de crear, importar y administras las claves propias dentro de Key Vault, el cual asume un control total sobre su ciclo de vida, esta última es totalmente relevante en entornos donde se requiere demostrar gobernanza y trazabilidad sobre los mecanismos de cifrado ya que facilita el cumplimiento de marcos regulatorios y estándares internacionales de seguridad de la información. Además, en esta herramienta se ofrece un mecanismo que asegura el ciclo de vida completa de las claves, las cual incluye su creación segura, almacenamiento en módulos de seguridad certificados, rotación periódica, registro, auditoria en cada acceso y su eliminación segura cuando ya no son necesarias.

E. Restringir envió de datos sensibles.

Este punto tiene como propósito evitar que la información clasificada como confidencial sea enviada a través de canales no autorizados, para esto, se implementa unas reglas de restricción configuradas en las políticas de DLP, las cuales bloquean o limitan el movimiento de estos datos, activándose sobre el contenido de uso, de reposo o de tránsito. Esta regla opera sobre la base de la clasificación previa y permite aplicar bloqueos automatizados, advertencias al usuario y registros de eventos según el nivel de sensibilidad del dato que se haya detectado.

F. Supervisar fugas y comportamientos anómalos.

Para complementar las medidas de cifrado, control de acceso y DLP el protocolo establece un sistema de monitoreo robusto que permite visualizar, analizar y reaccionar ante eventos relacionados con el uso de datos sensibles, siendo este el componente central Azure Monitor. Primero se realiza la **Integración con Azure Monitor para análisis de eventos**, esto con Azure Monitor recopila logs y métricas que incluyen accesos, modificaciones, fallos de acceso y eventos relacionados con la clasificación y protección de datos.

Luego se realiza la **implementación de alertas en caso de acceso no autorizado**, **s**e crean reglas de alerta basadas en logs, por ejemplo, para detectar lecturas masivas, accesos fuera de horario o fallos repetidos de autenticación. Las alertas pueden activarse por lo siguiente:

- Lectura de datos confidenciales desde ubicaciones no autorizadas.
- Cambios de la configuración de cifrado o claves
- Incidente de DLP detectados por Purview.

Al dispararse la alerta se genera notificaciones automáticas y se pueden integrar con SIEMs como Azure Sentinel o con flujo de trabajo de respuesta automatizada.

G. Evaluación de amenazas en los datos y servicios.

Dentro del protocolo luego de que no se detectó un intento de fuga de datos es necesario hacer una evaluación de las amenazas de los datos y servicios están expuestos a diversos tipos de amenazas

que pueden comprometer la confidencialidad, integridad o la disponibilidad de los datos, entonces ¿Qué activos son evaluados?

- **Datos en reposo**: Base de datos, archivos, backups que estén en (Azure SQL, Blob Storage, Key Vault).
- **Datos en tránsito**: Estas se basan en la comunicación entre usuarios, servicios y redes, este último son (TLS, túneles).
- **Servicios críticos**: Azure AD, RBAC, Key Vault, Sentinel, Virtual Machines, aplicaciones web.
- **Identidades y roles**: Usuarios, cuentas de servicio, scripts automatizados.

Lo anteriormente se visualiza en la siguiente Tabla 15 de evaluación de amenazas.

Amenaza	Activo en Riesgo	Probabilidad	Impacto	Controles Aplicados
Phishing y robo de credenciales	Azure AD, datos sensibles	Alta	Crítico	MFA, acceso condicional, revisión de roles, UEBA
Privilegios excesivos	Datos y servicios críticos	Media	Alto	Mínimos privilegios, RBAC granular, revisión periódica
Filtración de datos cifrados	Azure SQL, Blob, backups	Media	Crítico	AES-256, Key Vault, logging, DLP
Ataques Man-in-the-Middle (MITM)	Datos en tránsito	Baja	Alto	TLS 1.2+, VPN, ExpressRoute, VNet Encryption
Exfiltración por scripts o servicios	Datos sensibles	Media	Alto	Identidades administradas, sin claves estáticas, logging
Configuración incorrecta de servicios	VMs, bases de datos, almacenamiento	Alta	Alto	Acceso condicional, auditoría, Defender for Cloud
Pérdida o corrupción de datos	Backups, servicios críticos	Media	Alto	Azure Backup, restauración validada, entorno aislado
Uso indebido de datos públicos	Portales web, bases abiertas	Baja	Medio	Control de integridad, monitoreo, marcas visuales
Amenazas internas (insiders)	Toda la infraestructura	Media	Crítico	Logging, Sentinel, separación de funciones, UEBA

Tabla 15: Evaluación de amenazas en los datos y servicios.

Como fue definido en la sección 5.2.1.E, se aplica la escala semicuantitativa de riesgo, donde:

Riesgo = Probabilidad × Impacto

Puntaje total entre 1 y 25

La siguiente Tabla 16 muestra la aplicación de esta fórmula sobre las principales amenazas identificadas en la nube, considerando los activos críticos del protocolo.

Amenaza	**Probabilidad (1–5)**	**Impacto (1–5)**	**Riesgo Total (P×I)**	**Nivel de Riesgo**	**Acción Requerida**
Phishing y robo de credenciales	5 (muy alta)	5 (crítico)	25	Crítico	Aplicación de controles avanzados y vigilancia continua
Accesos indebidos por privilegios excesivos	3 (media)	4 (alto)	12	Alto	Revisar y restringir permisos, reforzar RBAC
Filtración de datos cifrados	3 (media)	5 (crítico)	15	Alto	Auditoría de accesos, activación de alertas DLP
Ataques MITM	2 (baja)	4 (alto)	8	Moderado	Reforzar TLS y túneles seguros
Exfiltración por cuentas de servicio	3 (media)	4 (alto)	12	Alto	Controlar identidades no humanas, monitorear accesos
Configuración incorrecta de servicios	4 (alta)	4 (alto)	16	Crítico	Automatizar recomendaciones de configuración segura
Pérdida o corrupción de datos	3 (media)	4 (alto)	12	Alto	Validar backups, probar restauraciones
Uso indebido de información pública	2 (baja)	3 (medio)	6	Moderado	Aplicar control de integridad y autenticidad
Amenazas internas (insiders)	3 (media)	5 (crítico)	15	Alto	Implementar monitoreo UEBA, separación de funciones

Tabla 16: Aplicación de escala semicuantitativa en amenazas.

5.2.4 Monitoreo, Detección y Respuesta ante Incidentes de Seguridad.

En esta fase se definen los mecanismos necesarios que permiten detectar de forma proactiva cualquier tipo de incidente de seguridad que afecte la integridad, disponibilidad o hasta la confidencialidad de los datos o servicios. Por esto se implementan herramientas de Azure como Defender for Cloud, Log Analytics y Sentinel, las cuales permiten realizar escaneos automatizados, analizar registros mediante consultas KQL y activar respuestas automáticas ante comportamientos anómalos, en la ilustración 13 se puede ver el diagrama completo de cómo funciona esta fase.

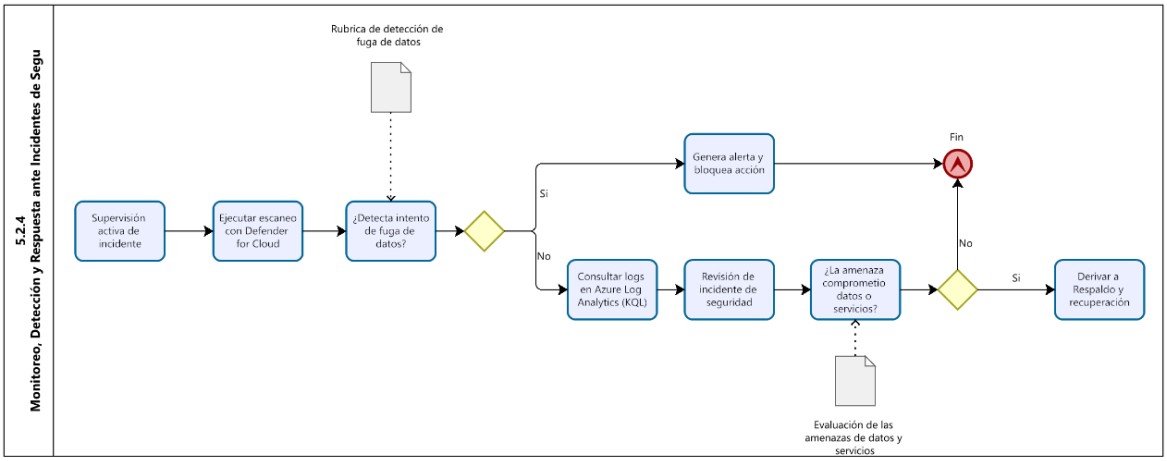

Ilustración 13: Diagrama BPMN 5.2.4.

Este apartado marca un punto vital para el protocolo, puesto que como se menciona anteriormente, es la fase que reacciona ante un evento de seguridad previo a que escalen. A través de la evaluación de amenazas y del análisis forense de registros, se define si es necesario activar procesos de restauración o contención. Con eso el sistema asegura una capacidad de respuesta estructurada, alineada con los principios de resiliencia y continuidad operativa en el entorno Cloud.

A. Supervisión Activa.

Consiste en tener una vigilancia constante en la red, sistemas y aplicaciones, con el fin de poder identificar patrones anormales, vulnerabilidades o accesos no autorizados antes de que se logre materializar el incidente. No busca limitarse a analizar logs pasivos, también busca probar y comprobar continuamente la seguridad del entorno.

B. Ejecutar escaneo con Defender for Cloud.

Uso de Microsoft Defender for Cloud para detección de amenazas, es una herramienta de seguridad que proporciona protección avanzada contra amenazas en entornos híbridos y multicloud. En el protocolo cumple el rol de detección continua de vulnerabilidades, accesos sospechosos, configuraciones inseguras y ataques en curso. La herramienta analiza el entorno de Azure y con su motor de inteligencia de amenazas permite:

- Identificar recursos expuestos, configuraciones incorrectas o falta de cifrado.
- Detectar comportamientos anormales en tiempo real (incluyendo accesos no autorizados, escalamiento de privilegios, entre otros)

- Correlacionar eventos de seguridad y priorizarlos mediante recomendaciones basadas en riesgo (Microsoft, 2025).

Para tener en claro este punto es necesario saber que una vulnerabilidad en ciberseguridad es cualquier debilidad o error en software, hardware, redes o hasta configuraciones que podrían ser explotadas por ataques, intentando acceder, alterar o destruir información de la organización. Estas fallas pueden ser ocasionadas por errores de programación, sistemas sin parches, configuraciones erróneas o haber hecho uso de malas prácticas. Según Microsoft "Una vulnerabilidad de seguridad es una debilidad en la lógica computacional (por ejemplo, el código) que, cuando se explota, provoca un impacto negativo en la confidencialidad, la integridad o la disponibilidad" (Microsoft, s.f.).

Realización de pruebas de penetración semestrales, estas pruebas consisten en simulaciones controladas de ataques que permiten descubrir vulnerabilidades no detectadas por herramientas automáticas, realizarlas con frecuencia garantiza que hasta los entornos con pocos cambios se identifiquen y corrijan fallas antes de ser aprovechadas por atacantes. Es por lo que se busca que con este protocolo disminuir al máximo los ataques realizando pruebas de penetración semestrales.

Aplicación de parches de seguridad de forma automatizada en recursos críticos, mantener un sistema actualizado es una línea primordial de defensa, puesto que sin parches suelen ser un vector común de ataque, un estudio de HIPAA Journal resalta "Las vulnerabilidades no parcheadas son ahora el principal vector de ataque en los ataques de ransomware" (Alder, 2022).

Exigiendo así aplicar parches de seguridad de forma automatizada en los recursos críticos (VMs, bases de datos, servidores expuestos) mediante herramientas disponibles en Azure como Update Management y Microsoft Defender for Cloud mencionado anteriormente.

C. Consultar logs en Azure Log Analytics (KQL).

Para este punto, es necesario configurar Azure Log Analytics para análisis forense y auditorías, al estar integrado en Azure Monitor, permite centralizar y consultar todos los registros que fueron generados por los servicios en la nube, obteniendo un acceso directo para investigar post-incidentes y la auditoria continua del sistema. Utilizando la herramienta para:

- Recopilar datos de diagnóstico desde Azure Storage, Azure SQL, Azure AD, Defender for Cloud, entre otros.
- Ejecutar consultas forenses mediante el lenguaje Kusto Query Langueage (KQL), permitiendo trazar cronologías detalladas de eventos (accesos, cambios, alertas).
- Conservar evidencia de auditoría, trazabilidad que permite reconstruir, verificar y validar las acciones realizadas en un sistema.

D. Revisión de incidentes de seguridad.

Al momento de recolectar las evidencias en el punto anterior mediante KQL, se procede con la revisión del incidente de seguridad, donde se identifican los vectores de ataque, la propagación del impacto y la efectividad de los controles aplicados. Esta etapa es clave para generar reportes, aplicar medidas correctivas y fortalecer la resiliencia futura.

5.2.5 Respaldo y Recuperación.

Esta fase busca garantizar la disponibilidad operativa del entorno cloud ante posibles incidentes o pérdidas de datos. Se establecen mecanismos automáticos de respaldo, validaciones periódicas y procedimientos de restauración utilizando herramientas como Azure Backup y Azure Site Recovery. A continuación, se detalla el flujo de respaldo y recuperación que se define en la ilustración 14.

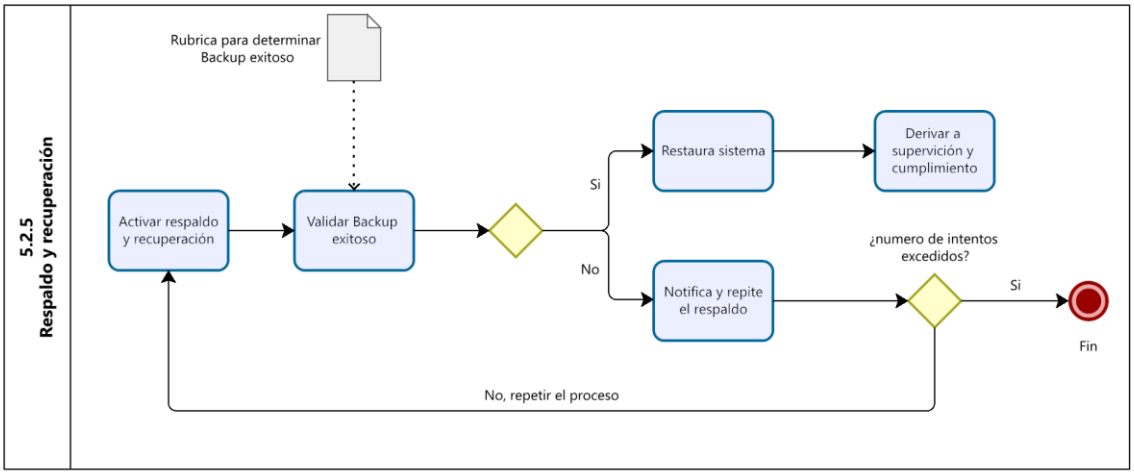

Ilustración 14: Diagrama BPMN 5.2.5.

La secuencia de la ilustración anterior permite mantener la continuidad operativa ante escenarios críticos, asegurando que los sistemas puedan ser restaurados con éxito mediante respaldos validados. El ciclo se repite automáticamente en caso de fallos hasta que este se cumpla de manera correcta y bajo las condiciones de éxito, lo que refuerza la resiliencia del entorno. Esta lógica garantiza que cualquier restauración pueda derivar de forma natural a procesos de auditoría y cumplimiento.

A. Activar respaldo y recuperación.

Las copias de seguridad son esenciales para garantizar la recuperación de los datos que están almacenados de forma segura, para poder recuperarlos en caso de pérdida, corrupción, eliminación accidental o intencional. Estos representan un pilar fundamental en cualquier estrategia de ciberseguridad y continuidad operativa ya que permiten restaurar sistemas y servicios a su estado funcional ante cualquier interrupción grave. Implementar esto de manera correcta asegura que los activos digitales puedan recuperarse en el menor tiempo posible, reduciendo el impacto operativo y financieros de una contingencia.

Es importante también tener una automatización de respaldos mediante Azure Backup con cifrado activado ya que el protocolo requiere que los sistemas críticos cuenten con respaldos automatizados que busquen asegurar mediante el cifrado, con el uso de Azure Backup como servicio centralizado de copias de seguridad, garantiza que todos los datos que se respalden estén cifrados, utilizando AES-256, se aplica esto en los datos en reposo dentro del Recovery Services vault como durante su almacenamiento en Azure Storage o durante la transferencia de datos también. Según Microsoft “Azure Backup cifra automáticamente todos sus datos de copia de seguridad mientras los almacena en la nube mediante el cifrado Azure Storage... Estos datos en reposo se cifran mediante el cifrado

AES de 256 bits (uno de los cifrados de bloque más potentes disponibles que cumple la norma FIPS 140-2)" (Microsoft, 2024). Además, permite optar por claves gestionadas por el cliente a través de Azure Key Vault, ayudando al control y trazabilidad (Microsoft, 2025). Estas medidas aseguran que los backups estén conformes a los estándares de confidencialidad, disponibilidad y regulaciones aplicables.

Aparte de lo anteriormente mencionado se debe de hacer una replicación en distintas regiones para continuidad operativa, con el fin de protegerse contra fallas sistemáticas o cortes prolongados, este protocolo exige habilitar las capacidades de replicación geográfica de Azure backup. Por defecto el uso de almacenamiento Geo-Redundant Sotrage (GRS), que replica los datos de respaldo a una región secundaria pareada. además, se recomienda activar la funcionalidad Cross Región Restore (CRR), permitiendo restaurar datos desde la región secundaria incluso cuando la primaria sigue activa (Microsoft, s.f.).

B. Validar Backup exitoso.

Para validar la efectividad operativa y técnica de las copias de seguridad implementadas, se establece la siguiente rúbrica que permite evaluar distintos aspectos claves del proceso de respaldo. La tabla 17 considera criterios como la automatización, el cifrado, la replicación geográfica, el monitoreo y el cumplimiento normativo. Cada dimensión se clasifica según su nivel de cumplimiento, lo que facilita la identificación de brechas y fortalezas en la estrategia de backups adoptada.

Dimensión	**¿Qué Evalúa?**	**Cumplimiento Alto**	**Cumplimiento Medio**	**Cumplimiento Bajo**
Automatización	Realización automática del backup	Azure Backup activo en todos los recursos críticos	Automatización parcial, requiere revisión frecuente	Manual o sin documentación
Cifrado	Protección de datos respaldados	AES-256 con claves CMK en Azure Key Vault	Cifrado por defecto (claves gestionadas por Microsoft)	Sin cifrado o no confirmado
Replicación geográfica	Continuidad operativa en otra región	GRS + Cross Region Restore habilitado y probado	Solo GRS habilitado, sin prueba de restauración	No existe replicación regional
Monitoreo y registros	Seguimiento y trazabilidad de los respaldos	Azure Monitor con alertas automáticas	Revisión manual, sin alertas ni integración	Sin monitoreo ni trazabilidad
Retención normativa	Ciclo de vida de copias y cumplimiento regulatorio	Políticas por tipo de dato y normativas ISO/GDPR	Retención básica por tiempo, sin segmentación	Sin políticas definidas, riesgo de incumplimiento

Tabla 17: Rúbrica para evaluación de backups exitosos.

C. Restaurar sistema.

Para asegurar que los sistemas pueden volver a operar después de un fallo o desastre, este protocolo integra dos mecanismos esenciales, pruebas periódicas de restauración y uso de Azure Site Recovery. Para la Implementación de pruebas de restauración periódica, se debe de realizar pruebas de restauración conocidas también como "test restores" o "disaster recovery drills", clave para validar que los respaldos se han realizado correctamente y que la recuperación se pueda ejecutar de forma eficaz. Según las mejores prácticas de Azure "No espere a que se produzca una catástrofe para descubrir que sus copias de seguridad no funcionan como esperaba" (Bertram, 2024). Las pruebas tienen una secuencia especifica siendo está de la siguiente forma:

1) En un entorno aislado para evitar interferencias con sistemas de producción.
2) Ejecutarse con una frecuencia previamente definida.
3) Registrar detalladamente los resultados obtenidos.
4) Formar parte de un plan formal de recuperación.

El protocolo contempla la integración de Azure Site Recovery (ASR) como mecanismo fundamental de continuidad operativa ante escenarios de desastre. Esta herramienta permite replicar cargas de trabajo y máquinas virtuales desde una región principal hacia una región secundaria de Azure o incluso hacia entornos locales, garantizando así la alta disponibilidad de los servicios críticos y una recuperación rápida en caso de interrupciones mayores. Azure Site Recovery permite definir un plan de recuperación ("Recovery Plan") donde se establece el orden, condiciones y dependencias entre sistemas al momento de restaurar, lo cual es esencial para evitar errores en ambientes complejos. Además, automatiza gran parte del proceso, reduciendo la intervención humana y acelerando los tiempos de respuesta.

Según Microsoft, "ASR simplifica la recuperación ante desastres al automatizar la replicación de máquinas virtuales y al permitir realizar pruebas sin afectar la producción" (Microsoft, 2025). Esto no solo refuerza la resiliencia técnica de la organización, sino que también permite cumplir con marcos normativos internacionales como ISO 22301. Dentro de este protocolo, ASR debe estar habilitado al menos para las cargas de trabajo clasificadas como críticas, y sus funcionalidades deben integrarse con Azure Backup y el monitoreo centralizado. Asimismo, se deben ejecutar pruebas programadas de failover para validar su funcionamiento, garantizando que la recuperación se pueda ejecutar sin pérdida de datos ni afectación operativa prolongada.

5.2.6 Supervisión, Cumplimiento y Auditoría.

Este punto es el último del protocolo, fase la cual busca mantener el entorno Cloud en constante evaluación, garantizando que las políticas implementadas se mantengan vigentes, efectivas y alineadas con las normativas. Además, se prioriza el uso de herramientas que permitan registrar, revisar y actuar sobre posibles desviaciones.

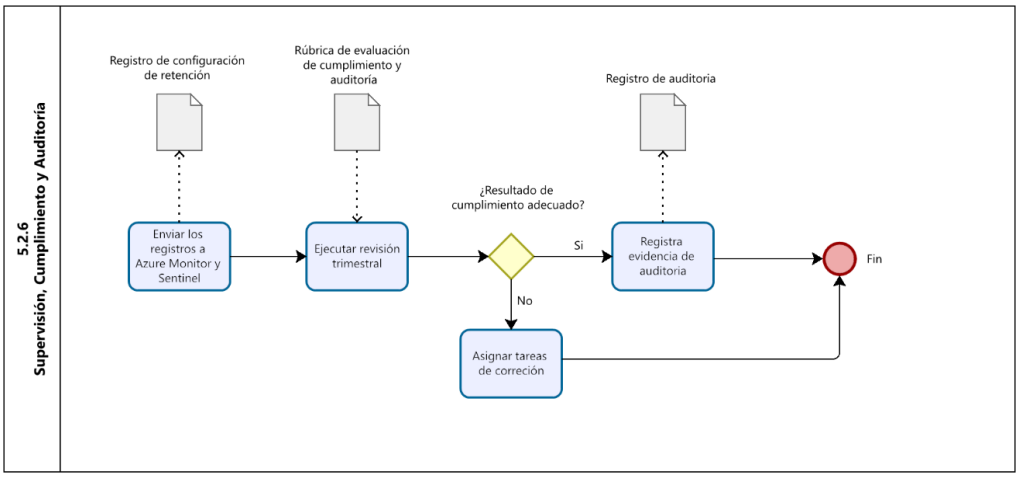

Ilustración 15: Diagrama BPMN 5.2.6.

Luego de visualizar el ciclo iterativo en la ilustración 15, este permite mantener una trazabilidad efectiva y proactiva sobre el cumplimiento de las políticas, asegurando la corrección oportuna de desviaciones mediante tareas específicas. La integración de auditorías periódicas y el uso de evidencias documentadas refuerzan el cumplimiento normativo, proporcionando un cierre formal a cada ejecución del protocolo.

A. Envió de registros a Azure Monitor y Sentinel.

Es un pilar fundamental para garantizar la seguridad, cumpliendo con las normas y la capacidad de respuesta ante incidentes. Estos registros permiten documentar todas las acciones relevantes que ocurren en los servicios, aplicaciones y usuarios dentro del entorno cloud, logrando proporcionar evidencia confiable para auditorias, análisis forenses y detección temprana de comportamiento anómalos. Todos los recursos implementados en Azure deben tener habilitada la generación y envíos de registros hacia Azure Monitor Logs y Microsoft Sentinel, permitiendo una supervisión continua del entorno.

Azure Monitor se encarga de recopilar las métricas y registros de diagnóstico tales como las actividades de red, acceso a almacenamiento, cambios de configuración, entre otros. Para luego almacenarlos en Log Analytics Workspaces para análisis detallados. Por otro lado, Microsoft Sentinel como solución de Security Information and Event Management (SIEM) permite correlacionar esos registros en tiempo real, identificando patrones sospechosos y activar alertas o respuestas automatizadas ante anomalías o amenazas. Además, según las normativas de ISO/IEC 27001, GDPR y la ley N°19.628 exige la conservación de los registros de auditoría por al menos 12 meses. La ventaja de utilizar Log Analytics, es que la información se puede retener hasta 730 días.

B. Ejecutar revisión trimestral.

La **evaluación continua** es esencial para mantener la eficiencia del protocolo de ciberseguridad a lo largo del tiempo. La gran ventaja de incluir este apartado es que busque garantizar que las medidas implementadas no solo sean vigentes al momento de implementarse, si no que se adapten proactivamente a nuevas amenazas, vulnerabilidades o actualizaciones en los marcos regulatorios. Permitiendo identificar desviaciones, corregir brechas y fortalecer la gobernanza de los

datos de forma iterativa y sistemática. La revisión trimestral con Compliance Manager de Microsoft, se establece un periodo de tiempo, en este caso será una revisión cada tres meses, utilizando la herramienta Microsoft Purview Compliance Manager, la cual proporciona una evaluación estructurada del nivel de cumplimiento de la organización frente a normativa internacional y chilena. Permitiendo así lo siguiente.

- Obtener una puntuación de cumplimiento a tiempo real, calculando en base al porcentaje de controles implementados, eficientes y revisados.
- Generar tareas automáticas con responsables asignados, fechas limite y enlaces a evidencias requeridas.
- Centralizar la documentación para auditorías internas o externas.
- Identificar brechas normativas y técnicas junto con sugerencias de mitigación específicas para entornos Azure, Microsoft 365 y otros servicios entregados.

C. Asignar tareas de corrección.

Este punto ocurre cuando el resultado de la evaluación revela desviaciones o incumplimientos, es aquí donde se genera el plan de acción con tareas correctivas asignadas, responsables definidos y seguimiento a través de las herramientas de gestión integradas, por ejemplo, Compliance Manager de Microsoft.

D. Registrar evidencia de auditoría.

Para asegurar que los procesos de cumplimiento y auditoría descritos se mantengan efectivos, actualizados y alineados con los estándares regulatorios, se establece la siguiente Tabla 18, la cual es una rúbrica de evaluación de cumplimiento y auditoría.

Criterio	Cumplimiento Alto	Cumplimiento Medio	Cumplimiento Bajo
Logging en servicios Azure	Habilitado en todos los recursos críticos. Centralizado en Log Analytics.	Logging parcial; solo algunos recursos críticos.	Deshabilitado o inexistente
Integración con Monitor y Sentinel	Operativos con alertas activas. Integración SIEM funcional.	Habilitados, pero sin alertas o integración completa.	Sin integración. Sin detección de anomalías
Retención de logs	Política activa por 12 meses o más. Alineado con normas GDPR/ISO.	Retención menor o no documentada.	No cumple normativa o sin política
Revisión del cumplimiento	Revisión trimestral con Compliance Manager. Evidencias registradas.	Revisión ocasional o sin respaldo formal.	No se revisa ni audita cumplimiento
Gestión de hallazgos	Tareas correctivas asignadas y cerradas con evidencia.	Brechas sin seguimiento ni cierre formal.	No hay registro ni acciones ante desviaciones

Tabla 18: Rúbrica de Evaluación de Supervisión y Cumplimiento.

Esta rúbrica permite verificar el grado de implementación y madurez de los mecanismos de trazabilidad, supervisión y mejora continua dentro del entorno Azure.

5.3 Medidas técnicas y herramientas de seguridad (Testing).

Este apartado tiene como finalidad realizar las pruebas correspondientes de validación sobre la implementación del protocolo en el entorno de Azure. Mediante estas verificaciones y pruebas fue posible comprobar que los controles técnicos diseñados funcionan correctamente en los casos permitidos por la suscripción gratuita, así como también permite identificar las limitaciones que impidieron una implementación completa de determinadas funcionalidades. Para facilitar el análisis, el testing se estructuró conforme a las fases previamente definidas en el protocolo (5.2.1 a 5.2.6).

5.3.1 Clasificación y evaluación de datos (5.2.1).

En primer lugar, se crearon los tres almacenes diferentes necesarios: confidencial, interno y público. Los cuales están asociados a su respectivo grupo de recurso, además cada uno de estos almacenes fue configurado para reflejar el nivel de sensibilidad de los datos que contendrían.

Para el almacén confidencial se restringe el acceso por red, habilitando solo la conexión desde la dirección IP del cliente autorizado. Con dicha configuración se comprobó que la cuenta rechazaba intentos de acceso no autorizados, cumpliendo con los lineamientos de confidencialidad lo que se puede ver en la ilustración 16.

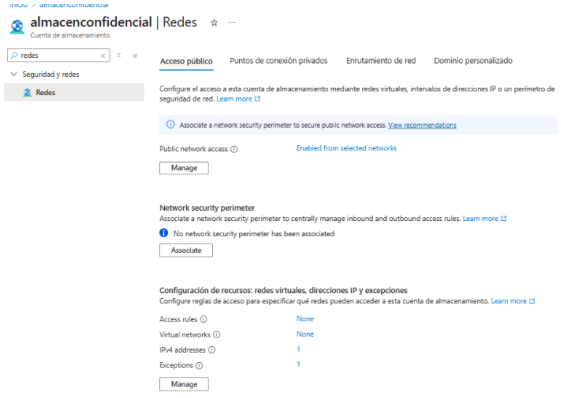

Ilustración 16: Configuración de red en "solo IP cliente" en AlmacenConfidencial.

Para el almacenamiento interno se mantuvo el acceso desde todas las redes, pero los contenedores se configuraron con nivel de acceso en privado, lo que obligaba a la autenticación de los usuarios con roles previamente otorgados. Al intentar acceder a un archivo directamente mediante un enlace, el sistema solicitó credenciales, mostrando el correcto funcionamiento de la política de acceso interno como se demuestra en la ilustración 17 y en la ilustración 18 se evidencia el error solicitando credenciales al intentar abrir un archivo interno.

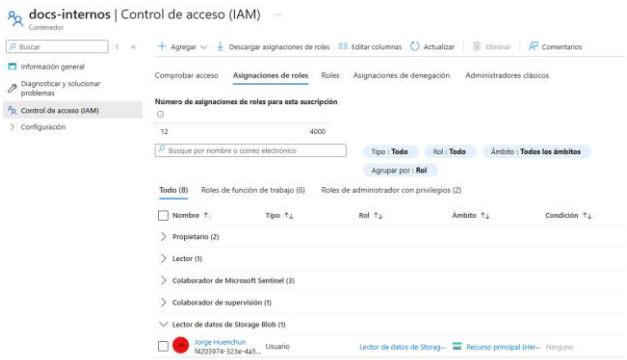

Ilustración 17: Permisos del contenedor privado en AlmacenInterno.

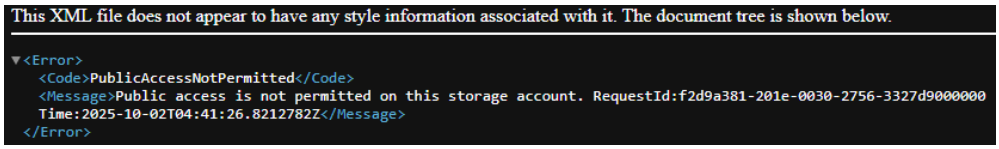

Ilustración 18: XML de error solicitando credenciales al intentar abrir un archivo interno.

En el almacén público se configuró un contenedor denominado docs-publicos con nivel de acceso blob (anónimo). Luego, se subió un archivo de prueba y se comprobó que este era accesible desde cualquier navegador sin necesidad de credenciales, validando así el acceso público para información de libre distribución como en la ilustración 19 junto a la 20 demostrando el archivo accesible en navegador sin credenciales.

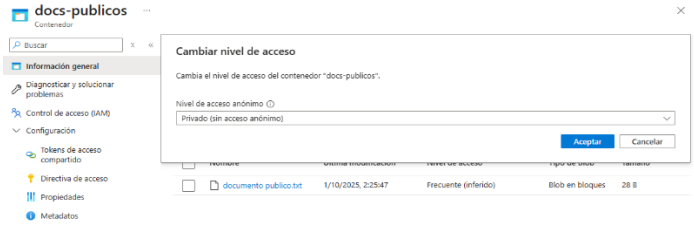

Ilustración 19: Nivel de acceso del contenedor público.

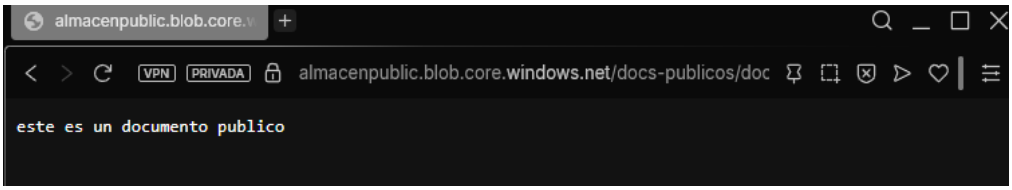

Ilustración 20: archivo accesible en navegador sin credenciales.

En este punto se encontró la limitación de etiquetado automático que se utiliza con Microsoft Purview no se encontraba disponible con la suscripción gratuita.

5.3.2 Control de Identidad y Acceso (5.2.2).

Para este punto se verificó la aplicación de RBAC (Role-Based Access Control) mediante la asignación de permisos diferenciados sobre las cuentas de almacenamiento y otros recursos críticos. A través de Azure Cloud Shell se listaron los roles efectivos de cada usuario y recursos, confirmando la asignación de permisos como Lector, Contribuidor y el administrador de Key Vault en la ilustración 21 se ven en función de las necesidades del protocolo.

Principal	Role	Scope
jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Owner	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f
jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Owner	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f
jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Reader	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f/resourceGroups/GR-Interno
jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Monitoring Contributor	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f/resourceGroups/GR-Interno
jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Reader	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f/resourceGroups/GR-Confidencial
jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Key Vault Administrator	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f/resourceGroups/GR-Confidencial/providers/Microsoft.KeyVault/vaults/KV-Confidencial
jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Key Vault Crypto Service Release User	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f/resourceGroups/GR-Confidencial/providers/Microsoft.KeyVault/vaults/KV-Confidencial
8ee8fdad-f234-4243-8f3b-15c294843740	Microsoft Sentinel Contributor	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f
8ee8fdad-f234-4243-8f3b-15c294843740	Microsoft Sentinel Contributor	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f
fc780465-2017-40d4-a0c5-307022471b92	Microsoft Sentinel Contributor	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f

Ilustración 21: Roles asignados.

Además, la tabla 19 muestra que Azure exporta en un csv los roles visualizando todos los roles y la información necesaria.

RoleAssignmentId	Scope	DisplayName	SignInName	RoleDefinitionName
dffafa7d-7404-404b-b1c3-269185b0c983	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f	Jorge Huenchun	jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Propietario
c170371d-b668-474d-ac15-3b959fa0544c	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f	Jorge Huenchun	jorgehuenchun7a_gmail.com#EXT#@jorgehuenchun7agmail.onmicrosoft.com	Propietario
80d9675f-8895-4fa3-b5a6-a8d1843e2f09	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f	Microsoft Threat Protection		Colaborador de Microsoft Sentinel
0800ce70-411f-4919-bbe1-628ab59e0858	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f	Microsoft Threat Protection		Colaborador de Microsoft Sentinel
c046d695-1852-443a-ab3f-7726525e7196	/subscriptions/1c7066e2-6dad-442b-803f-dd883bb49a4f	WindowsDefenderATP		Colaborador de Microsoft Sentinel

Tabla 19: Csv de roles exportados.

Adicional se probó el acceso a los contenedores con usuarios sin rol asignado, obteniendo como resultado la denegación de acceso, lo que valida que el sistema si cumple con el principio de mínimos privilegio.

En este punto se encontró que la suscripción gratuita no permitió habilitar Privileged Identity Management (PIM) ni Access Reviews, funcionalidades que en un entorno empresarial habría permitido gestionar los accesos temporales y auditorias periódicamente de los permisos.

5.3.3 Cifrado, Protección y prevención de fugas (5.2.3).

Para el cifrado confirmaron que todos los recursos de almacenamiento fueron creados con cifrado habilitado por defecto mediante claves administradas por Microsoft. La ilustración 22 muestra el panel de “cifrado” en AlmacenConfidencial, donde se validó este mecanismo fue validado al consultar la sección de cifrado de cada cuenta, donde se evidenció que ningún archivo podría almacenarse sin ser protegido automáticamente.

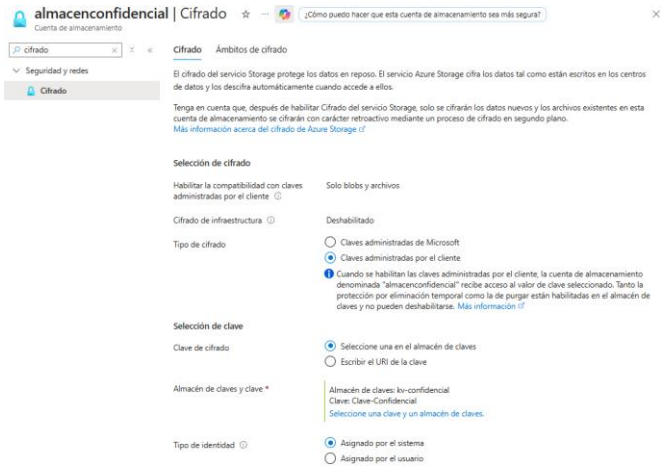

Ilustración 22: Panel de "Cifrado" en AlmacenConfidencial mostrando cifrado activo.

En esta fase se intentó configurar el cifrado con las claves administradas por el cliente (CMK) alojadas en Azure Key Vault, sin embargo, la opción se encontró restringida con la suscripción gratuita, esta al no estar disponible la activación de identidades administradas para la cuenta de almacenamiento. La ilustración 23 se evidencia el error al intentar activar la asignación por el sistema, lo que obligó a utilizar la medida alternativa, se utilizó el rol Key Vault Administrator sobre el recurso KV-Condifencial para manejar claves manualmente, dejando la integración automatizada como diseño propuesto.

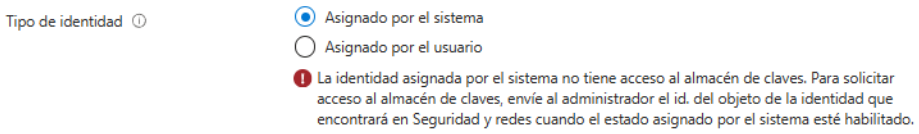

Ilustración 23: Error al intentar activar la asignación por el sistema en la cuenta de almacenamiento.

5.3.4 Monitoreo, Detección y Respuesta (5.2.4).

En este punto se validó la integración de la máquina virtual, la denominada MV-Ciberseguridad con el área de trabajo de Log Analytics, esto con consultas KQL como Heartbeat, se confirmó que los registros eran enviados correctamente, generando evidencia de actividad y conectividad del agente de monitoreo. La ilustración 24 presenta la captura de la consulta en Log Analytics con los resultados obtenidos.

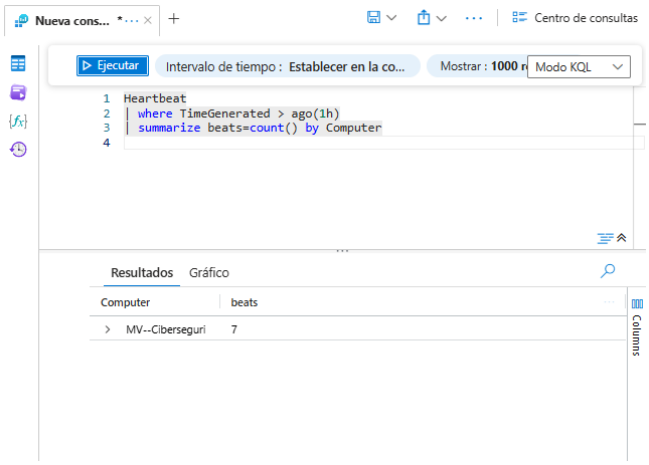

Ilustración 24: Captura de consulta KQL en Log Analytics con resultados.

Adicionalmente, se habilitó Microsoft Defender for Cloud que emitió múltiples recomendaciones de seguridad como la necesidad de proteger discos de máquinas virtuales o reforzar configuraciones en cuentas de almacenamiento. Estas alertas evidencian la capacidad del sistema para detectar configuraciones inseguras y generar directrices de remediación como se puede ver la ilustración 25 con el listado de recomendaciones.

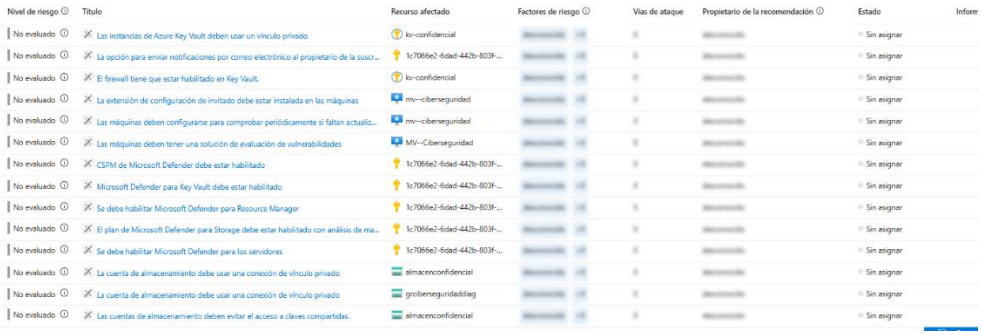

Ilustración 25: Listado de recomendaciones en Defender for Cloud.

En este punto el uso de Microsoft Sentinel en su versión completa no fue posible debido a las restricciones de la suscripción, por lo que las pruebas se limitaron al monitoreo y alertas básicas.

5.3.5 Respaldo y Recuperación (5.2.5).

La prueba de respaldo se realizó configurando un Recovery Services Vault asociado a la máquina virtual MV-Ciberseguridad. Una vez creado el contenedor de recuperación, se activó la política de backup, validando posteriormente la existencia de un punto de recuperación en el almacén. La ilustración 26 muestra la lista de "Elementos de copia de seguridad" con la VM protegida, y la ilustración 27 evidencia el estado correcto de la copia de seguridad de la máquina virtual.

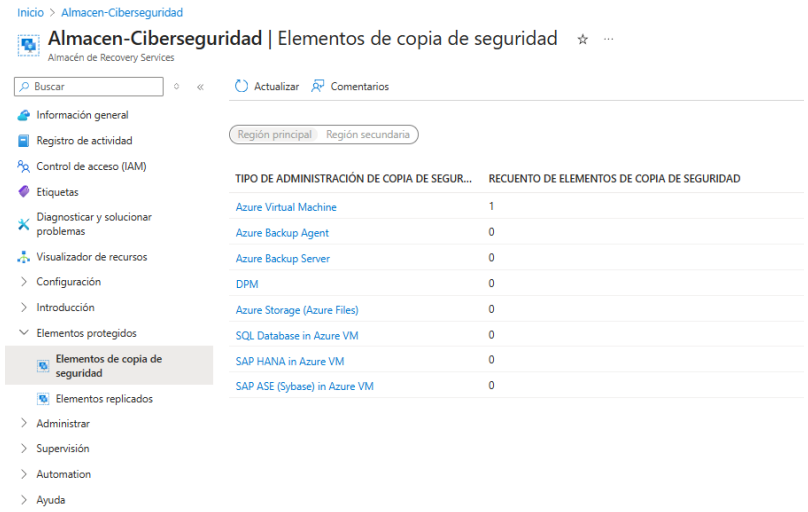

Ilustración 26: Lista de "Elementos de copia de seguridad" mostrando la VM protegida.

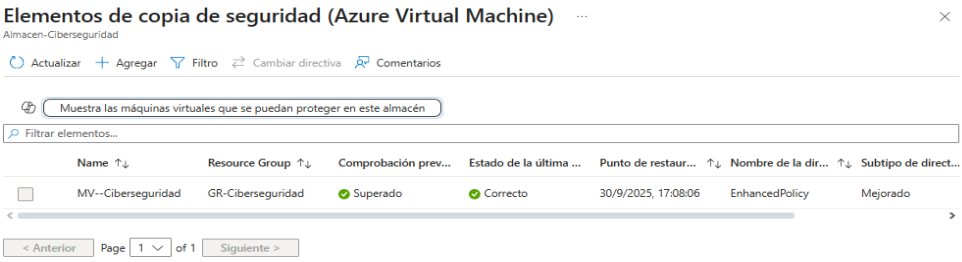

Ilustración 27: Estado de la copia de seguridad de la máquina virtual.

Este resultado de las ilustraciones confirma que el sistema de respaldo funciona adecuadamente, permitiendo restaurar la VM en caso de falla o incidente.

5.3.6 Supervisión, cumplimiento y auditoria (5.2.6).

Finalmente, se validaron las políticas de cumplimiento a través de Azure Policy, obteniendo un reporte donde se reflejó que un porcentaje de los recursos aparecían como No conformes. Esto ocurrió principalmente a configuraciones avanzadas que no podían aplicarse con la suscripción gratuita. La ilustración 28 muestra el Dashboard de Azure Policy, donde se observa un 18% de compatibilidad.

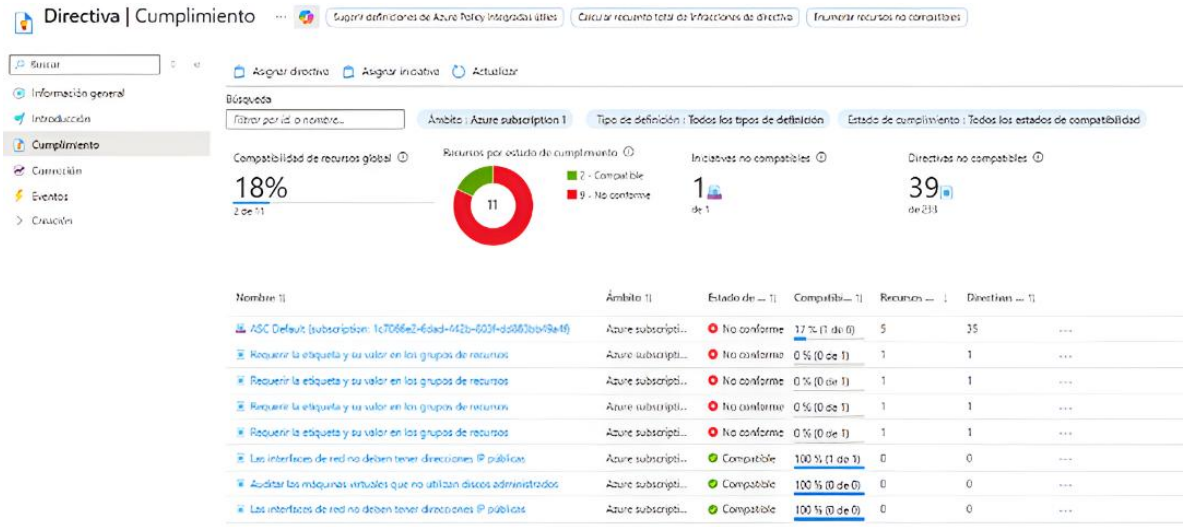

Ilustración 28: Dashboard de Azure Policy con 18% de compatibilidad.

El hallazgo fue documentado como evidencia de que el protocolo es capaz de auditar el estado de los recursos, aunque ciertas no conformidades permanecen sin resolución debido a limitaciones externas al diseño del protocolo. Este 18% de compatibilidad es un pequeño porcentaje de los recursos en la suscripción de Azure están completamente alineados con las políticas de seguridad establecidas, es importante destacar que este porcentaje está directamente influenciado por las limitaciones de la suscripción gratuita de Azure, la cual causa una restricción en el acceso a ciertas funcionalidades claves, como el uso de herramientas avanzadas como Microsoft Purview para etiquetado automático, la integración de identidades administradas para el cifrado con claves de cliente (CMK) y la activación completa de Microsoft Sentinel. Estas limitaciones afectan negativamente la implementación completa del protocolo de seguridad y la capacidad de asegurar el cumplimiento total de las políticas. En un entorno con una suscripción completa, es razonable esperar un nivel de cumplimiento mucho más alto, ya que todas las funcionalidades necesarias para un control completo y la implementación de las políticas de seguridad estarían disponibles. En este contexto el 18% de compatibilidad no refleja el rendimiento esperado de un protoclo bien implementado en un entorno empresarial, si no que resalta las restricciones actuales debido al uso de una suscripción limitada.

5.3.7 Evaluación del porcentaje de implementación del protocolo.

Al encontrar limitantes en el testing fue necesario cuantificar el nivel de implementación alcanzado en el protocolo de ciberseguridad propuesto, se definió un criterio de evaluación basado en todas las fases descritas en el apartado 5.2. Cada fase fue evaluada considerando tes posibles estados.

- Cumplida completamente (1 punto): la funcionalidad fue implementada y probada exitosamente.
- Cumplida parcialmente (0,5 puntos): la funcionalidad fue implementada de forma parcial, presentado limitaciones derivadas de la suscripción gratuita.
- No cumplida (0 puntos): la funcionalidad no pudo implementarse en el entorno de prueba, quedando únicamente como diseño conceptual.

La tabla 20 resume los resultados obtenidos en la evaluación de cada fase del protocolo. Gracias a esta evaluación el protocolo logró implementar de manera efectiva la mayoría de las fases diseñadas con un 83% de cumplimiento dentro de las restricciones que son impuestas por la suscripción gratuita de Azure, las principales limitaciones son el uso de Microsoft Purview para etiquetado automático, la integración de identidades administradas para cifrado con clave de cliente (CMK) y la activación completa de Microsoft Sentinel. Bajo términos metodológicos, este análisis permitió validar empíricamente que el protocolo es factible y operativo bajo un contexto limitado para poder tener una correcta activación con una licencia mejor, marcando un punto a de mejora a futuro, dado que todas estas funcionalidades están contempladas en el diseño y solo dependen de un entorno con acceso correspondiente.

Fase del protocolo	**Descripción resumida**	**Estado de implementación**	**Puntaje**
Clasificación y evaluación de datos (ver 5.2.1)	Configuración de tres niveles de almacenamiento (confidencial, interno y público) con restricciones diferenciadas.	Cumplida	1
Control de Identidad y Acceso (RBAC) (ver 5.2.2)	Asignación de roles y permisos diferenciados; validación de acceso por roles.	Cumplida	1
Cifrado, vigilancia y prevención de fuga de datos (ver 5.2.3)	Cifrado por defecto habilitado, prueba con claves en Key Vault limitada por suscripción.	Parcial	0,5
Monitoreo, Detección y Respuesta (ver 5.2.4)	Log Analytics funcionando, consultas KQL ejecutadas; Defender for Cloud entregó alertas. Sentinel completo no disponible.	Parcial	0,5
Respaldo y Recuperación (ver 5.2.5)	Configuración de Recovery Services Vault, verificación de copia de seguridad de VM.	Cumplida	1
Supervisión, Cumplimiento y Auditoría (ver 5.2.6)	Reportes de cumplimiento en Azure Policy, se evidenciaron limitaciones por recursos no conformes.	Cumplida	1

Tabla 20: Checklist de implementación del protocolo.

Es importante mencionar que las pruebas realizadas en este trabajo se asumieron que los repositorios con datos estaban inicialmente vacíos y que los datos de pruebas se cargaron manualmente, simulando la recepción de información desde los sistemas correspondientes. Esta suposición se hizo debido a la naturaleza del entorno de prueba, los cuales no incluyen datos reales ni de usuarios humanos. En un entorno de producción real, los repositorios estarían llenos de datos provenientes de fuentes externas o internas, por lo que se requiere realizar pruebas con datos reales para validar adecuadamente el funcionamiento del protocolo. Dado que la implementación se realizó en un entorno controlado mediante una máquina virtual, donde tampoco fue posible probar el sistema con usuarios reales, ni con datos sensibles de una organización. Las pruebas se centraron en la validación técnica del protocolo y se recomendó realizar pruebas adicionales con datos reales una vez que se obtenga un entorno empresarial con licencias completas.

6. CONCLUSIONES Y RECOMENDACIONES.

6.1 Conclusiones.

El desarrollo de este protocolo de ciberseguridad en la nube basado en Microsoft Azure surge de la necesidad concreta de poder dotar a las organizaciones de un marco estructurado, coherente y adaptable para la protección de sus datos e infraestructuras en los entornos cloud. En un contexto en que la migración a la nube se ha acelerado, pero en el que permanecen desafíos vinculados a la gestión de accesos, la clasificación de datos, la trazabilidad, la detección de incidentes y la recuperación ante desastres, volviéndose imprescindible contar con protocolos claros y basados en buenas prácticas internacionales.

En relación con el Objetivo 1: Seleccionar distintos procesos y secuencias lógicas que permitan un ciclo eficiente en un protocolo de ciberseguridad en la nube. Se concluye que el uso de fases claramente definidas (clasificación de datos, control de acceso, cifrado, monitoreo, respaldo y cumplimiento) permitió construir una secuencia lógica y eficiente, operaciones que fueron representadas en un diagrama BPMN que al estar diseñado en un único esquema global y posteriormente desglosado en diagramas específicos por fases se logra una representación clara del flujo de seguridad que incluye actividades, decisiones, roles y herramientas aplicadas en cada etapa para una mejor comprensión para cualquier equipo de seguridad de una empresa. Esta eficiencia se logró comprobar mediante la reducción de redundancias entre fases, realizando trazabilidad de las tareas en el modelo BPMN y la validación práctica del flujo en Azure, que permitió completar los procesos sin interrupciones ni pasos innecesarios.

Respecto al Objetivo 2: Modelar el protocolo de seguridad de datos en Microsoft Azure utilizando notación BPMN y políticas de acceso, se logró estructurar un modelo modular y aplicable con una suscripción gratuita que a pesar de las limitaciones es un protocolo fundamentado en normas internacionales (ISO/IEC 27001, NIST SP 800-53, GDPR) y por parte las normas chilenas con la Ley 19.628. El protocolo fue diseñado en base a herramientas nativas de Azure como Azure Policy, Microsoft Entra ID, Defender for Cloud, Key Vault, entre otras. Con esto se asegura su coherencia con el ecosistema de Microsoft y su aplicabilidad real.

En cuanto al Objetivo 3: Implementar y evaluar medidas técnicas del protocolo en un entorno controlado de Azure, al realizar el testing completo se pudieron identificar limitantes que se mencionan de forma más específica en el capítulo 6.3, pero aun así se alcanzó un nivel de implementación del 83% de las funcionalidades propuestas, de acuerdo con la evaluación presentada en el capítulo 5.3. Este porcentaje se calculó considerando el total de funcionalidades planificadas frente a las que fueron implementadas de manera efectiva en Microsoft Azure por los registros de configuración y pruebas documentadas en la tabla de evaluación del capítulo 5.3, lo que permite cuantificar la viabilidad técnica del modelo con base en evidencias concretas. Las pruebas demostraron el correcto funcionamiento de medidas como la restricción de accesos en cuentas de almacenamiento, la asignación de roles RBAC, la habilitación de cifrado por defecto, la detección de vulnerabilidades mediante Defender for Cloud y la creación de respaldos con Recovery Services Vault. Pero, al contrario, ciertas funcionalidades avanzadas como el etiquetado automático de datos con Microsoft Purview, la integración de identidades administradas y la versión completa de Microsoft Sentinel. Estas quedaron documentadas como diseño conceptual debido a las limitaciones de la suscripción gratuita utilizada, Es bajo esta idea que se calcula el 83% de implementación, con las herramientas que se establecieron de un inicio contra las que no se pudieron implementar por limitaciones.

Finalmente, en el Objetivo 4: Depurar el protocolo, formulado en el objetivo 2, con evaluación de un experto de ciberseguridad, de acuerdo con los errores identificados en el objetivo 3. El modelo fue sometido a la revisión de dos especialistas en ciberseguridad en la nube, quienes validaron la pertinencia del enfoque y la coherencia del diseño propuesto. Si bien la retroalimentación se recibió a través de correos electrónicos y no mediante informes formales, este feedback permitió ajustar detalles en la redacción, reforzar la estructura del BPMN, herramientas a utilizar y áreas a mejorar para poder confirmar la aplicabilidad del protocolo en entornos reales.

El protocolo alcanzó los objetivos propuestos, se logró diseñar una secuencia estructurada de operaciones de seguridad, donde se implementó un modelo de ciberseguridad aplicable en Azure, se realizaron pruebas prácticas que confirmaron la viabilidad del diseño en un 83% y se depuró el modelo con apoyo experto. Este trabajo representa un aporte en la sistematización de buenas prácticas de seguridad en la nube, ofreciendo a las organizaciones una guía clara, modular y adaptable para fortalecer su postura de seguridad en un contexto digital cada vez más complejo y exigente.

Es importante señalar que, aunque el protocolo ha sido exitoso en su diseño, este mismo requiere una considerable participación humana en las primeras etapas de implementación, lo cual puede ser engorroso para algunos equipos que busquen implementar este diseño en su empresa, especialmente en organizaciones pequeñas con recursos limitados. Ya que, en las primeras fases, donde se definen políticas de acceso, configurando el cifrado, establecer roles, revisión de configuraciones, es necesario un esfuerzo significativo de intervención humana para asegurar que todo funcione correcto. Si bien, es una carga inicial importante, aunque garantiza una correcta implementación, puede ser un obstáculo para las organizaciones que no cuentan con un equipo profesional dedicados o con la capacidad de destinar tiempo a tareas que son manuales y demandan atención constante. A medida que el protocolo se afianza y se automatizan más procesos, esta carga podría disminuir, pero si es algo importante a considerar.

6.2 Recomendaciones.

Dentro de todas las áreas de la informática es fundamental mantener actualizado los conocimientos y herramientas, por esa razón el protocolo es primordial mantenerlo actualizado frente a la evolución de las amenazas y equipos, cambios en las normativas o transformaciones de la propia organización. Se sugiere calendarizar revisiones semestrales o anuales con anticipación de las áreas de TI, seguridad, cumplimiento y usuarios clave con el fin de garantizar que las medidas adoptadas sigan siendo pertinentes y efectivas.

De la mano con lo anterior, el factor humano es uno de los principales vectores de ataque en la ciberseguridad. Es por esto por lo que es crucial establecer un programa de capacitación y concientización continua para los colaboradores, idealmente se abarque desde la clasificación de los datos a la respuesta ante incidentes y la respuesta inmediata a eventos sospechosos. Un plan de entrenamiento bien estructurado puede reducir significativamente los riesgos de phishing, ingeniería social o uso indebido de credenciales.

Con el fin de garantizar que el protocolo funciones, se recomienda que antes de implementarlo es necesario realizar pruebas y simulacros, buscando la efectividad del plan de respuesta a incidentes. La idea de estas pruebas es identificar brechas, optimizar tiempos de reacción y fortalecer la coordinación entre áreas.

Para disminuir peligros se recomienda el principio de mínimo privilegio, ayuda a reducir la superficie de ataque, requiere de estar revisando regularmente los permisos otorgados, desactivar cuentas innecesarias y aplicar RBAC de forma granular y asegurar que cada usuario solo acceda a los recursos estrictamente necesarios para el cumplimiento de funciones y responsabilidades.

No se debe de olvidar tener en cuenta continuamente del cumplimiento regulatorio dada la creciente relevancia de los marcos normativos como ISO/IEC 27001, GDPR, NIST SP 800-53 y la legislación chilena. Para esto se recomienda el uso de herramientas como Manager de Microsoft, que logran permitir documentar evidencias y centralizar auditorias.

Finalmente, se aconseja establecer un ciclo de mejora continua en la gestión de la ciberseguridad. Esto implica definir indicadores de desempeño (KPIs), analizar resultados y aplicar ajustes progresivos que fortalezcan la optimización en la protección de datos en la nube. Además, Se recomienda automatizar tareas como sea posible durante su implementación, con herramientas adicionales que integran flujos de trabajo y sistemas de gestión de identidad y acceso (IAM) que minimicen intervención humana, buscando facilitar la adopción del protocolo, especialmente en organizaciones con menos personal especializado.

6.3 Limitaciones.

Estas limitaciones no impidieron el desarrollo del protocolo, pero sí condicionaron su alcance práctico dentro del entorno de prueba, por lo que fueron debidamente documentadas como aspectos a considerar para futuras implementaciones en entornos empresariales con licenciamiento completo y acceso a todos los servicios necesarios ya que con una correcta suscripción de pago no existirían estas limitantes.

En la implementación del protocolo se presentaron diversas limitaciones técnicas que en su mayoría fueron causadas por las restricciones de la suscripción gratuita de la plataforma. Una de las primeras dificultades fue la imposibilidad de acceder a Microsoft Purview en su totalidad, lo que impidió ejecutar escaneos automáticos de datos sensibles, crear reglas de clasificación y aplicar etiquetas de sensibilidad directamente desde esa herramienta. Como alternativa, se documentaron los pasos requeridos para su aplicación futura en entornos productivos con licenciamiento adecuado ya que para acceder se necesita una suscripción pagada.

Dentro de la aplicación no se logró ingresar portal Microsoft 365 Compliance Center, generando problemas que imposibilitó configurar las políticas de Prevención de Pérdida de Datos (DLP) y aplicar etiquetas de sensibilidad mediante el etiquetado automático, esta limitación afectó directamente a las políticas de control sobre datos clasificados como Confidenciales, ya que no fue posible bloquear o advertir sobre el uso indebido de dichos documentos mediante reglas preconfiguradas.

En la misma línea el servicio Microsoft Sentinel no se encontraba habilitado en la cuenta de Azure utilizada por lo que no se pudieron crear reglas analíticas para detectar comportamientos sospechosos, tales como inicios de sesión desde ubicaciones que no correspondan a una persona de la empresa o de algunas descargas masivas de datos. La imposibilidad de activar UEBA (User and Entity Behavior Analytics) también fue una consecuencia directa de esta restricción, lo que impidió una correlación más avanzada de los eventos registrados en Log Analytics.

Otra limitante importante fue la ausencia de la herramienta Microsoft Compliance Manager, lo que impidió realizar evaluaciones estructuradas de cumplimiento normativo, asignar tareas de mitigación automáticamente y mantener evidencia de cumplimiento desde una consola centralizada. Estos controles de igual forma se pudieron realizar de manera manual, pero no se alcanzó el nivel de automatización y trazabilidad deseado y planteado en el protocolo.

Una limitación significativa es su dependencia del tier de pago, que es necesario para poder acceder a funciones avanzadas

No fue posible implementar restricciones avanzadas como el bloqueo por ubicación geográfica, debido a la falta de acceso a licencias premium de Microsoft Entra ID las cuales permiten ese tipo de funcionalidades. A pesar de esto, se aplicaron controles de RBAC y asignación de roles ajustados al principio de mínimo privilegio.

Por último, se detectó que algunas funcionalidades como el acceso remoto mediante Azure Bastion presentó errores por las configuraciones incompletas en la red virtual, lo que requirió la creación manual de subredes específicas y nuevos intentos de despliegue para resolver los conflictos presentados.

6.4 Trabajos a futuro.

En primera parte como proyección es importante disponer de una suscripción empresarial completa que permita validar el protocolo en toda su extensión. Esto permitiría probar servicios avanzados como Purview, Sentinel, Compliance Manager y PIM, lo que lograría comprobar el funcionamiento integral del modelo propuesto.

Otra parte para mejorar es evaluar la posibilidad de integrar el protocolo en entornos multi-nube, que logre integrar plataformas como AWS o Google Cloud. De esta manera, sería posible medir la adaptabilidad del protocolo y validar su carácter modular en escenarios híbridos o multinube, cada vez más comunes en grandes organizaciones.

También se considera importante poder aplicar el protocolo en una organización real, involucrando a los incidentes de seguridad concretos y midiendo indicadores de desempeño tales como tiempos de detección, velocidad de respuesta, porcentaje de cumplimiento de auditorías, entre otros. Esto aportaría evidencia práctica sobre la efectividad del modelo.

Una idea interesante es intentar implementar la automatización avanzada con Inteligencia Artificial, en particular el uso de modelos de aprendizaje automático para la detección de anomalías y la respuesta adaptativa ante amenazas. Esta integración permitiría evolucionar el protocolo hacia un enfoque de ciberseguridad predictiva, buscando reducir los tiempos de reacción y mejorando también el entorno en la nube.

7. GLOSARIO.

- **AES-256:** Estándar de cifrado simétrico por excelencia. Es la opción más robusta y usada para blindar datos críticos.
- **API (Application Programming Interface):** Son las reglas que permiten que dos sistemas o aplicaciones distintas puedan "hablar" e intercambiar información entre ellas.
- **ASG (Application Security Groups):** Es la manera de agrupar tus máquinas virtuales de Azure de forma lógica. Así es mucho más fácil aplicar reglas de seguridad de red en conjunto.
- **Azure Backup:** El servicio clave para automatizar y gestionar todos tus respaldos directamente en la nube, incluyendo el cifrado obligatorio.
- **Azure Bastion:** La solución que te permite conectarte a tus máquinas virtuales de forma segura, pero sin la necesidad de exponer ninguna de sus direcciones IP públicas a internet.
- **Azure Blob Storage:** El almacenamiento masivo de Azure, diseñado para manejar grandes volúmenes de datos no estructurados (archivos, vídeos, logs). Viene con cifrado activado de base.
- **Azure Key Vault:** Esencialmente, es el cajafuerte centralizado de Azure, donde gestionas y proteges claves criptográficas, certificados digitales y otros secretos.
- **Azure Monitor:** La plataforma que unifica todo el monitoreo en Azure. Recopila métricas, logs y genera alertas sobre el estado y rendimiento de tus recursos.
- **Azure Policy:** Un servicio que fuerza el cumplimiento. Evalúa continuamente la configuración de tus recursos para asegurar que se adhieran a las políticas de gobernanza que definiste.
- **Azure Private Link:** Te permite acceder a servicios de Azure (como Storage o Key Vault) a través de una conexión privada que se queda dentro de tu propia red, sin tocar el internet público.
- **Microsoft Sentinel:** Nuestra plataforma SIEM/SOAR. Recoge todos los eventos de seguridad, detecta amenazas usando inteligencia y automatiza las respuestas a incidentes.
- **Azure VNet (Virtual Network):** La red virtual de Azure. Su función principal es segmentar y controlar el flujo de tráfico dentro de tu entorno cloud.
- **BPMN (Business Process Model and Notation):** La notación gráfica estándar que utilizamos para diagramar y representar procesos empresariales de forma clara.
- **Ciberseguridad:** La práctica fundamental de proteger sistemas, redes y datos de ataques maliciosos o de accesos indebidos.
- **CMK (Customer-Managed Keys):** Las claves de cifrado que están bajo tu control directo, y que gestionas a través de Azure Key Vault.
- **Confidencialidad:** La garantía de que solo las personas o sistemas autorizados pueden acceder a una información específica.
- **CSPM (Cloud Security Posture Management):** Un conjunto de herramientas diseñadas para evaluar de forma continua y automática el nivel de seguridad de tu infraestructura en la nube.
- **DLP (Data Loss Prevention):** Los controles implementados para evitar que información sensible o confidencial se filtre o se fugue de la organización.

- **DNS (Domain Name System):** El sistema que traduce los nombres de dominio que escribes (ej. https://www.google.com/search?q=google.com) a las direcciones IP que la red necesita para funcionar.
- **DTLS (Datagram Transport Layer Security):** La versión de TLS adaptada para proteger comunicaciones más rápidas basadas en datagramas.
- **Microsoft Entra ID:** La solución de identidad en la nube de Microsoft, que se encarga de gestionar la autenticación y los permisos de acceso de todos los usuarios.
- **ExpressRoute:** Una línea dedicada que conecta tus instalaciones físicas directamente con Azure. La conexión es privada y de alta velocidad, sin pasar por el internet general.
- **GDPR (General Data Protection Regulation):** El reglamento europeo clave que dicta cómo se deben tratar y proteger los datos personales de los ciudadanos.
- **Gestión de identidad:** Los procesos y las herramientas que usamos para administrar todo lo relativo a los usuarios, sus accesos y sus credenciales.
- **HSTS (HTTP Strict Transport Security):** Un mecanismo de seguridad que le dice al navegador que siempre debe conectarse a ese sitio web usando la versión cifrada (HTTPS).
- **IAM (Identity and Access Management):** Todo el conjunto de prácticas y tecnología para gestionar la identidad de los usuarios y controlar qué pueden hacer.
- **Impacto:** Simplemente, la consecuencia o el daño que sufriría la organización si un riesgo de seguridad llegara a ocurrir.
- **ISO/IEC 27001:** La norma internacional de referencia para establecer, implementar y administrar un Sistema de Gestión de Seguridad de la Información (SGSI).
- **KQL (Kusto Query Language):** El lenguaje de consulta que usamos en Log Analytics para buscar y analizar datos dentro de los logs.
- **Log Analytics:** Un servicio esencial de Azure que te permite almacenar, consultar y correlacionar grandes volúmenes de logs y registros operativos.
- **MACsec (Media Access Control Security):** Un protocolo de cifrado que opera a nivel de Capa 2, especialmente utilizado para asegurar conexiones directas como ExpressRoute Direct.
- **MFA (Multi-Factor Authentication):** El método de autenticación que siempre exige más de una forma de verificación (no solo la contraseña) antes de dar acceso.
- **Microsoft Defender for Cloud:** La herramienta principal de Azure. Está constantemente analizando vulnerabilidades y ofreciendo recomendaciones claras para mejorar tu postura de seguridad.
- **Microsoft Purview:** Una plataforma diseñada para clasificar, etiquetar y establecer el gobierno (políticas) sobre todos tus datos a lo largo de la empresa.
- **MITM (Man-in-the-Middle):** El famoso ataque donde un tercero se interpone de forma secreta entre dos partes que se comunican para interceptar o alterar la información.
- **NIST SP 800-53:** Un catálogo muy extenso de controles de seguridad que se usa como una referencia obligada en muchos entornos corporativos y gubernamentales.
- **OSI (Open Systems Interconnection):** El modelo conceptual clásico que divide la comunicación de red en las conocidas siete capas.
- **Peering de VNets:** Conectar dos redes virtuales de Azure directamente para que se comuniquen como si estuvieran en el mismo segmento de red, sin túneles intermedios.

- **PKI (Public Key Infrastructure):** La infraestructura necesaria para emitir y gestionar certificados digitales, que son esenciales para las comunicaciones seguras (como TLS).
- **Principio de Mínimo Privilegio:** Una regla de oro: solo se otorgan los permisos que son estrictamente necesarios para que la persona o el servicio haga su trabajo. Nada más.
- **Probabilidad:** Es la medida que usamos para estimar qué tan posible o factible es que un evento o riesgo de seguridad se materialice.
- **RBAC (Role-Based Access Control):** El sistema donde los permisos no se dan al usuario individual, sino que se asignan a roles predefinidos (ej. "Lector de Datos").
- **Recovery Services Vault:** Es el contenedor seguro en Azure donde se almacenan y protegen todos los puntos de recuperación y las copias de seguridad.
- **Respaldo incremental:** Una copia de seguridad mucho más eficiente que solo captura y guarda los datos que han cambiado desde la última vez que se hizo el backup.
- **SIEM (Security Information and Event Management):** El sistema que recolecta, centraliza y analiza todos los eventos y logs de seguridad para detectar patrones y amenazas.
- **SOAR (Security Orchestration, Automation and Response):** La tecnología que toma las alertas del SIEM y automatiza la respuesta, ejecutando acciones predefinidas sin intervención humana.
- **SSH (Secure Shell):** El protocolo seguro que se usa para establecer una conexión remota y acceder a servidores o dispositivos de red.
- **TLS (Transport Layer Security):** El protocolo criptográfico que se encarga de cifrar y proteger las comunicaciones que viajan a través de internet (la base del HTTPS).
- **VNet Encryption:** Una función de Azure que cifra automáticamente el tráfico de datos que se mueve internamente entre las máquinas virtuales y las subredes.
- **VPN Gateway:** El servicio de Azure que te permite establecer túneles cifrados para conectar tu red local con la nube.
- **Vulnerabilidad:** Una debilidad, error o falla en el sistema que, si es explotada por un atacante, puede comprometer la seguridad.
- **WAF (Web Application Firewall):** Un firewall especializado que protege las aplicaciones web de ataques específicos y comunes, como inyección SQL o scripts XSS.
- **Zero Trust:** El modelo de seguridad actual. La filosofía es: no confíes en nadie, nunca. Todo usuario o dispositivo debe ser verificado continuamente, incluso dentro de la red.

8. LISTA DE ABREVIATURAS.

- AES: Advanced Encryption Standard.
- API: Application Programming Interface.
- ASG: Application Security Group.
- BPMN: Business Process Model and Notation.
- BR: Backup & Recovery (dominio MCSB).
- CMK: Customer-Managed Key.
- CSPM: Cloud Security Posture Management.
- DLP: Data Loss Prevention.
- DP: Data Protection (dominio MCSB).
- DNS: Domain Name System.
- DTLS: Datagram Transport Layer Security.
- GDPR: General Data Protection Regulation.
- GS: Governance & Strategy (dominio MCSB).
- HSTS: HTTP Strict Transport Security.
- IAM: Identity and Access Management.
- IM: Identity Management (dominio MCSB).
- Ipsec: Internet Protocol Security.
- ISO: International Organization for Standardization.
- KQL: Kusto Query Language.
- LT: Logging & Threat Detection (dominio MCSB).
- MACsec: Media Access Control Security.
- MFA: Multi-Factor Authentication.
- MCSB: Microsoft Cloud Security Benchmark.
- MITM: Man-in-the-Middle.
- NIST: National Institute of Standards and Technology.
- OSI: Open Systems Interconnection.
- P2S: Point-to-Site.
- PIM: Privileged Identity Management.
- PKI: Public Key Infrastructure.
- PMK: Platform-Managed Key.
- RBAC: Role-Based Access Control.
- S2S: Site-to-Site.
- SIEM: Security Information and Event Management.
- SOAR: Security Orchestration, Automation and Response.
- SSH: Secure Shell.
- TLS: Transport Layer Security.
- VNet: Virtual Network.
- VPN: Virtual Private Network.
- VM: Virtual Machine.
- WAF: Web Application Firewall.

9. BIBLIOGRAFIA.

Adobe. (s.f.). *Adobe*. Obtenido de about adobe pdf: https://www.adobe.com/acrobat/about-adobe-pdf.html

Alder, S. (2022, 02 04). *the hipaa journal*. Obtenido de Unpatched Vulnerabilities are the Most Common Attack Vector Exploited by Ransomware Actors: https://www.hipaajournal.com/unpatched-vulnerabilities-are-the-most-common-attack-vector-exploited-by-ransomware-actors

Bertram, A. (2024, 07 01). *n2w*. Obtenido de Azure Backup: Best Practices: https://n2ws.com/blog/microsoft-azure-cloud-services/azure-best-practices

BrendaCarter. (2025, 02 27). *Whar is Zero Trust*. Obtenido de Microsoft: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

businessmap. (s.f.). *¿Qué es Kanban? Explicación para principiantes.* Obtenido de businessmap: https://businessmap.io/es/recursos-de-kanban/primeros-pasos/que-es-kanban

Chavez, J. J. (2024, 04 29). *Protocolos de seguridad informática: ¿Cuáles son y cómo implementarlos?* Obtenido de https://www.deltaprotect.com/blog/protocolos-seguridad-informatica

Chica, M. (2025, 03 03). *Protocolos de transferencia de archivos: FTP, SFTP y SSH*. Obtenido de https://www.cdmon.com/es/blog/protocolos-de-transferencia-de-archivos-ftp-sftp-y-ssh

ciberseguridad. (s.f.). *¿Qué es HSTS (HTTP Strict Transport Security)?* Obtenido de https://ciberseguridad.com/guias/hsts-http-strict-transport-security

Cloudfire. (2024). *¿Qué es TLS (Transport Layer Security)?* Obtenido de https://www.cloudflare.com/es-es/learning/ssl/transport-layer-security-tls

cloudflare. (2024, 05 19). *cloudflare*. Obtenido de https://www.cloudflare.com/es-es/learning/access-management/role-based-access-control-rbac/

Entel. (2025). *Reporte de ciberseguridad.* e) digital.

Force, J. T. (2020, marzo). *Security and Privacy Controls for Information Systems and Organizations*. Obtenido de NIST: https://csrc.nist.gov/pubs/sp/800/53/r5/fpd

Gallego, R. H. (2023). *Análisis de ciberseguridad a una infraestructura de red*. Obtenido de https://repository.libertadores.edu.co/server/api/core/bitstreams/511dfb24-98f7-48d5-8f47-baad80c06a9e/content

Goodwin, M. (s.f.). *What is an API (application programming interface)?* Obtenido de IBM: https://www.ibm.com/think/topics/api

IBM. (s.f.). *¿Qué es el marco de ciberseguridad del NIST?* Obtenido de https://www.ibm.com/mx-es/topics/nist

IBM. (2025). *IBM*. X-Force. Obtenido de IBM X-Force 2025 Threat Intelligence Index: https://www.ibm.com/reports/threat-intelligence

IBM. (2025). *Informe "Cost of a Data Breach" de 2025*. IBM. Obtenido de https://www.ibm.com/downloads/documents/es-es/137a3e32273ed1f5

Im, H.-J. (2024, 06 04). *What is the Microsoft Zero Trust Security Model? All You Need to Know!* Obtenido de Proserveit: https://www.proserveit.com/blog/what-is-microsoft-zero-trust-security-model

Jaakkonen, H. (2025, 05 22). *cloudpartner*. Obtenido de Mandatory MFA in Microsoft Entra: What You Need to Know: https://www.cloudpartner.fi/?p=18221

Kapko, M. (2025, 7 30). *Research shows data breach costs have reached an all-time high*. Obtenido de Cyberscoop: https://cyberscoop.com/ibm-cost-data-breach-2025

Key management in Azure. (2025, 04 16). Obtenido de Microsoft: https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management

kodekloud. (s.f.). *kodekloud*. Obtenido de Application Security Groups: https://notes.kodekloud.com/docs/Updated-AZ-104-Microsoft-Azure-Administrator/Administer-Virtual-Networking/Application-Security-Groups

Lark Editorial Team. (2024, 1 16). *Kanban for Cybersecurity Teams*. Obtenido de Lark: https://www.larksuite.com/en_us/topics/project-management-methodologies-for-functional-teams/kanban-for-cybersecurity-teams/

Lean Enterprise Institute. (s.f.). *What is Lean?* Obtenido de Lean Enterprise Institute: https://www.lean.org/explore-lean/what-is-lean

LogicMonitor. (2024, 09 20). *What is Microsoft Entra ID (Formerly Azure Active Directory?)*. Obtenido de logicmonitor: https://www.logicmonitor.com/blog/what-is-azure-active-directory

López, S. L. (2023, 01). *Infraestructura de Seguridad en la nube de Azure.* Obtenido de https://openaccess.uoc.edu/bitstream/10609/147879/4/sergiolopezlopezTFG0123memoria.pdf

Loyola, J. S. (2024). *Resúmenes de las Leyes Fundamentales de.* Santiago.

McGill, M. (s.f.). *hbs*. Obtenido de Risk Assessment: Likelihood and Impact: https://www.hbs.net/blog/risk-assessment-likelihood-impact

Microsoft. (2023, 11 15). *Microsoft*. Obtenido de Recommendations for data classification: https://learn.microsoft.com/en-us/azure/well-architected/security/data-classification

Microsoft. (2023, 11 15). *Microsoft*. Obtenido de Recommendations for data classification: https://learn.microsoft.com/en-us/azure/well-architected/security/data-classification

Microsoft. (2024, 05 21). *Automate Yhreat reponse with playbooks in Microsoft Sentinel*. Obtenido de Microsoft: https://learn.microsoft.com/en-us/azure/sentinel/automation/automate-responses-with-playbooks

Microsoft. (2024, 09 27). *Azure security best practices and patterns*. Obtenido de Microsoft: https://learn.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns

Microsoft. (2024, 12 12). *Microsoft*. Obtenido de Microsoft Fabric end-to-end security scenario: learn.microsoft.com/en-us/fabric/security/security-scenario

Microsoft. (2024, 02 05). *Microsoft*. Obtenido de Recommendations for data encryption: https://learn.microsoft.com/en-us/azure/well-architected/security/encryption

Microsoft. (2024, 08 01). *Microsoft*. Obtenido de Define network encryption requirements: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/define-network-encryption-requirements

Microsoft. (2024, 09 11). *Microsoft*. Obtenido de Encryption in Azure Backup: https://www.hipaajournal.com/unpatched-vulnerabilities-are-the-most-common-attack-vector-exploited-by-ransomware-actors

Microsoft. (2025, 06 26). *¿Que es Azure Private Link?* Obtenido de Microsoft Learn: https://learn.microsoft.com/en-us/azure/private-link/private-link-overview

Microsoft. (2025, 07 25). *Application security groups*. Obtenido de Microsoft: https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

Microsoft. (2025, 04 25). *Aprenda acerca de Microsoft Purview*. Obtenido de Microsoft Learn: https://learn.microsoft.com/es-es/purview/purview

Microsoft. (2025, 04 16). *Microsoft*. Obtenido de Key management in Azure: https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management

Microsoft. (2025, 09 07). *Microsoft*. Obtenido de What is Azure VPN Gateway?: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Microsoft. (2025, 07 21). *Microsoft*. Obtenido de Archived release notes in Azure Backup: https://docs.azure.cn/en-us/backup/backup-release-notes-archived

Microsoft. (2025, 01 04). *Microsoft*. Obtenido de Azure monitor logs overview: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs

Microsoft. (2025, 05 23). *Microsoft*. Obtenido de Azure Monitor overview: https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/overview

Microsoft. (2025, 06 10). *Microsoft*. Obtenido de Auditing best practices for production environments: https://learn.microsoft.com/en-us/azure/azure-sql/database/auditing-best-practices?view=azuresql

Microsoft. (2025, 07 07). *Microsoft*. Obtenido de Planning for mandatory multifactor authentication for Azure and other admin portals: learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication

Microsoft. (2025, 04 03). *Microsoft*. Obtenido de Block access by location: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-by-location

Microsoft. (2025, 05 19). *Microsoft*. Obtenido de Conditional Access: Filter for devices: https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-condition-filters-for-devices

Microsoft. (2025, 07 03). *Microsoft*. Obtenido de Introducción a las claves, secretos y certificados de Azure Key Vault: https://learn.microsoft.com/es-es/azure/key-vault/general/about-keys-secrets-certificates

Microsoft. (2025, 07 09). *Microsoft*. Obtenido de What is Azure VPN Gateway?: learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Microsoft. (2025, 07 23). *Microsoft*. Obtenido de What is Microsoft Defender for Cloud?: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Microsoft. (2025, 05 26). *Microsoft*. Obtenido de Encrypt backup data by using customer-managed keys: https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk?tabs=portal

Microsoft. (2025, 04 01). *Microsoft*. Obtenido de About Site Recovery: https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

Microsoft. (2025). *Microsoft defender for cloud documentation*. Obtenido de Microsoft Learn: https://learn.microsoft.com/en-us/azure/defender-for-cloud

Microsoft. (2025). *Microsoft Entra ID*. Obtenido de Microsoft Security: https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

Microsoft. (2025). *Microsoft Sentinel documentation*. Obtenido de Microsoft Learn: https://learn.microsoft.com/en-us/azure/sentinel

Microsoft. (2025, 03 14). *What is Azure Bastion?* Obtenido de Microsoft Learn: https://learn.microsoft.com/en-us/azure/bastion/bastion-overview

Microsoft. (2025, 03 14). *What is Azure Bastion?* Obtenido de Microsoft: https://learn.microsoft.com/en-us/azure/bastion/bastion-overview

Microsoft. (2025, 06 26). *What is Azure Private Link?* Obtenido de Microsoft: https://learn.microsoft.com/en-us/azure/private-link/private-link-overview

Microsoft. (2025, 08 19). *What is managed identities for Azure resources?* Obtenido de Microsoft: https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview

Microsoft. (2025, 01 07). *What is Microsoft Entra Privileged Identity Management?* Obtenido de Microsoft: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

Microsoft. (2025, 02 27). *What is Zero Trust*. Obtenido de Microsoft: learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

Microsoft. (s.f.). *Autenticación multifactor de Microsoft Entra*. Obtenido de Microsoft: https://www.microsoft.com/es-cl/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication

Microsoft. (s.f.). *Customer-managed keys for Azure Storage encryption*. Obtenido de Microsoft: https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview

Microsoft. (s.f.). *Learn about data loss prevention*. Obtenido de Microsoft: https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp?view=o365-worldwide

Microsoft. (s.f.). *Microsoft*. Obtenido de Azure Backup - Frequently asked questions: learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq

Microsoft. (s.f.). *Microsoft*. Obtenido de Definición de vulnerabilidad de seguridad: https://www.microsoft.com/en-us/msrc/definition-of-a-security-vulnerability

Microsoft. (s.f.). *Microsoft*. Obtenido de Azure Backup pricing: https://azure.microsoft.com/en-us/pricing/details/backup

NIST. (2020, 09). *Security and Privacy Controls for Information Systems and Organizations*. Obtenido de NIST: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

paloalto. (s.f.). *paloalto*. Obtenido de What Is Data Classification?: https://www.paloaltonetworks.com/cyberpedia/data-classification

Phung, J. (2024, 11 07). *Incident Response to Brute-Force Attack: A Study of Azure and Traditional Approaches.* Obtenido de Metropolia University of Applied Sciences: https://www.theseus.fi/bitstream/handle/10024/871237/Phung_Julius.pdf?sequence=2&isAllowed=y

Pirani. (s.f.). *ISO 27001: de que se trata y como implementarla.* Obtenido de pirani: https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla?utm_term=&utm_campaign=Performance+max+-

+Generico&utm_source=adwords&utm_medium=ppc&hsa_acc=9508207643&hsa_cam=22234655473&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&

Quiroz-Vásquez, C. (2024, 03 12). *What is the DNS protocol?* Obtenido de https://www.ibm.com/think/topics/dns-protocol

SentinelOne. (2025, 09 14). *50+ Cloud Security Statistics in 2025*. Obtenido de SentinelOne: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics

Smith, P. (2025, 01 21). *Recordpoint*. Obtenido de A guide to data classification: confidential data vs. sensitive data vs. public information: https://www.recordpoint.com/blog/a-guide-to-data-classification-confidential-vs-sensitive-vs-public-information

SSL. (2025, 05 04). *What is HTTPS?* Obtenido de https://www.ssl.com/faqs/what-is-https/

Standards Development Organization. (2010, 12). *Business Process Model And Notation*. Obtenido de omg: https://www.omg.org/spec/BPMN/2.0

Unión Internacional de Telecomunicaciones. (2015, 09 10). *Tercer Foro Regional sobre Interconectividad,*. Obtenido de https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2015/0910-PA-IXP/11%20Viernes%20Palacios%20ITU%20Cybersecurity%20CIRT.pdf

University of miami health system. (s.f.). *Reglamento General de Protección de Datos (GDPR)*. Obtenido de umiamihealth: https://umiamihealth.org/es/website-disclaimers/declaración-de-privacidad/reglamento-general-de-protección-de-datos-(gdpr)#:~:text=El%20Reglamento%20General%20de%20Protección%20de%20Datos,vigencia%20el%2025%20de%20mayo%20de%202018.

Zareen, A. A. (2020). *Security Requirements Engineering Framework with*. Islamabad.

zscaler. (s.f.). *zscaler*. Obtenido de ¿Qué es la DLP en la nube (prevención de la pérdida de datos)?: https://www.zscaler.com/es/resources/security-terms-glossary/what-is-cloud-dlp-data-loss-prevention

ANEXO

1. Como Implementar las herramientas de seguridad en Azure.

Con el desarrollo del protocolo finalizado, esta sección tiene por objetivo mostrar de forma práctica, detallada y lo más sencilla posible de cómo se llevó a cabo la implementación técnica de las herramientas y configuraciones definidas en las distintas fases del modelo. A través de forma secuencial se van presentando los pasos a realizar en Azure para materializar las políticas de seguridad, clasificación de datos, monitoreo, control de acceso, respaldo y cumplimiento normativo.

En la siguiente subsección se presenta la primera fase correspondiente a la clasificación de los datos y la creación de recursos, donde se establecen las bases para aplicar controles diferenciados según el de sensibilidad de la información.

Fase 1. Clasificación y evaluación de datos (5.2.1).

Se definieron los niveles de sensibilidad de los datos, Confidencial, Interno y Público. Para cada categoría se crearon grupos de recursos en Azure, con etiquetas específicas que permiten su identificación y gestión diferenciada.

Para ello, se accedió al apartado Grupo de recursos y se creó un nuevo recurso, definiendo nombre, suscripción y región. Se eligió la región Brasil South por razones de estabilidad y compatibilidad, luego se añadieron etiquetas de clasificación, según corresponda:

- Nombre de la etiqueta: Clasificación
- Valor: Confidencial

Se repitió el procedimiento para los valores Internos y Públicos, generando tres grupos de recursos diferenciados.

Posteriormente, se creó el recurso destinado al monitoreo, denominado GR-Ciberseguridad, siguiendo el mismo proceso, pero asignándole la etiqueta correspondiente para su uso específico en políticas de seguridad. En la ilustración 29 se puede observar donde se debe configurar la primera ventana.

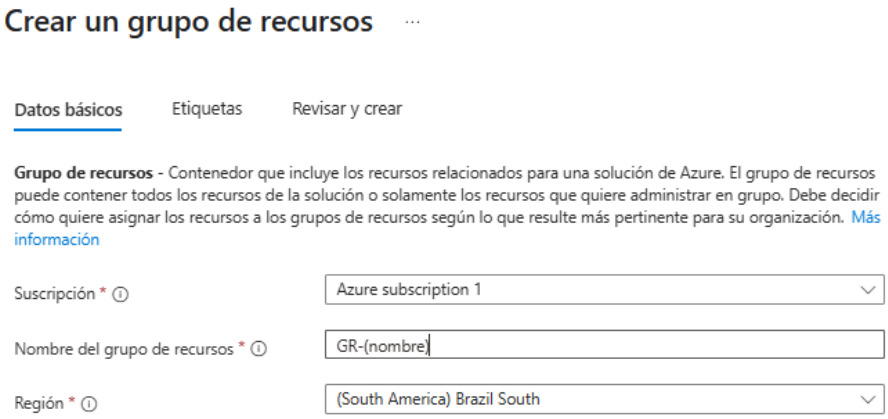

Ilustración 29: Creación de grupos de recursos en Azure con etiquetas de clasificación.

Con todos los grupos de recursos creados y etiquetados, se procedió a aplicar las políticas de Azure Policy para forzar controles automáticos basados en estas etiquetas. Teniendo así 4 grupos de recurso como se visualiza en la ilustración 30.

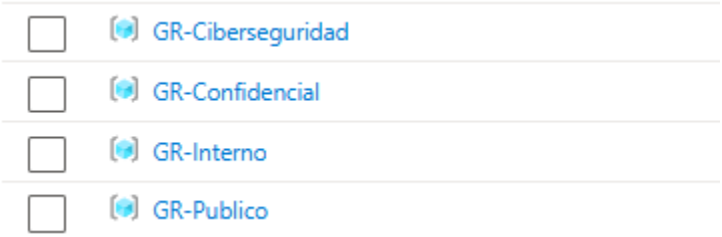

Ilustración 30: Recursos creados.

Primero se seleccionó la política *Audit VMs that do not use managed disks* para el grupo *GR-Confidencial* que se ve en la ilustración 31, permitiendo auditar máquinas virtuales que no cumplan con el cifrado en reposo.

Ilustración 31: Configuración política para datos confidenciales.

Después, se configuró la política *Network interfaces should not have public IPs* para impedir la creación de direcciones IP públicas en el grupo de recursos confidencial, evitando exposición

innecesaria. Finalmente, se aplicó *Require a tag and its value on resource groups* para exigir la presencia de la etiqueta de clasificación en todos los recursos, garantizando la trazabilidad. En este caso, se especificó el nombre de la etiqueta como *Clasificación* y el valor como *Confidencial* como se visualiza en la ilustración 32.

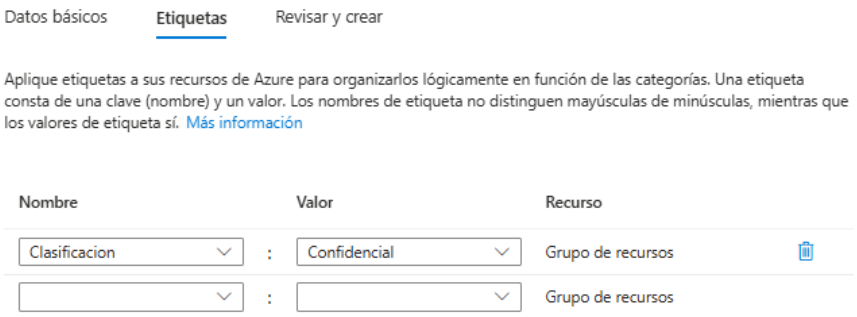

Ilustración 32: Etiquetado para trazabilidad

Para los datos confidenciales se implementaron tres controles principales:

- Auditoría del cifrado en reposo.
- Bloqueo de direcciones IP públicas.
- Aplicación obligatoria de etiquetas para trazabilidad.

Para los datos internos y públicos se aplicaron políticas similares de requerimiento de etiqueta y valor en los grupos de recursos, garantizando la coherencia en la clasificación y su correcta identificación dentro del entorno de Azure.

En esta fase es importante también dejar las cuentas de almacenamiento que corresponden a cada nivel de clasificación, siendo esta para confidencial, interno y público. El objetivo es que cada almacén quede con sus políticas diferenciadas según el nivel de sensibilidad establecido. Por lo tanto, para crearlas se realiza de la siguiente forma, cada grupo de recursos se desplegaron cuentas con los siguientes parámetros:

- **Nombre:** almacenconfidencial, almaceninterno, almacenpublico
- **Tipo de cuenta:** StorageV2 (general-purpose v2)
- **Redundancia:** LRS (Locally Redundant Storage)
- **Performance:** Standard
- **Cifrado en reposo:** Habilitado (claves administradas por Microsoft por defecto)

Para la Configuración de acceso a las redes de cada almacén.

- **AlmacenConfidencial:** configurado con opción Redes seleccionadas, añadiendo únicamente la IP del cliente autorizado. Esto asegura que el recurso solo pueda ser accedido desde direcciones previamente definidas.

- **AlmacenInterno:** habilitado con Todas las redes, pero sujeto a control de acceso mediante RBAC y etiquetas de clasificación.
- **AlmacenPublico:** habilitado con Todas las redes, permitiendo acceso abierto, dado que corresponde a datos sin restricción de confidencialidad.

Además, se debe verificar que el cifrado en reposo estuviera activo en las tres cuentas. Para la cuenta **Confidencial** se documentó la propuesta de habilitar **claves administradas por el cliente (CMK)** en **Azure Key Vault**, con rotación programada cada 90 días. Sin embargo, esta funcionalidad quedó en diseño no implementado por las limitaciones de la suscripción gratuita (falta de identidades administradas).

Finalmente se asignaron definiciones de políticas con alcance a los grupos de recursos:

- **Require a tag and its value on resource groups**: obliga a incluir la etiqueta "Clasificación" en todos los recursos.
- **Network interfaces should not have public IPs**: aplicada a GR-Confidencial para impedir interfaces de red con IP pública.
- **Audit VMs that do not use managed disks**: audita el uso de discos administrados en máquinas virtuales del mismo grupo.

Fase 2. Control de Identidad y Acceso (5.2.2).

El objetivo de esta fase fue definir quién podía acceder a cada grupo de recursos, asignando roles adecuados según la sensibilidad y aplicando el principio de mínimo privilegio.

Para los datos confidenciales, se accedió al grupo correspondiente y se utilizaron las opciones de *Control de acceso (IAM)* para gestionar las asignaciones de roles. En este entorno se contempló la posibilidad de otorgar permisos estrictamente a los usuarios o grupos autorizados para el manejo de datos altamente sensibles.

En el caso de los datos internos, se asignó el rol de *Colaborador* al equipo de TI, permitiéndoles crear y modificar recursos, pero sin otorgarles la capacidad de conceder acceso a otros usuarios. Este enfoque aseguró el principio de mínimo privilegio y limitó la superficie de exposición.

Posteriormente, se agregó el rol *Colaborador de supervisión* para el equipo de auditoría o monitoreo, garantizando la capacidad de observación sin intervención en la gestión de recursos.

Finalmente, se asignó el rol *Lector* a quienes requerían únicamente permisos de consulta, asegurando una separación clara de responsabilidades y manteniendo la trazabilidad de las asignaciones, un ejemplo es la ilustración 33, se configura de la misma forma según corresponda en cada rol.

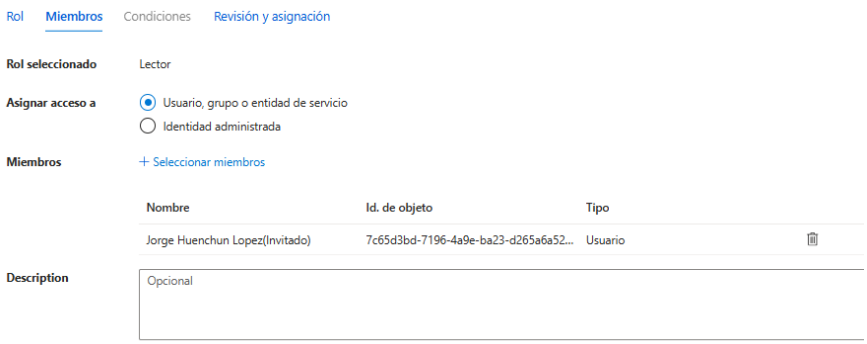

Ilustración 33: Configuración de la asignación de roles

De esta manera, las asignaciones de rol quedaron claramente delimitadas y documentadas, facilitando su revisión y auditoría posterior.

Para Aplicar Control RBAC en los Servicios se debe crear en Azure Key Vault y definir alcance de acceso con RBAC y además se debe de usar identidades administradas o roles personalizados si aplica.

En la Autenticación de Servicios con Identidades Administradas al crear la MV-Ciberseguridad, en el paso de seguridad activar:

- Identidad del sistema = Activada
- En Key Vault > Acceso > asignar rol a la identidad administrada de la MV.

Con la Auditoría de Cumplimiento de Políticas de Acceso se tuvieron problemas, puesto que la opción requiere licencias premium de Microsoft Entra ID Governance, no disponibles en nuestra suscripción. Se debería habilitar Access Reviews desde el panel de Entra ID si se contara con dicha licencia.

Con las asignaciones de rol ya configuradas en cada grupo de recursos, se generó evidencia mediante la descarga de un archivo en formato CSV. Esto se puede realizar desde Control de acceso (IAM) > Asignaciones de rol > Descargar, obteniendo así un respaldo completo de las asignaciones activas para cada nivel de clasificación (Confidencial, Interno y Público) como se puede ver en la tabla 19 en el punto 5.3.2.

En el caso de la integración de RBAC con Azure Key Vault, se documentó la imposibilidad de habilitar Identidades Administradas en las cuentas de almacenamiento debido a las restricciones de la suscripción gratuita. Como alternativa temporal, se asignó el rol Key Vault Administrator de forma manual a los usuarios responsables. No obstante, el diseño contempla que en un entorno productivo se utilicen Managed Identities junto con RBAC granular, lo que permitiría autenticar servicios sin exponer credenciales. Caso similar para la auditoría de cumplimiento de políticas de acceso que se dejó documentado que las revisiones periódicas de acceso de Access Reviews es necesario tener disponible las licencias premium de Microsoft Entra ID Governance, no disponibles en el entorno de pruebas.

Fase 3. Cifrado, vigilancia y prevención de fuga de datos (5.2.3).

En primera instancia se debe de configurar el apartado de cifrado, por lo que se realiza de la siguiente forma el paso a paso, es importante detallarlo al máximo, puesto que el cifrado es nuestro escudo principal ante los datos más relevantes como se ve en la ilustración 34.

Cifrado en Reposo con Azure Key Vault

Crear nuevo:

- Nombre: vault-confidencial
- Grupo de recursos: GR-Confidencial
- Ubicación: Brasil South
- Pricing Tier: Standard

Crear nueva clave:

- Nombre: clave-confidencial
- Tipo: RSA
- Tamaño: 2048 o 4096 bits
- Activar expira y rotación cada 90 días

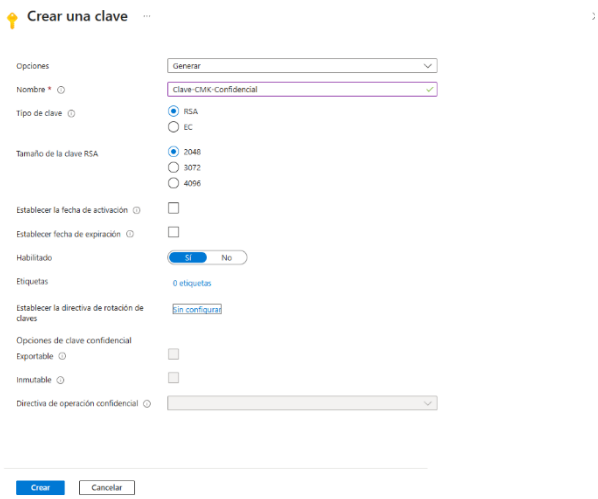

Ilustración 34: Creación de la clave.

Activar Políticas DLP (Data Loss Prevention). Para lograr este punto se requiere acceso al Microsoft 365 Compliance Center (licencia E5).

En caso de contar con acceso, se debe crear una nueva regla DLP para documentos etiquetados como "Confidencial" que impida descargas o envíos no autorizados. En este protocolo se considera como medida propuesta no ejecutada debido a limitaciones de licencia. En cuanto al cifrado en tránsito, se verificó que las conexiones hacia los recursos de almacenamiento utilizan TLS 1.2 de manera predeterminada, garantizando la protección de los datos en movimiento. Se documentó como medida

propuesta la integración de VPN Gateway o Azure ExpressRoute para escenarios productivos, donde se requiere un canal dedicado y cifrado entre la organización y Azure. En esta fase también se busca garantizar que toda actividad quedara registrada, permitiendo una respuesta proactiva ante incidentes y cumpliendo con normas de trazabilidad.

Se creó un *Área de trabajo de Log Analytics*, asignándola al grupo de recursos *GR-Ciberseguridad* y ubicándola en la región *Brasil South*, mostrado en la ilustración 35. Esta área centralizó la recolección y análisis de logs y métricas.

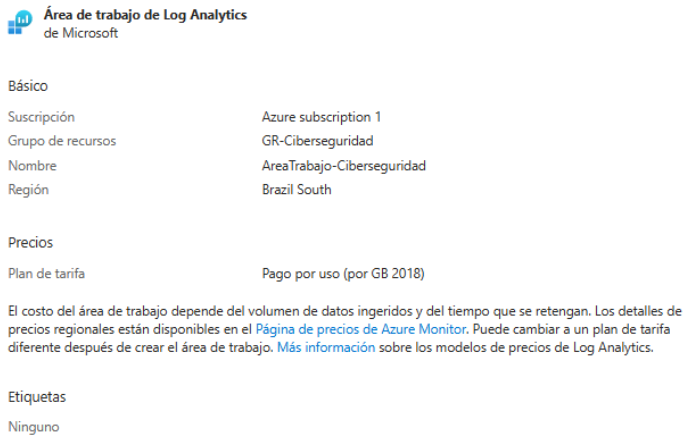

Ilustración 35: Configuración del área de trabajo

Luego, se creó una máquina virtual denominada *MV-Ciberseguridad* mostrada por la ilustración 36. Durante su configuración, se definieron las siguientes características:

- Imagen: *Windows Server 2022 Datacenter: Azure Edition – Gen2*.
- Tamaño: *Standard E2s v3* (2 vCPU, 16 GiB RAM).
- Almacenamiento: HDD estándar con cifrado en reposo habilitado.
- Seguridad: *Secure Boot* y *vTPM* activados.
- Redes: Red virtual *MV-Ciberseguridad-vnet* con subred predeterminada y control de IP pública.
- Monitoreo: Diagnósticos de arranque y del SO invitado-habilitados, con destino al Área de trabajo de Log Analytics.
- Etiquetas: Clasificación = ciberseguridad.

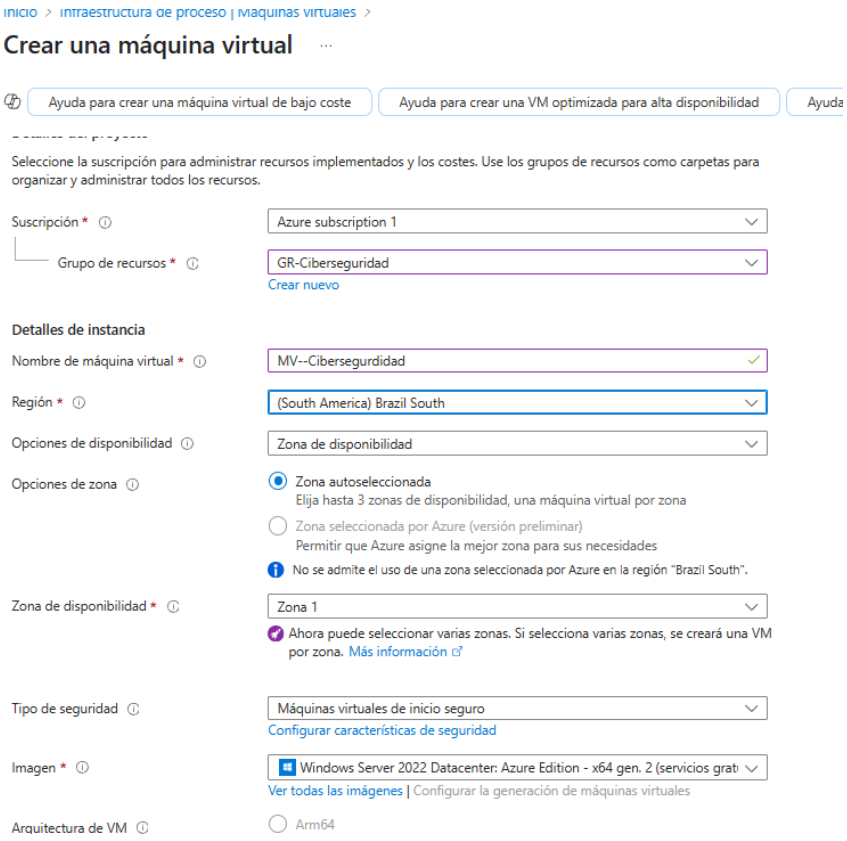

Ilustración 36: Configuración para crear máquina virtual.

Tras el despliegue de la máquina virtual, se creó una *Regla de recopilación de datos (DCR)* para definir qué datos recolectar y dónde enviarlos. La regla incluyó contadores de rendimiento y registros de eventos de Windows, ambos dirigidos al Área de trabajo de Log Analytics de la ilustración 37.

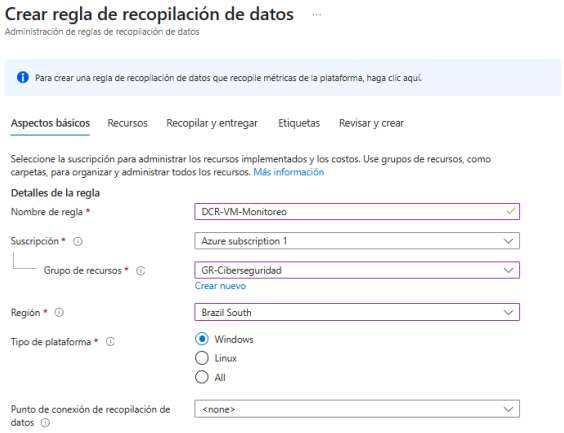

Ilustración 37: Configuración para crear regla de recopilación de datos.

Finalmente, se instaló el *Azure Monitor Agent* en la máquina virtual para habilitar la recopilación de métricas y logs. En caso de no aparecer en el portal, se utilizó PowerShell para instalarlo manualmente:

```
Set-AzVMExtension `
-ResourceGroupName "GR-Ciberseguridad" `
-VMName "MV-Ciberseguridad" `
-Name "AzureMonitorWindowsAgent" `
-Publisher "Microsoft.Azure.Monitor" `
-ExtensionType "AzureMonitorWindowsAgent" `
-TypeHandlerVersion "1.1" `
-Location "brazilsouth" `
-EnableAutomaticUpgrade $true
```

Luego de ingresar esa línea de comando para corroborar que se tuvo éxito, debe de mostrar un mensaje como la ilustración 38.

```
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
--------- ------------------- ---------- ------------
                         True         OK
```

Ilustración 38: Mensaje de confirmación para Azure Monitor.

Fase 4. Monitoreo, Detección y Respuesta ante Incidentes de Seguridad (5.2.4).

En esta fase se buscó detectar intentos de fuga de datos, generar alertas, bloquear acciones indebidas y habilitar supervisión activa. Se habilitó *Microsoft Defender for Cloud* en la suscripción *Azure subscription 1*, que contenía tanto el grupo de recursos *GR-Ciberseguridad* como el Área de trabajo de Log Analytics. Con el plan Básico (gratuito), se garantizó la evaluación continua de seguridad, recomendaciones automáticas de mejora y monitoreo permanente de la configuración como se puede ver en la ilustración 39.

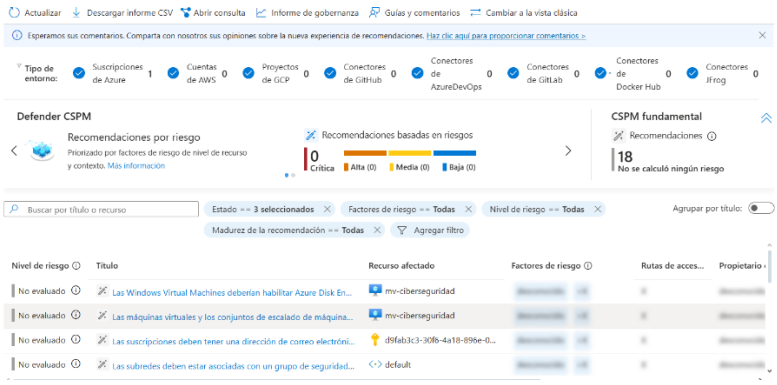

Ilustración 39: Microsoft Defender for Cloud

Posteriormente, se accedió al apartado *Recomendaciones* para visualizar alertas y sugerencias de mejora, asegurando la capacidad de respuesta proactiva ante incidentes y la supervisión continua del entorno. Luego de estar habilitado, se desplegó el apartado de Recomendaciones de seguridad, donde se listaron alertas asociadas a configuraciones inseguras, como discos de máquinas virtuales sin cifrar, configuraciones de red expuestas y cuentas de almacenamiento sin diagnósticos habilitados. Estas notificaciones cumplen la función de guiar la respuesta temprana y priorizar acciones de remediación, el panel se puede visualizar en la ilustración 27 en el apartado 5.3.6.

Fase 5. Respaldo y Recuperación (5.2.5).

Para garantizar la disponibilidad y recuperación ante desastres, se creó un *Almacén de Recovery Services* en el grupo *GR-Ciberseguridad*, manteniendo la consistencia de la región con el resto de los recursos, la ilustración 40 muestra como es la creación del almacén.

Ilustración 40: Creación del almacén de Recovey Services

A continuación, se configuró la copia de seguridad para la máquina virtual *MV-Ciberseguridad* en el almacén creado. Se seleccionó la directiva *EnhancedPolicy*, obligatoria debido al uso de *Secure Boot* y *vTPM*, procurando mantener las siguientes configuraciones, así como lo muestra también la ilustración 41.

- Copias completas cada 4 horas (12 horas diarias desde las 8:00 AM UTC).
- Retención diaria de 30 días.
- Restauración instantánea habilitada durante 2 días.

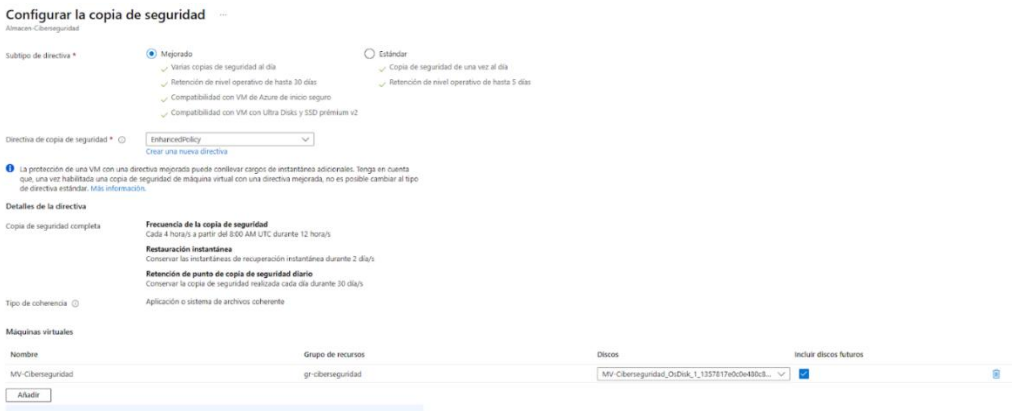

Ilustración 41: Configuración para copia de seguridad.

Se verificó la realización correcta de la copia de seguridad accediendo a *Elementos de copia de seguridad* en el almacén, confirmando la existencia de un elemento protegido de tipo *Azure Virtual Machine*. Esta configuración aseguró la continuidad operativa y la existencia de puntos de restauración automáticos.

En caso de incidente, se dejó documentado el procedimiento para restaurar la máquina virtual desde el almacén, seleccionando el punto de restauración deseado y eligiendo entre recuperar en su forma original o como nueva instancia. La configuración se realizó en el portal de Azure accediendo a Recovery Services Vaults y seleccionando la opción Crear. Se definió el nombre del contenedor de recuperación, el grupo de recursos (GR-Ciberseguridad) y la región (Brazil South), asegurando consistencia con el resto de la infraestructura.

Una vez creado el almacén, en el menú lateral se seleccionó la opción Backup y se configuró como origen la máquina virtual MV-Ciberseguridad, asignando la directiva EnhancedPolicy con frecuencia de copias completas cada 4 horas y retención diaria de 30 días. La opción Restauración instantánea quedó habilitada de forma predeterminada durante 2 días.

Posteriormente, desde el menú Elementos de copia de seguridad, se verificó que la máquina virtual aparecía como recurso protegido. Para comprobar la restauración, se accedió a la opción Recuperar VM, seleccionando un punto de restauración y validando que era posible desplegarla tanto en su configuración original como en una instancia alternativa.

Fase 6. Supervisión, Cumplimiento y Auditoría (5.2.6)

Finalizando la implementación, para poder tener una correcta supervisión y cumplimiento, se debe trabajar con el Log Analytics y Azure Policy para cumplir estas tareas. En primer lugar, desde el recurso GR-Ciberseguridad se accede al apartado de uso y estimaciones, pasando luego a la retención de datos, la cual confirma que el nivel de precio es el gratuito, otorgando una retención predeterminada de 30 días como se visualiza en la ilustración 28 en el punto 5.3.6. Posteriormente, se aplicaron definiciones de *Azure Policy* para poder evaluar el grado de cumplimiento de los recursos frente a los estándares de seguridad definidos en el protocolo. Para esto, se ingresa a *Azure Policy* en el apartado *Asignaciones* se selecciona *Asignar directiva* y se define el alcance sobre los grupos de recursos creados.