UNIVERSIDAD POLITÉCNICA DE MADRID

E.T.S. DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

PROYECTO FIN DE GRADO

GRADO EN INGENIERÍA DE COMPUTADORES

Desviaciones en los controles de seguridad CIS y su Automatización

Desarrollado por: Alejandro Belinchón Álvarez

Dirigido por: Juan Manuel Castelo Gómez

Madrid, 14 de julio de 2025

Desviaciones en los controles de seguridad CIS y su Automatización
Desarrollado por: Alejandro Belinchón Álvarez
Dirigido por: Juan Manuel Castelo Gómez
Proyecto Fin de Grado, 14 de julio de 2025

E.T.S. de Ingeniería de Sistemas Informáticos
Campus Sur UPM, Carretera de Valencia (A-3), km. 7
28031, Madrid, España

Si deseas citar este trabajo, la entrada completa en BibTeX es la siguiente:

```
@mastersthesis{Belin2025,
    title = {Desviaciones en los controles de seguridad CIS y su Automatización},
    type = {Bachelor's Thesis},
    author = {Alejandro Belinchón Álvarez},
    school = {E.T.S. de Ingeniería de Sistemas Informáticos},
    year = {2025},
    month = {7},
}
```

Agradecimientos

Quisiera expresar mi más sincero agradecimiento a todas las personas que han contribuido, directa o indirectamente, a la realización de este Trabajo de Fin de Grado.

En primer lugar, agradezco al profesor Juan Manuel, por su orientación, disponibilidad y apoyo a lo largo del desarrollo del proyecto. Su experiencia y consejos han sido fundamentales para superar los desafíos técnicos y metodológicos planteados.

También me gustaría agradecer al equipo de la empresa dónde estoy realizando mis prácticas; por brindarme la oportunidad de realizar este proyecto en un entorno profesional real y por facilitarme los recursos necesarios y fomentar un entorno de aprendizaje enriquecedor y colaborativo.

No puedo dejar de mencionar a mi familia, por su apoyo incondicional, su paciencia y por estar siempre ahí en cada etapa del camino. A mis amigos y compañeros, gracias por las conversaciones técnicas (y no tan técnicas), por su compañía, y por compartir tantos momentos importantes durante esta etapa.

A todos, gracias por haber formado parte de este proceso. Sin vuestra ayuda, este trabajo no habría sido posible.

Y dicho esto, demos comienzo a la lectura del proyecto.

Resumen

Este Trabajo de Fin de Grado aborda el diseño e implementación de una solución automatizada para la gestión y visibilidad de desviaciones de seguridad en entornos cloud.

En la actualidad, muchas organizaciones enfrentan dificultades para mantener el cumplimiento continuo de sus controles de seguridad debido a procesos manuales, fragmentados y con escasa trazabilidad. Para resolver este problema, se ha desarrollado un sistema basado en herramientas ampliamente adoptadas en entornos corporativos como Prisma Cloud, Power Automate, SharePoint, Power BI y Microsoft Teams.

La solución normaliza y registra los hallazgos en listas estructuradas de SharePoint, clasifica y prioriza las desviaciones y genera notificaciones automáticas a los responsables técnicos. Además, se ha integrado una solución basada en inteligencia artificial mediante modelos de lenguaje grandes (LLMs) para enriquecer el análisis técnico de las desviaciones, alineando los hallazgos con marcos como MITRE ATT&CK y los controles del centro de controles de seguridad de Internet (CIS).

El desarrollo se ha llevado a cabo en un entorno de pruebas controlado, siguiendo principios de mínimo privilegio y buenas prácticas de automatización y seguridad. Se han considerado aspectos de sostenibilidad, impacto económico y cumplimiento ético y normativo, incluyendo el tratamiento de datos sensibles y el uso responsable de inteligencia artificial. Como resultado, la solución permite reducir la carga operativa, mejorar la trazabilidad y acelerar la toma de decisiones frente a riesgos de seguridad en entornos multicloud.

Palabras clave:

Seguridad en la nube, Desviaciones de seguridad, Inteligencia artificial, Cumplimiento normativo

Abstract

This Bachelor's Thesis addresses the design and implementation of an automated solution for managing and visualizing security deviations in cloud environments.

Currently, many organizations struggle to maintain continuous compliance with their security controls due to manual, fragmented processes with limited traceability. To address this issue, a system has been developed based on widely adopted tools in corporate environments, such as Prisma Cloud, Power Automate, SharePoint, Power BI, and Microsoft Teams.

The solution standardizes and logs findings in structured SharePoint lists, classifies and prioritizes deviations, and generates automatic notifications to the responsible technical personnel. Additionally, an AI-based solution using Large Language Models (LLMs) has been integrated to enrich the technical analysis of deviations, aligning findings with frameworks such as MITRE ATT&CK and Center for Internet Security Controls (CIS).

The development was carried out in a controlled test environment, following principles of least privilege and best practices in automation and security. Sustainability, economic impact, and ethical and regulatory compliance were also taken into account, including the handling of sensitive data and the responsible use of artificial intelligence. As a result, the solution reduces operational workload, improves traceability, and accelerates decision-making in response to security risks in multicloud environments.

Keywords:

Cloud Security, Security Deviations, Artificial Intelligence, Regulatory Compliance

Historial de ediciones y revisiones

Revisión	Fecha	Autor(es)	Descripción
1.0	10/04/2025	ABA	Creación del Documento
1.1	03/06/2025	ABA, JCG	Primera revisión
2.0	06/06/2025	ABA	Versión revisada incompleta
3.0	29/06/2025	ABA, JCG	Versión final
3.1	02/07/2025	ABA, JCG	Segunda revisión
4.0	14/07/2025	ABA, JCG	Versión final revisada

LISTA DE DISTRIBUCIÓN DEL DOCUMENTO

Rol	Apellido(s) y Nombre
Estudiante	Belinchón Álvarez, Alejandro
Tutor del proyecto	Castelo Gómez, Juan Manuel

Escrito por:	Revisado y aprobado por:
Fecha: 10/04/2025	Fecha: 14/07/2025
Nombre: Alejandro Belinchón Álvarez	Nombre: Juan Manuel Castelo Gómez
Rol: Autor/a del Proyecto	Rol: Director del Proyecto

Índice general

Índice de figuras

Índice de tablas

1. Introducción

La adopción de infraestructuras Cloud por parte de las organizaciones ha crecido de forma exponencial en los últimos años, principalmente impulsada por la necesidad de escalabilidad, flexibilidad y reducción de costos operativos. Este cambio de paradigma permite a las empresas modernizar sus servicios y adaptarse con mayor agilidad a las demandas del mercado. Sin embargo, también introduce una serie de desafíos específicos, especialmente en el ámbito de la ciberseguridad.

En los entornos tradicionales On-premise, las organizaciones mantenían un control total sobre todos los niveles de la infraestructura y los mecanismos de protección asociados. En cambio, en la nube, los modelos de responsabilidad compartida y la naturaleza dinámica de los recursos requieren una vigilancia constante para garantizar la seguridad. Los controles de seguridad deben revisarse de forma continua y su eficacia evaluarse frente a configuraciones erróneas, cambios no autorizados o brechas de cumplimiento. La capacidad de respuesta ante estos eventos es crítica para minimizar el impacto potencial sobre los sistemas, los datos y la reputación de la organización.

Actualmente, muchas empresas continúan utilizando procesos manuales para supervisar el cumplimiento de las políticas de seguridad y gestionar las desviaciones detectadas en sus entornos multicloud. Una desviación de seguridad hace referencia a cualquier situación en la que un recurso, servicio o configuración incumple un control de seguridad previamente establecido, ya sea por una mala configuración, un error humano o una modificación no autorizada. Estas tareas suelen implicar la extracción de informes, el análisis de desviaciones en hojas de cálculo y la documentación en plataformas de colaboración, lo que no solo consume una cantidad considerable de tiempo y recursos humanos, sino que también introduce un alto riesgo de error y una pérdida de trazabilidad. Esta situación es especialmente crítica en grandes entornos, donde el volumen de alertas puede crecer de forma no lineal y dificultar la priorización efectiva de las remediaciones necesarias.

Además, la falta de visibilidad consolidada y la baja automatización en estos procesos dificultan el cumplimiento de normativas como el Reglamento General de Protección de Datos (RGPD) o los marcos de referencia como la guía Center for Internet Security Controls (CIS), y reducen la capacidad de anticipación ante amenazas. En este sentido,

la automatización de la gestión de desviaciones, junto con la representación visual del estado de seguridad y la asignación eficiente de responsabilidades, se convierte en una necesidad clave dentro de las estrategias modernas de ciberseguridad.

Este Trabajo de Fin de Grado se centra en el diseño y desarrollo de una solución automatizada que permita mejorar la visibilidad, trazabilidad y control sobre las desviaciones de los controles de seguridad en entornos Cloud computing. A través de la integración de diversas herramientas, se plantea una propuesta que optimiza el proceso de supervisión de la postura de seguridad, reduce la intervención manual y facilita una respuesta más eficiente, robusta y alineada con las buenas prácticas del sector.

1.1. Objetivos

El objetivo principal de este proyecto es mejorar la eficiencia en la detección, análisis, notificación y resolución de desviaciones en controles de seguridad dentro de entornos cloud, mediante el uso de herramientas integradas como Prisma Cloud [1],Power Automate [2],SharePoint [3],Power BI [4] o Microsoft Teams [5]. A través de esta solución, se pretende transformar un proceso fragmentado y manual en un flujo estructurado, automatizado y fácilmente auditable.

Además de la optimización técnica, este proyecto busca contribuir a una mejora global de la postura de seguridad Cloud, asegurando el cumplimiento de buenas prácticas y marcos de referencia como los del CIS. La implementación de paneles visuales e informes automáticos permitirá una toma de decisiones más informada y ágil, adaptándose a las necesidades tanto del equipo técnico como de los responsables de cumplimiento normativo.

Objetivos específicos:

Para alcanzar el objetivo principal, se plantean los siguientes objetivos específicos:

- Analizar el estado actual del proceso de detección y gestión de desviaciones de seguridad en entornos Cloud.
- Identificar los puntos críticos de ineficiencia en el proceso manual de control y seguimiento.

- Diseñar un flujo de trabajo automatizado para la ingesta, tratamiento y almacenamiento de las desviaciones detectadas por Prisma Cloud.
- Implementar un sistema de almacenamiento estructurado utilizando SharePoint como backend ligero.
- Automatizar la generación y distribución de informes diarios mediante Power Automate y notificaciones en Microsoft Teams.
- Desarrollar paneles visuales dinámicos con Power BI que permitan el seguimiento continuo de las desviaciones y su evolución en el tiempo.
- Validar la solución propuesta en un entorno real de empresa, evaluando su efectividad, escalabilidad y facilidad de mantenimiento.

1.2. Motivación

El presente proyecto surge como respuesta a la necesidad de optimizar la gestión de desviaciones de seguridad en entornos Cloud, una problemática recurrente en organizaciones que operan bajo modelos de infraestructura compleja y multicloud. En muchos casos, los procesos actuales para el control de cumplimiento se apoyan en métodos manuales y herramientas heterogéneas, lo que genera fragmentación, sobrecarga operativa, escasa trazabilidad y una respuesta limitada ante incidentes.

Ante este contexto, se plantea el diseño de una solución automatizada que permita estructurar de forma integral el ciclo de vida de las desviaciones, desde su detección hasta su resolución. La propuesta se apoya en herramientas ampliamente adoptadas en entornos empresariales como Prisma Cloud [1], Power Automate [2], SharePoint [3] y Power BI [4], con el objetivo de consolidar un flujo de trabajo eficiente, trazable y accesible para equipos técnicos y responsables de cumplimiento.

La relevancia de esta iniciativa radica en su contribución al fortalecimiento de la postura de seguridad cloud mediante la mejora del control sobre los hallazgos técnicos y su resolución. Asimismo, permite avanzar en la integración de procesos de gobernanza y automatización, alineándose con las tendencias actuales del sector y los principios de eficiencia, cumplimiento normativo y reducción de riesgos operativos en ciberseguridad.

1.3. Metodología y plan de trabajo

El desarrollo del proyecto se dividirá en distintas fases, siguiendo un enfoque iterativo y orientado a la resolución de problemas reales en entornos empresariales. Esta metodología se inspira en prácticas recomendadas para la automatización de procesos en seguridad cloud y la mejora continua de la postura de cumplimiento [6], [7].

- **Análisis del estado actual:** se realizará una revisión del proceso vigente de gestión de desviaciones en entornos Cloud, identificando los puntos críticos, las herramientas utilizadas y las limitaciones operativas detectadas [6].
- **Recolección y categorización de desviaciones:** se recopilarán datos reales de cumplimiento de controles de seguridad mediante Prisma Cloud y otras fuentes. El análisis incluirá criterios como criticidad, recurrencia o tipo de control afectado, de acuerdo con guías como CIS Controls [8].
- **Diseño del flujo automatizado:** se definirá una arquitectura funcional basada en herramientas como Power Automate, SharePoint, Power BI y Microsoft Teams, orientada a orquestar las tareas de seguimiento, asignación, análisis, remediación y visualización de las desviaciones [2][3][4][5].
- **Implementación técnica:** se desarrollarán los flujos automatizados utilizando conectores y scripts adaptados al entorno empresarial. Las listas de seguimiento se construirán sobre SharePoint [3] y se integrarán con las plataformas de automatización y visualización.
- **Validación y pruebas:** la solución será evaluada en un entorno de pruebas, comprobando su capacidad para reducir tareas manuales, mejorar la trazabilidad y facilitar el análisis de cumplimiento normativo mediante paneles en Power BI [4].
- **Documentación y evaluación final:** se documentará todo el proceso de diseño, implementación y resultados obtenidos, analizando los beneficios en términos de eficiencia, visibilidad y alineación con las buenas prácticas de seguridad cloud [7].

1.3.1. Plan de Trabajo

En la Figura 1.1 y en la Tabla 1.1 podemos ver el flujo del proyecto respecto al tiempo de desarrollo.

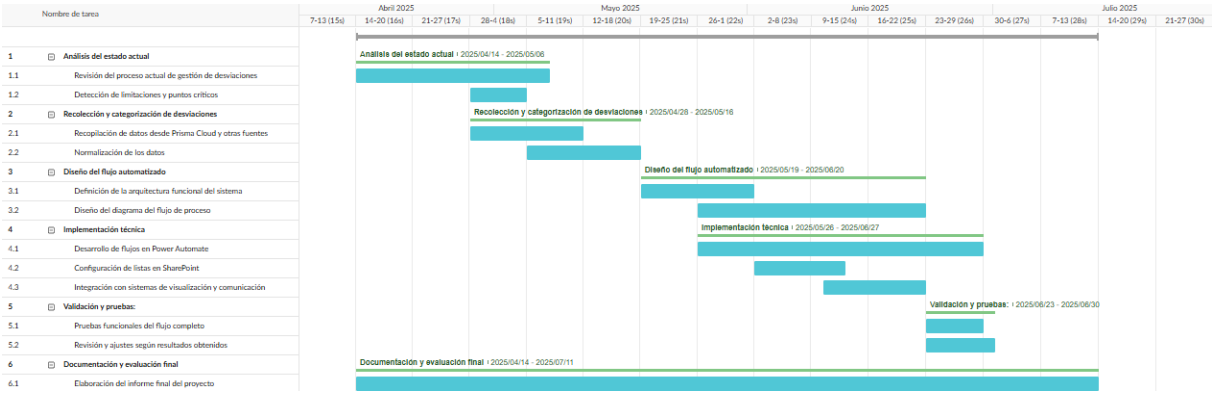


Figura 1.1. Desarrollo del proyecto respecto al tiempo.

Tarea	Subtareas
1. Análisis del estado actual	1.1 Revisión del proceso actual de gestión de desviaciones 1.2 Detección de limitaciones y puntos críticos
2. Recolección y categorización de desviaciones	2.1 Recopilación de datos desde Prisma Cloud y otras fuentes 2.2 Normalización de los datos
3. Diseño del flujo automatizado	3.1 Definición de la arquitectura funcional del sistema 3.2 Diseño del diagrama del flujo de proceso
4. Implementación técnica	4.1 Desarrollo de flujos en Power Automate 4.2 Configuración de listas en SharePoint 4.3 Integración con sistemas de visualización y comunicación
5. Validación y pruebas	5.1 Pruebas funcionales del flujo completo 5.2 Revisión y ajustes según resultados obtenidos
6. Documentación y evaluación final	6.1 Elaboración del informe final del proyecto

Tabla 1.1. Tareas y subtareas del proyecto según el diagrama de Gantt 1.1

1.4. Estructura del proyecto

El presente trabajo se organiza como la Figura 1.2, cada capítulo enfocado en una fase concreta del desarrollo del proyecto:

- **Capítulo 1 – Introducción:** presenta el contexto general del trabajo, junto con la motivación, justificación, objetivos y metodología planteada.
- **Capítulo 2 – Estado del arte:** recoge los fundamentos teóricos y técnicos necesarios, abordando los modelos de computación en la nube, los principales retos de seguridad cloud y las tendencias actuales, con especial énfasis en la automatización de procesos.
- **Capítulo 3 – Material y desarrollo del proyecto:** detalla el escenario de partida, el diseño funcional y técnico de la solución, la implementación práctica y el proceso de validación mediante pruebas reales.
- **Capítulo 4 – Análisis de sostenibilidad e implicaciones éticas:** evalúa el impacto medioambiental, económico y social del proyecto, así como su alineación con principios éticos y normativas relevantes.
- **Capítulo 5 – Conclusiones y mejoras futuras:** resume los principales resultados obtenidos, identifica las limitaciones encontradas y propone posibles líneas de evolución y mejora del sistema desarrollado.

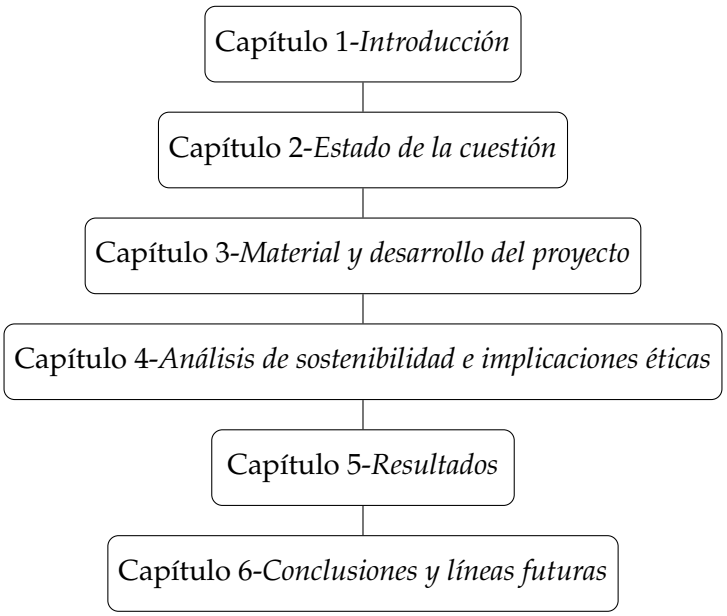


Figura 1.2. Estructura lógica del proyecto

2. Estado de la cuestión

Antes de abordar el problema propuesto, debemos comprender el contexto tecnológico y conceptual en el que se enmarca este proyecto. En este capítulo se revisan los conceptos clave relacionados con la **computación en la nube**, se analiza el estado actual de la **ciberseguridad en entornos cloud**, y se profundiza en los retos asociados a la **visibilidad y gestión de desviaciones de seguridad**.

Esta revisión permite identificar las limitaciones de los enfoques actuales y justificar la necesidad de una solución automatizada, integrada y visual, como la que se plantea en este trabajo.

2.1. Computación Cloud

La Cloud —o computación en la nube— es un modelo tecnológico que permite el acceso bajo demanda a recursos informáticos a través de Internet. En lugar de almacenar y ejecutar aplicaciones localmente en dispositivos físicos, este modelo se basa en una red global de servidores remotos que actúan como un único ecosistema, ofreciendo servicios de almacenamiento, procesamiento, redes, software y datos a través de plataformas distribuidas.

En la Figura 2.1 podemos ver un sistema básico de la arquitectura de un servicio Cloud.

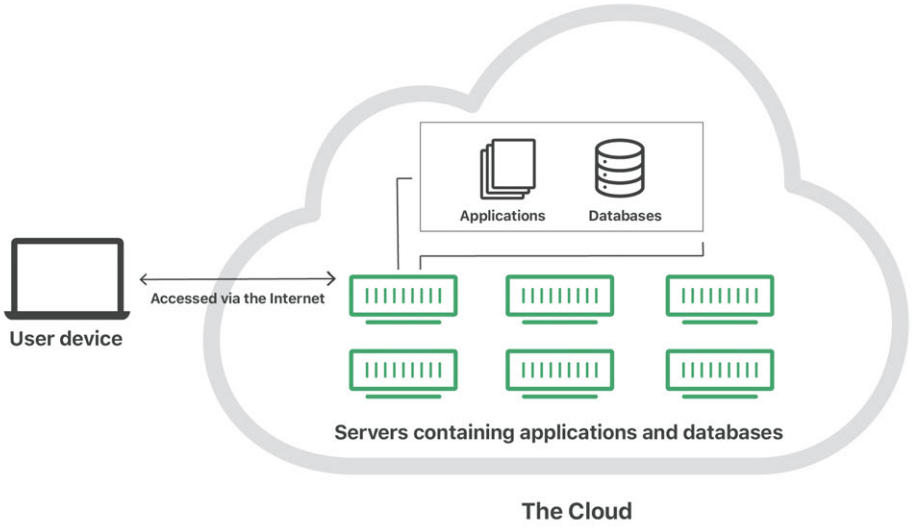


Figura 2.1. Diagrama básico de la Cloud [7]

La adopción del Cloud computing ha supuesto una transformación profunda en las Tecnologías de la Información (TI), tanto para usuarios particulares como para empresas. Desde pequeñas *startups* hasta grandes corporaciones, la nube ofrece flexibilidad, escalabilidad y acceso remoto a datos y aplicaciones, eliminando la necesidad de mantener infraestructura física local.

Hoy en día, el Cloud computing se ocupa de actividades cotidianas como enviar un correo o ver una serie, hasta procesos empresariales complejos como el teletrabajo, la gestión omnicanal de clientes o el entrenamiento de modelos de inteligencia artificial. Estos servicios son gestionados por proveedores de servicios en la nube (Cloud Service Provider (CSP)), que los alojan en centros de datos remotos y los ofrecen generalmente mediante modelos de suscripción o pago por uso.

Para comprender mejor el alcance y la utilidad del modelo cloud, es necesario analizar sus principales componentes: los modelos de implementación, los servicios disponibles y las ventajas que aporta su adopción.

2.1.1. Modelos de implementación

El modelo de implementación de la nube define cómo se despliegan y gestionan los recursos informáticos y servicios dentro de una organización. Esta decisión tiene un impacto directo sobre la seguridad, el control, la escalabilidad y el coste de la infraestructura tecnológica. Existen diversas formas de implementar una solución basada en Cloud computing, y su elección depende de factores como los requisitos de cumplimiento normativo, la sensibilidad de los datos, la criticidad de las aplicaciones o la necesidad de flexibilidad operativa.

A continuación, se explican los diferentes modelos de uso de la infraestructura:

Nube pública

En un entorno de *nube pública*, los recursos de computación —como servidores, almacenamiento y redes— son propiedad y están gestionados por proveedores externos de servicios en la nube, como Amazon Web Services (AWS) [9], Microsoft Azure (Azure) [10], Google Cloud Platform (GCP) [11], Infraestructura y servicios cloud de International Business Machines (IBM Cloud) [12] o Oracle Cloud Infrastructure (OCI) [13]. Estos recursos se comparten entre múltiples clientes mediante un modelo de Tenencia múltiple, donde cada organización accede a entornos virtualizados aislados, aunque alojados en la misma infraestructura física.

Este modelo permite una escalabilidad prácticamente ilimitada, alta disponibilidad, rapidez de despliegue y una amplia gama de servicios avanzados. Además, suele operar bajo esquemas de pago por uso, lo que reduce la inversión inicial. No obstante, al compartir infraestructura con otros clientes, pueden surgir desafíos relacionados con la seguridad, la segmentación de datos y el cumplimiento de normativas específicas.

Nube privada

La *nube privada* es una infraestructura dedicada exclusivamente a una sola organización. Puede estar alojada en las propias instalaciones de la empresa (On-premise) o ser proporcionada por un proveedor externo como podemos ver en la Figura 2.2, pero, en cualquier caso, los recursos son exclusivos y no se comparten con otras entidades.

Este modelo ofrece un control completo sobre la configuración, los datos y las políticas de seguridad, siendo especialmente adecuado para organizaciones que gestionan información sensible, que deben cumplir requisitos regulatorios estrictos o que necesitan personalizar su infraestructura. A cambio, presenta mayores costos de despliegue y mantenimiento, y una escalabilidad más limitada en comparación con la nube pública.

Una variante relevante es la Virtual Private Cloud (VPC), una red privada virtual aislada dentro de un entorno de nube pública. La VPC permite segmentar recursos virtualizados con un alto grado de control sobre aspectos como direcciones IP, subredes y reglas de seguridad, combinando algunas ventajas de la nube privada con la flexibilidad de la nube pública.

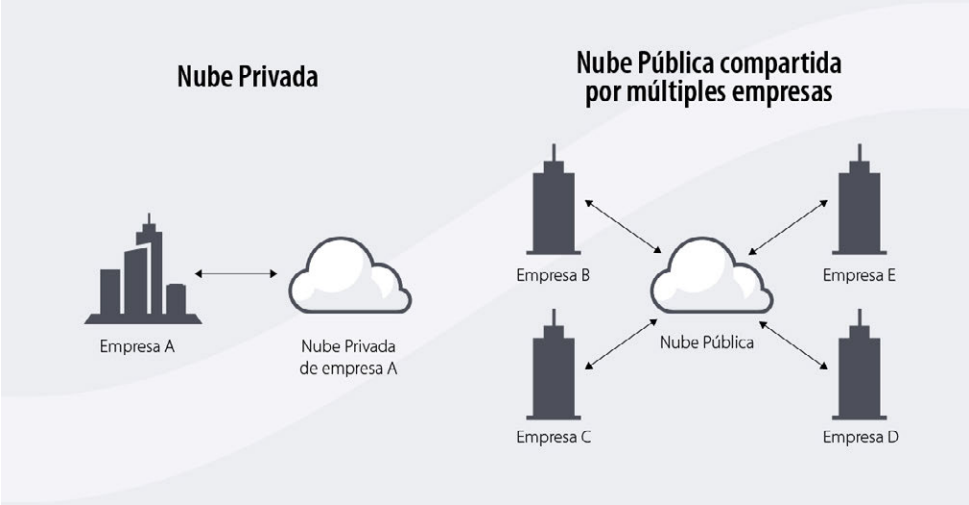


Figura 2.2. Modelo de nube privada y pública [14]

Nube híbrida

Este modelo combina servicios de nube pública y privada, permitiendo la portabilidad de datos y aplicaciones entre ambos entornos. Permite aprovechar la elasticidad de la nube pública para picos de demanda, mientras se mantienen operaciones sensibles en la nube privada. Es una opción muy flexible para organizaciones que buscan escalabilidad sin comprometer el control.

El modelo de *nube híbrida* combina entornos de Cloud pública, Cloud privada e incluso Infraestructura heredada local (On-premise) en una arquitectura unificada. Esta combinación permite a las organizaciones distribuir sus cargas de trabajo entre distintos entornos en función de criterios como la sensibilidad de los datos, el coste, la disponi-

bilidad o los requisitos normativos.

Una de las principales ventajas de este enfoque es la flexibilidad para adaptar la ubicación de los recursos según las necesidades. Por ejemplo, las aplicaciones críticas o que manejan datos confidenciales pueden permanecer en la nube privada o en infraestructura local, mientras que las aplicaciones de menor sensibilidad o que requieren mayor escalabilidad pueden migrarse a la nube pública. Esta separación ayuda a optimizar el rendimiento y la eficiencia operativa sin sacrificar el control sobre la información más crítica.

Además, la nube híbrida permite responder de forma dinámica ante picos de demanda mediante el uso de Cloud bursting, es decir, el redireccionamiento automático de cargas de trabajo a la nube pública cuando los recursos locales no son suficientes. También facilita migraciones graduales, integración de Infraestructura heredada y garantiza el Business Continuity, especialmente útil en entornos con alta dependencia tecnológica.

Este modelo, si bien ofrece lo mejor de ambos mundos, también presenta desafíos importantes, ya que las operaciones entre plataformas se vuelven más complejas, la complejidad en la gestión de la seguridad es notablemente superior y la necesidad de herramientas de orquestación avanzadas para garantizar una operación coherente se vuelve imprescindible.

Multinube

El enfoque *multicloud* o *multinube* se basa en la utilización de múltiples plataformas de Cloud públicas ofrecidas por distintos proveedores, como AWS, Azure, GCP, IBM Cloud o OCI, dentro de una misma organización. A diferencia del modelo híbrido, en el que se combinan entornos públicos y privados, la estrategia multinube se enfoca en diversificar la infraestructura cloud exclusivamente entre proveedores públicos.

Este modelo permite seleccionar el proveedor más adecuado para cada tipo de carga de trabajo en función de factores como rendimiento, disponibilidad regional, costes, servicios específicos o cumplimiento normativo. Además, proporciona mayor resiliencia operativa y evita el *vendor lock-in*, es decir, la dependencia exclusiva de un único proveedor.

No obstante, la adopción de una estrategia multinube también introduce retos adicionales. Entre ellos, destacan la complejidad de gestionar entornos heterogéneos, la nece-

sidad de estandarizar mecanismos de autenticación, monitoreo y gestión de configuración, así como la integración entre plataformas. Para facilitar su adopción, suelen utilizarse herramientas de orquestación y plataformas de administración unificadas, que permiten abstraer las diferencias entre proveedores y centralizar el control.

En un contexto empresarial donde la resiliencia, la disponibilidad global y la flexibilidad son prioritarias, la estrategia multinube se presenta como una solución robusta y la más escalable, especialmente en organizaciones de gran tamaño o con operaciones distribuidas.

En la Figura 2.3 podemos observar el funcionamiento del modelo multicloud.

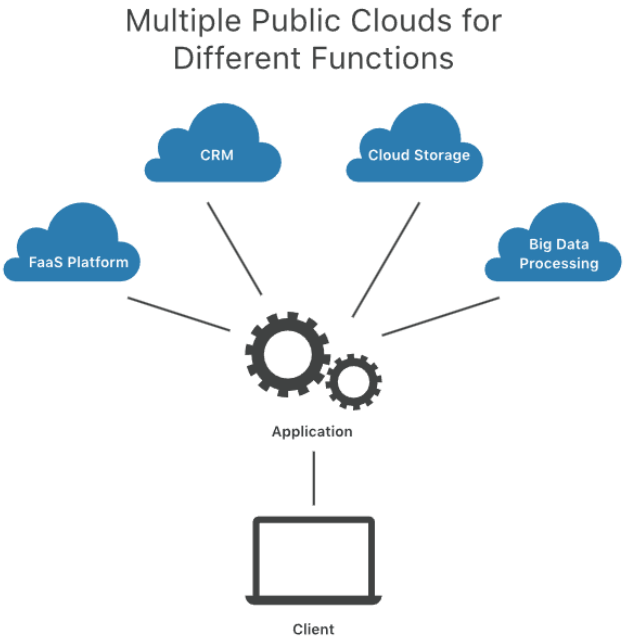


Figura 2.3. Modelo MultiCloud [15]

2.1.2. Tipos de servicios

Además de los modelos de implementación, la computación en la nube ofrece distintos niveles de servicio, que definen el grado de control y responsabilidad que asume el proveedor frente al cliente. Estos modelos se representan habitualmente como capas de abstracción que van desde la provisión directa de recursos virtualizados hasta el consumo de aplicaciones completamente gestionadas.

Los principales modelos de servicio son: Infrastructure as a Service (IaaS), Platform as

a Service (PaaS), Software as a Service (SaaS), Function as a Service (FaaS) y Container as a Service (CaaS). Cada uno proporciona distintas funcionalidades, ventajas y niveles de abstracción, siendo adecuados para distintos casos de uso y perfiles técnicos.

A medida que se asciende en la pila, el usuario cede más responsabilidades al proveedor: desde la gestión de máquinas virtuales y redes (en IaaS) hasta la ejecución de código sin preocuparse por la infraestructura (en FaaS). En este contexto, también existen modelos especializados como Backend as a Service (BaaS), orientados al desarrollo rápido de aplicaciones móviles y web.

En las siguientes secciones se detallan las características principales de cada modelo de servicio.

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) es el modelo de servicio en la nube que ofrece recursos de infraestructura virtualizados —como máquinas virtuales, almacenamiento, redes o sistemas de virtualización— directamente a través de Internet. El proveedor se encarga de la gestión de la infraestructura física, incluyendo servidores, centros de datos y redes, mientras que el cliente mantiene el control restante para sus preferencias específicas. Esto proporciona una gran flexibilidad y escalabilidad, sin necesidad de adquirir ni mantener hardware físico, aunque requiere conocimientos técnicos por parte del usuario.

Entre los principales proveedores se encuentran AWS [9] con Elastic Compute Cloud (EC2), Azure [10] con sus *Virtual Machines*, GCP [11] con Compute Engine, así como IBM Cloud [12], OCI [13], DigitalOcean y plataformas de código abierto como OpenStack. El modelo IaaS es ideal para equipos técnicos que necesitan construir entornos personalizados, especialmente en proyectos donde se requiere controlar el entorno operativo o escalar dinámicamente según la carga de trabajo.

Container as a Service (CaaS)

Container as a Service (CaaS) es un modelo intermedio entre IaaS y PaaS que proporciona una plataforma completa para gestionar Contenedores como recurso principal. A través de este servicio, los desarrolladores pueden desplegar, ejecutar, escalar y administrar aplicaciones contenidas sin tener que gestionar directamente la infraestructura

subyacente. Aunque el cliente mantiene el control sobre el código y la configuración de sus contenedores, el proveedor se encarga del entorno de ejecución, las herramientas de orquestación y la infraestructura de soporte.

Este modelo está especialmente orientado a arquitecturas basadas en microservicios, ya que facilita la portabilidad, la escalabilidad automática y la implementación continua (*CI/CD*). Entre las plataformas más representativas se encuentran Google Kubernetes Engine (GKE) [16], Amazon Elastic Kubernetes Service (EKS) [17] y Azure Kubernetes Service (AKS) [18]. Aunque a veces se considera una extensión especializada del modelo IaaS, CaaS abstrae gran parte de la complejidad operativa asociada a la ejecución de contenedores, permitiendo a las organizaciones centrarse en el ciclo de vida de sus aplicaciones sin comprometer el control sobre su despliegue.

Platform as a Service (PaaS)

Platform as a Service (PaaS) es un modelo de servicio en la nube que proporciona un entorno completo para desarrollar, ejecutar y gestionar aplicaciones, sin que el cliente tenga que administrar la infraestructura subyacente. El proveedor ofrece desde el sistema operativo hasta el servidor de aplicaciones, incluyendo herramientas de desarrollo, bases de datos y Middleware, permitiendo a los equipos enfocarse exclusivamente en el ciclo de vida del software. Este modelo reduce significativamente el tiempo de despliegue, facilita la colaboración entre desarrolladores y mejora la eficiencia operativa, especialmente en metodologías ágiles y enfoques DevOps.

Entre los servicios más representativos se encuentran Google App Engine, Microsoft Azure App Service, Heroku y Red Hat OpenShift [19]. Algunos proveedores también integran funcionalidades propias de BaaS, ofreciendo Application Programming Interface (API)s preconfiguradas para autenticación, almacenamiento o gestión de usuarios. PaaS es especialmente útil para desarrolladores que necesitan desplegar aplicaciones rápidamente sin preocuparse por la configuración del servidor, escalado automático o actualizaciones de sistema. Como en otros modelos de Cloud, se basa en el acceso bajo demanda y el modelo de pago por uso, con escalabilidad flexible según las necesidades de la aplicación.

Function as a Service (FaaS)

Function as a Service (FaaS), también conocida como computación sin servidor, es un modelo de servicio en la nube que permite ejecutar fragmentos de código en respuesta a eventos, sin necesidad de gestionar servidores ni mantener entornos persistentes. El proveedor se encarga del aprovisionamiento automático, el escalado dinámico y la infraestructura subyacente, mientras que el cliente se limita a desarrollar funciones individuales que responden a activadores específicos como peticiones HTTP, eventos en bases de datos o mensajes en colas.

Entre las plataformas más representativas se encuentran AWS Lambda [20], Google Cloud Functions [21], Azure Functions [22] y IBM Cloud Functions [23]. FaaS es especialmente adecuado para arquitecturas orientadas a eventos, microservicios y cargas de trabajo esporádicas, ya que permite reducir costos al facturar solo por el tiempo efectivo de ejecución. Su modelo sin estado y de alta escalabilidad lo convierte en una solución muy eficiente para tareas automatizadas, procesos desencadenados por eventos o entornos de desarrollo ágiles.

Software as a Service (SaaS)

Software as a Service (SaaS) es el modelo más alto de abstracción en la computación en la nube. En él, el proveedor gestiona de forma integral toda la pila tecnológica: desde la infraestructura hasta las aplicaciones, incluyendo el sistema operativo, la plataforma de desarrollo, el almacenamiento y la seguridad. El usuario final accede a la aplicación directamente a través de Internet, sin necesidad de instalación, configuración ni mantenimiento local, lo que facilita el uso inmediato y reduce la complejidad operativa.

SaaS es ideal para soluciones empresariales y de productividad, ya que ofrece escalabilidad, actualizaciones automáticas y acceso multiplataforma. Entre los servicios más conocidos se encuentran Microsoft 365 [24], Google Workspace [25], Salesforce [26], Dropbox [27], Slack [28] y Mailchimp [29], que permiten a usuarios y organizaciones consumir software de manera flexible bajo modelos de suscripción o pago por uso. Este modelo es especialmente útil cuando se busca rapidez de adopción, reducción de costes de infraestructura y accesibilidad desde cualquier ubicación.

En la figura 2.4, se detallan las responsabilidades de gestión y seguridad que tienen el cliente y el proveedor para cada modelo explicado:

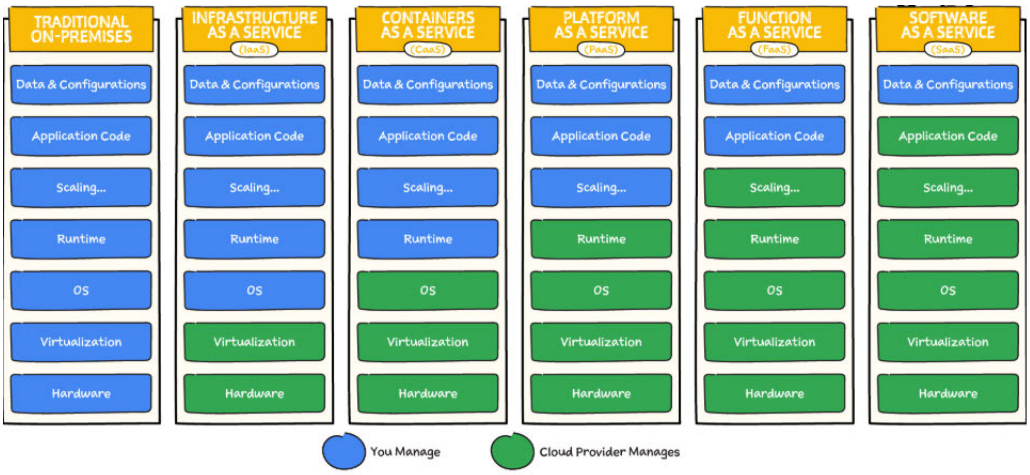


Figura 2.4. Esquema completo de las diferencias entre los servicios [30]

2.1.3. Ventajas y oportunidades

La adopción del modelo Cloud computing ha supuesto una evolución significativa en la forma en que las organizaciones gestionan sus recursos tecnológicos. A través de servicios bajo demanda, escalabilidad automática y gestión centralizada, el cloud computing facilita un entorno ágil, seguro y resiliente, alineado con las necesidades actuales de transformación digital.

- **Optimización de costes.** El modelo de facturación *pay-as-you-go* permite pagar exclusivamente por los recursos utilizados, evitando inversiones iniciales elevadas en infraestructura física y reduciendo los costes operativos. Esto libera a los equipos de TI para que puedan enfocarse en tareas estratégicas en lugar de en el mantenimiento de hardware.
- **Escalabilidad y flexibilidad.** La nube permite ajustar dinámicamente la capacidad de procesamiento, almacenamiento y red en función de la demanda del momento. Esta elasticidad evita el sobredimensionamiento y permite responder con agilidad a cambios en el volumen de usuarios, tráfico o datos procesados.
- **Alta disponibilidad y resiliencia.** Los principales CSPs implementan arquitecturas distribuidas y redundantes que garantizan la disponibilidad continua de los servicios, incluso ante fallos en una región o centro de datos. Además, la nube facilita estrategias de Disaster Recovery (DR) con menores costes y tiempos de recuperación optimizados.

- **Agilidad y velocidad de despliegue.** La infraestructura en la nube puede aprovisionarse en cuestión de minutos, lo que permite lanzar entornos de desarrollo, pruebas o producción sin las demoras típicas de los entornos On-premise. Esta agilidad mejora el Time-to-market y acelera los procesos de innovación.
- **Rendimiento optimizado.** Los entornos cloud suelen funcionar sobre hardware de última generación, con mantenimiento continuo y posibilidad de seleccionar zonas geográficas próximas al usuario final para minimizar la latencia. Esto se traduce en aplicaciones más rápidas y eficientes.
- **Colaboración y acceso global.** Al estar basados en Internet, los servicios en la nube permiten el acceso remoto y simultáneo desde cualquier ubicación, fomentando la colaboración entre equipos distribuidos y facilitando modalidades de trabajo como el teletrabajo.
- **Seguridad gestionada.** A pesar de las dudas iniciales, la nube ofrece capacidades avanzadas de seguridad gracias a la supervisión constante, parches automáticos, cifrado por defecto y gestión de identidades centralizada, que se engloba dentro del conceppto de Identity and Access Management (IAM). Los CSPs integran también mecanismos de cumplimiento normativo y auditoría.
- **Innovación y acceso a tecnologías emergentes.** Plataformas cloud ofrecen servicios integrados de inteligencia artificial, *machine learning*, analítica avanzada, Internet of Things (IoT) o blockchain, que pueden activarse de forma inmediata sin necesidad de infraestructura dedicada. Esto democratiza el acceso a capacidades tecnológicas de alto valor y potencia la competitividad.

2.2. Ciberseguridad en los entornos Cloud

El crecimiento exponencial del Cloud computing ha traído consigo una transformación en la forma en que las organizaciones diseñan, despliegan y gestionan sus sistemas de información. Sin embargo, este nuevo paradigma también ha introducido retos específicos en materia de seguridad. La ciberseguridad en entornos cloud no solo debe proteger los datos y sistemas, sino también adaptarse a un entorno altamente dinámico, distribuido y compartido, donde la responsabilidad se reparte entre el proveedor y el cliente bajo el modelo de responsabilidad compartida.

Garantizar la confidencialidad, integridad y disponibilidad de la información alojada en la nube requiere no solo herramientas técnicas, sino también una estrategia de seguridad integral que contemple controles preventivos, detectivos y correctivos, así como el cumplimiento de marcos de referencia internacionales como CIS, Organización Internacional de Normalización (ISO) o National Institute of Standards and Technology (NIST).

2.2.1. Desafíos y riesgos en entornos cloud

La adopción de entornos Cloud conlleva una serie de beneficios, pero también introduce desafíos de seguridad específicos que deben ser gestionados de forma proactiva. La naturaleza dinámica y distribuida de la nube obliga a replantear los mecanismos tradicionales de protección de la información, los accesos y la infraestructura. A continuación, se describen los principales retos que enfrentan las organizaciones en este ámbito.

Gestión de identidades y accesos.

Uno de los pilares fundamentales de la seguridad en la nube es el control de quién accede a qué recursos y en qué condiciones. La implementación de soluciones de IAM permite centralizar y auditar los accesos de usuarios, aplicaciones y servicios. En este contexto, modelos como Role-Based Access Control (RBAC) asignan privilegios en función de roles específicos dentro de la organización, mientras que enfoques como el modelo Zero Trust exigen validaciones continuas independientemente de la ubicación o del dispositivo desde el que se realiza el acceso. Estos mecanismos permiten reducir la superficie de ataque y garantizar el Principio de menor privilegio.

Protección de datos.

Los datos representan uno de los activos más críticos y vulnerables en entornos cloud. Su protección requiere adoptar medidas durante todo su ciclo de vida:

- Cifrado en tránsito mediante Transport Layer Security (TLS), y en reposo con algoritmos como AES-256.
- Gestión de claves con herramientas como Key Management Service (KMS) o Azure Key Vault.
- Políticas de retención y borrado seguro alineadas con normativas.

- Implementación de Backups cifrados y planes de Disaster Recovery (DR).

Estas prácticas permiten garantizar la confidencialidad, integridad y disponibilidad de la información, incluso en escenarios de fallo o incidente.

Cumplimiento normativo.

Las organizaciones deben asegurar el cumplimiento de normativas nacionales e internacionales, especialmente en sectores regulados. Entre los marcos más relevantes se encuentran el RGPD, ISO, el NIST Cybersecurity Framework y los CISs Controls. Este último, siendo con el que se trabaja en este proyecto, proporciona una lista priorizada de controles que permiten evaluar y fortalecer la postura de seguridad, adaptándose a distintos entornos IaaS. La falta de cumplimiento no solo expone a la organización a riesgos de seguridad, sino también a sanciones legales y pérdida de confianza.

Monitorización continua y visibilidad.

La supervisión activa de los recursos desplegados en la nube es clave para detectar incidentes, vulnerabilidades y configuraciones indebidas. Las herramientas de Cloud Security Posture Management (CSPM), como Prisma Cloud, permiten auditar de forma continua la configuración de los servicios cloud en tiempo real y detectar desviaciones respecto a las buenas prácticas o a marcos de referencia como los CISs Controls. En el contexto de este proyecto, Prisma Cloud actúa como la herramienta principal para supervisar la postura de seguridad en entornos IaaSs, proporcionando una visión consolidada del estado de cumplimiento y las brechas de seguridad existentes.

Por su parte, las soluciones SIEM, como DEVO, desempeñan un papel crucial en la detección de amenazas a nivel de eventos. Estos sistemas permiten recolectar, analizar y correlacionar grandes volúmenes de datos generados por distintos componentes de la infraestructura, incluyendo logs de aplicaciones, sistemas operativos, redes, bases de datos o servicios cloud. A través de reglas de correlación, algoritmos de detección de anomalías y análisis en tiempo real, los SIEMs ofrecen capacidades avanzadas para identificar comportamientos sospechosos, trazas de posibles ataques y responder ante incidentes de forma proactiva. Además, proporcionan un historial auditable que puede ser clave en procesos de análisis forense o cumplimiento normativo.

No obstante, la información técnica generada por estas herramientas puede resultar compleja de interpretar para perfiles no especializados. Por ello, la incorporación de paneles visuales dinámicos mediante Power BI permite representar los datos de forma más accesible y comprensible. Esta visualización facilita la toma de decisiones tanto pa-

ra los equipos técnicos como para los responsables de cumplimiento o incluso clientes externos, favoreciendo una comunicación más efectiva y una respuesta más rápida ante riesgos identificados.

2.2.2. Tendencias en seguridad cloud

El ecosistema de seguridad en entornos Cloud se encuentra en constante evolución. Las organizaciones deben adaptarse a nuevas amenazas, tecnologías emergentes y metodologías avanzadas para proteger su infraestructura. A continuación, se detallan algunas de las principales tendencias que están redefiniendo la ciberseguridad en la nube.

Aplicación de inteligencia artificial y aprendizaje automático

La integración de soluciones basadas en IA y Machine Learning (ML) ha mejorado significativamente las capacidades de detección y respuesta ante incidentes. Estas tecnologías permiten analizar grandes volúmenes de datos, identificar patrones anómalos, anticipar comportamientos maliciosos y priorizar alertas en tiempo real. Además, son clave en la automatización de sistemas SIEM, mejorando la eficiencia operativa y la toma de decisiones frente a amenazas avanzadas como los Advanced Persistent Threat (APT).

Seguridad en Infrastructure as Code (IaC)

El paradigma Infrastructure as Code (IaC) ha transformado la forma en que se despliega y gestiona la infraestructura cloud. Herramientas como Terraform [31] permiten definir los recursos como código, facilitando despliegues reproducibles y controlados. Sin embargo, este enfoque también implica nuevos riesgos: errores en el código pueden traducirse en configuraciones inseguras. Para mitigar estos riesgos, se emplean herramientas como Checkov [32] o KICS [33], que escanean los scripts y detectan posibles vulnerabilidades antes de ser aplicados. Este enfoque de seguridad temprana es esencial para construir entornos seguros desde su diseño.

Computación cuántica y criptografía post-cuántica

Aunque la computación cuántica aún no ha alcanzado su madurez comercial, su potencial impacto en el ámbito de la ciberseguridad es significativo. Los algoritmos criptográficos actuales como RSA y los basados en ECC podrían quedar obsoletos ante la capacidad de procesamiento de un ordenador cuántico, capaz de romper claves criptográficas mediante algoritmos como el Algoritmo de Shor. Ante este panorama, instituciones como el NIST están desarrollando estándares de criptografía post-cuántica, diseñados para resistir ataques incluso en contextos donde la computación cuántica sea una realidad.

Análisis de *attack paths*

El análisis de rutas de ataque permite visualizar de forma contextual las posibles cadenas de explotación que un atacante podría seguir dentro del entorno cloud. Esta metodología se basa en la correlación entre identidades, permisos, configuraciones inseguras y servicios expuestos. Gracias a tecnologías de análisis de grafos y soluciones especializadas, las organizaciones pueden identificar rutas críticas, reforzar controles en puntos estratégicos y prevenir ataques antes de que se materialicen. Este enfoque se alinea con modelos proactivos de defensa y cobra especial relevancia en entornos multicloud.

2.2.3. Automatización de flujos de seguridad

La automatización de flujos en seguridad cloud reduce la intervención manual, mejora la eficiencia operativa y minimiza el error humano. Herramientas como Power Automate[2] permiten construir flujos que integran múltiples plataformas, gestionan eventos y generan respuestas inmediatas ante desviaciones.

Ejemplos de automatización incluyen:

- Notificaciones automáticas a responsables ante incidentes críticos.
- Integración de datos desde fuentes heterogéneas en repositorios como SharePoint.
- Priorización automatizada de eventos por criticidad.
- Generación de alertas y visualización en tiempo real en Power BI.

Estas prácticas permiten aplicar de forma coherente las políticas de seguridad, mantener actualizada la visibilidad del entorno y garantizar tiempos de reacción más cortos ante amenazas emergentes.

2.2.4. Contribución del proyecto al estado de la cuestión

La solución propuesta en este proyecto responde a muchos de los desafíos y tendencias anteriormente descritos. Mediante la integración de datos desde Prisma Cloud, su almacenamiento en SharePoint, su tratamiento con Power Automate y su visualización mediante Power BI, se proporciona un flujo completamente automatizado, auditable y comprensible para equipos técnicos y responsables de cumplimiento.

El proyecto destaca por:

- Unificar diferentes fuentes de información en una única plataforma de análisis.
- Detectar y visualizar desviaciones de seguridad en tiempo real.
- Aplicar filtros dinámicos que permiten priorizar acciones correctivas.
- Alinearse con los controles del manual CIS, fortaleciendo la postura de seguridad cloud y el cumplimiento normativo.

2.3. Visibilidad y gestión de desviaciones

La visibilidad sobre las configuraciones, accesos y eventos es fundamental para detectar posibles incumplimientos de las políticas de seguridad establecidas. En este contexto, la identificación y gestión eficaz de desviaciones se convierte en un proceso crítico para prevenir incidentes, garantizar el cumplimiento normativo y mantener la integridad de los sistemas.

Antes de abordar los mecanismos técnicos que permiten su monitorización y resolución, es importante definir con claridad el concepto de desviación de seguridad, su tipología y el papel que desempeña dentro de la gestión del riesgo en entornos cloud.

2.3.1. Qué es una desviación de seguridad

Una desviación de seguridad en entornos cloud se define como cualquier discrepancia entre el estado actual de un recurso o configuración y las políticas, estándares o buenas prácticas de seguridad predefinidos. Estas desviaciones pueden incluir permisos excesivos, puertos abiertos sin justificación, recursos sin cifrado, almacenamiento expuesto públicamente o la ausencia de controles de Disaster Recovery (DR).

Las desviaciones pueden ser accidentales —como errores de configuración por parte de los desarrolladores— o intencionales, como resultado de actividades maliciosas. Detectarlas de manera temprana es esencial para mitigar su impacto y evitar su explotación por parte de actores maliciosos.

En este contexto, los controles de seguridad definidos por el CIS, así como normativas como el RGPD, proporcionan un marco de referencia para identificar desviaciones de forma sistemática. La automatización de esta detección y el uso de flujos de trabajo permiten no solo visibilizar estas desviaciones, sino también clasificarlas, priorizarlas y resolverlas con mayor agilidad.

En la Figura 2.5 podemos ver cómo funciona un control de la guía CIS .

Figura 2.5. Esquema Compliance-Deviation. Proporcionada por el equipo de trabajo.

2.3.2. Visibilidad en seguridad cloud y su necesidad

La visibilidad en entornos Cloud se refiere a la capacidad de obtener información detallada y actualizada sobre el estado de los recursos, configuraciones, identidades, accesos y eventos de seguridad. Esta capacidad resulta crítica debido a la naturaleza dinámica y distribuida de los entornos Cloud, donde los activos pueden desplegarse y modificarse constantemente sin intervención directa de los equipos de seguridad.

Sin una visibilidad adecuada, las organizaciones se enfrentan a una superficie de ataque ampliada, con una mayor probabilidad de sufrir brechas por errores de configuración, accesos no autorizados o actividades maliciosas no detectadas. Por ello, las estrategias modernas de ciberseguridad cloud integran herramientas como Cloud Security Posture Management (CSPM), SIEM o EDR que permiten recopilar, correlacionar y analizar grandes volúmenes de datos operacionales y de seguridad.

En este proyecto, la visibilidad se mejora mediante la integración de Prisma Cloud como solución de Cloud Security Posture Management (CSPM), junto con flujos de automatización que recogen eventos y desviaciones, y los representan mediante paneles visuales en Power BI. Esto no solo permite actuar ante riesgos en tiempo real, sino que habilita la auditoría continua y la trazabilidad de las decisiones tomadas.

3. Material y desarrollo del proyecto

Este capítulo detalla los aspectos técnicos y metodológicos relacionados con el desarrollo de la solución propuesta para la gestión automatizada de desviaciones de seguridad en entornos Cloud. Se abordan tanto los elementos previos que definen el contexto del proyecto como el diseño funcional, la implementación de flujos automatizados, las herramientas utilizadas y el proceso de validación.

Para comprender el alcance y la motivación detrás de la solución, es fundamental analizar primero la situación de partida y las limitaciones detectadas en los procedimientos actuales de supervisión y gestión de desviaciones. Este análisis inicial sienta las bases sobre las que se construyó la propuesta de automatización.

3.1. Escenario previo

La gestión de desviaciones es un proceso crítico para garantizar el cumplimiento de políticas y la identificación proactiva de riesgos en los entornos Cloud, asegurando así la protección de los activos.

En el entorno multicloud sobre el que se ha desarrollado este proyecto, se emplean herramientas como Prisma Cloud para analizar la postura de seguridad, alineadas con la versión correspondiente de los CISs adaptada a cada CSP. Cuando Prisma Cloud no ofrece cobertura completa sobre una recomendación de seguridad, se recurre a los Cloud Security Posture Management (CSPM)s nativos del proveedor, como AWS Security Hub [34] o Microsoft Defender for Cloud [35], mediante la ejecución periódica de scripts o validaciones manuales.

Actualmente, la gestión de desviaciones derivadas de los controles de Prisma Cloud se realiza mediante un enfoque manual y descentralizado, lo que implica una alta carga de trabajo operativo y escasa trazabilidad.

El proceso actual se detalla a continuación junto con sus principales limitaciones:

- **Extracción manual de datos.** Los informes CSV de Prisma Cloud se extraen manualmente, lo que expone el proceso a errores humanos y retrasa las actualizaciones del estado de los controles.
- **Análisis manual.** Los archivos son analizados manualmente con hojas de cálculo, donde se filtran por política, cuenta y recurso. Este proceso consume tiempo y dificulta el seguimiento continuo.
- **Actualización en Confluence.** Tras el análisis, el estado de cada desviación se actualiza manualmente en Confluence, lo cual representa una tarea tediosa con riesgo de inconsistencias.
- **Reuniones sin seguimiento formal.** Las desviaciones se revisan semanalmente con los equipos técnicos, pero las decisiones se toman de forma verbal y sin plazos definidos, dificultando la trazabilidad y la resolución efectiva.
- **Documentación fragmentada.** Los acuerdos y observaciones de las reuniones se registran de forma breve en Confluence, sin una sistematización clara del avance ni del estado de las desviaciones.

Este escenario evidenció la necesidad de establecer un sistema automatizado, centralizado y auditable que permita optimizar la gestión de desviaciones, facilitar el análisis de cumplimiento y mejorar la capacidad de respuesta ante riesgos de seguridad.

3.1.1. Definición formal de la gestión de desviaciones

En el contexto de este proyecto, la gestión de desviaciones hace referencia al proceso de control, revisión y seguimiento de los hallazgos de seguridad generados por herramientas Cloud Security Posture Management (CSPM) como Prisma Cloud.

Prisma Cloud clasifica cada desviación a través de distintos campos que permiten realizar su seguimiento técnico y funcional:

- **Estado (*Status*):** determina el ciclo de vida de la desviación. Los estados más habituales son:
  - *Open* – la desviación está activa y pendiente de análisis o resolución.
  - *Dismissed* – se ha descartado manualmente por considerarse justificada o no aplicable.

  - *Resolved* – la desviación ha sido corregida tras aplicar una acción técnica o correctiva.
  - *Snoozed* – la alerta ha sido pospuesta temporalmente y no será notificada durante un periodo definido.

- **Política (*Policy*):** especifica el control de seguridad violado, como "Storage bucket publicly accessible" o "IAM user has admin privileges".
- **Severidad (*Severity*):** indica la criticidad de la desviación, clasificada como `Low`, `Medium`, `High` o `Critical`, en función del impacto potencial sobre la seguridad.
- **Cuenta (*Cloud Account*):** identifica la suscripción, proyecto o tenant en el que se ha generado el hallazgo.
- **Recurso afectado (*Resource*):** proporciona el nombre, tipo y ubicación del recurso comprometido.
- **Primera detección y última aparición:** fechas que permiten distinguir si la desviación es nueva o persistente en el tiempo.
- **Etiquetas y comentarios:** campos auxiliares utilizados por los equipos para añadir observaciones, responsables o decisiones relacionadas con el tratamiento del hallazgo.

Además del análisis individual de cada hallazgo, se realiza una categorización funcional avanzada para facilitar su priorización y trazabilidad. Esta clasificación organiza las desviaciones según los siguientes criterios:

- **Proveedor cloud:** identificación del entorno donde se produce la desviación (e.g., AWS, Azure, GCP).
- **Categoría del control:** taxonomía asociada a la familia del control violado, como redes, gestión de identidades, cifrado, almacenamiento o gestión de logs.
- **Estado funcional:** condición actual del hallazgo a efectos de su gestión, como "activa", "justificada", "recurrente" o "pendiente de validación".
- **Nivel de criticidad:** evaluación del impacto técnico y organizativo potencial, basada en la severidad asignada por Prisma Cloud y criterios internos de riesgo.

En la Tabla 3.1 podemos ver los campos elegidos por Prisma Cloud para la descripción de una desviación de seguridad.

Campo	Descripción
Cloud Type	Tipo de proveedor cloud donde se detecta la desviación (como AWS, Azure, GCP). Permite segmentar el análisis por entorno.
Account Name / ID	Identificador de la cuenta o suscripción donde reside el recurso afectado. Ayuda a ubicar el contexto técnico y organizativo.
Policy Name	Nombre de la política violada. Define qué control se evalúa (por ejemplo, accesibilidad pública de almacenamiento).
Policy Category	Familia de control (Identidad, Red, Monitorización, etc.) que facilita la clasificación temática de los hallazgos.
Resource ID / Name	Identificador o nombre del recurso afectado, como una máquina virtual, bucket o base de datos.
Severity	Nivel de criticidad asignado (Crítica, Alta, Media, Baja), útil para priorizar las acciones.
Status	Estado actual del hallazgo: *Open*, *Resolved*, *Suppressed*, *Dismissed*.
First Seen	Fecha en que se detectó por primera vez el hallazgo. Ayuda a identificar desviaciones persistentes.
Last Seen	Última fecha en que el hallazgo estuvo presente. Sirve para evaluar la vigencia.
Remediation	Recomendación técnica proporcionada por Prisma Cloud para corregir la desviación.
Justification	Explicación documentada en casos donde no se resuelve el hallazgo por decisión técnica o de negocio.

Tabla 3.1. Campos principales asociados a una desviación de seguridad en Prisma Cloud.

La extracción de esta información se realiza de forma manual mediante la descarga periódica de informes en formato `.csv` desde la consola de Prisma Cloud. Posteriormente, los datos se procesan y analizan con hojas de cálculo o herramientas de inteligencia de negocio como Power BI, que permiten consolidar múltiples dimensiones de análisis.

3.2. Herramientas y tecnologías utilizadas

Durante el desarrollo de la solución, se han empleado diversas herramientas tecnológicas que permiten automatizar, centralizar y visualizar el proceso de gestión de desviaciones de seguridad en entornos Cloud. Estas herramientas han sido seleccionadas por su integración con servicios empresariales, su capacidad de automatización y su flexibilidad para adaptarse a las necesidades específicas del flujo diseñado.

3.2.1. Prisma Cloud

Prisma Cloud actúa como componente central de supervisión de la postura de seguridad en la nube. Esta plataforma de Cloud Security Posture Management (CSPM) ofrece capacidades avanzadas de análisis y detección de desviaciones, evaluando la configuración de los recursos desplegados en entornos IaaSs. En el proyecto, Prisma Cloud es la fuente principal de datos sobre hallazgos de seguridad, que se extraen manualmente o mediante su API en formato `.csv`, permitiendo así alimentar el flujo de trabajo con información técnica estructurada. Gracias a su integración con marcos de referencia como CIS, se garantiza el alineamiento con estándares de seguridad ampliamente reconocidos.

3.2.2. Power Automate

Power Automate se ha empleado para automatizar múltiples etapas del flujo de trabajo. Esta herramienta permite crear procesos desencadenados por eventos, como la creación o modificación de registros en SharePoint. En el contexto del proyecto, Power Automate se encarga de tareas como:

- La ingestión automática de desviaciones exportadas desde Prisma Cloud.
- La asignación de responsables técnicos en función del tipo de desviación.
- La generación de correos o tickets (Sistema de Atención de Incidencias (SAI)) personalizados.
- La preparación de datos para su visualización en Power BI.

3.2.3. SharePoint

SharePoint se ha utilizado como repositorio centralizado para almacenar las desviaciones extraídas desde Prisma Cloud. Se han definido listas específicas con una estructura basada en los campos técnicos detallados previamente, lo que permite organizar y filtrar la información de forma eficiente. SharePoint también facilita la colaboración entre equipos al permitir el acceso compartido y controlado a los datos, así como el seguimiento de versiones y modificaciones sobre los registros. Su integración nativa con otras herramientas de Microsoft resulta clave para automatizar procesos y garantizar la trazabilidad de las desviaciones.

3.2.4. Outlook

Outlook ha sido la herramienta empleada para la comunicación automatizada dentro del flujo de trabajo. A través del conector integrado en Power Automate, se ha configurado el envío de correos electrónicos técnicos dirigidos a los responsables de cada desviación.

Estos correos contienen información clave generada a lo largo del flujo, incluyendo la descripción del hallazgo, el análisis técnico de riesgo, las recomendaciones de remediación y las referencias a controles de seguridad violados. Gracias a esta integración, se logra una notificación inmediata y trazable de las acciones requeridas, evitando retrasos en la respuesta ante hallazgos críticos.

Además, la capacidad de personalización del mensaje y el uso dinámico de variables en Power Automate permiten adaptar el contenido del correo según el tipo de desviación, la criticidad y el destinatario, manteniendo una comunicación clara, profesional y contextualizada.

3.2.5. Power BI

Power BI ha sido la herramienta utilizada para la visualización de los datos procesados a lo largo del flujo de trabajo. Mediante su integración con el flujo, se han creado modelos que permiten representar de forma dinámica y comprensible el estado y evolución de las ejecuciones del flujo.

Gracias a su capacidad de actualización periódica y conexión directa con las listas estructuradas de SharePoint, Power BI garantiza una visibilidad en tiempo real.

3.3. Diseño de la solución

Una vez identificado el escenario de partida y las carencias del proceso actual, se procede al diseño de una solución que permita optimizar la gestión de desviaciones de seguridad en entornos cloud.

El diseño se apoya en herramientas ampliamente adoptadas en entornos corporativos y sigue principios de modularidad, escalabilidad y automatización. Para estructurar este diseño, se definen a continuación los objetivos clave que deben guiar su desarrollo.

3.3.1. Objetivos de diseño

El objetivo principal del diseño es transformar el proceso manual de gestión de desviaciones en una solución automatizada, estructurada y escalable, que reduzca la carga operativa, elimine errores humanos y mejore la visibilidad de la postura de seguridad en entornos multicloud.

Para ello, la solución busca:

- Automatizar la ingesta y clasificación de desviaciones desde distintas fuentes (Prisma Cloud, SEGCLD, inputs manuales).
- Centralizar el almacenamiento y trazabilidad de las desviaciones en un repositorio accesible (SharePoint).
- Implementar flujos automáticos de análisis, asignación, seguimiento y validación mediante Power Automate.
- Ofrecer visualizaciones dinámicas en Power BI que permitan analizar desviaciones por proveedor, criticidad, estado o responsable.
- Integrar mecanismos de retroalimentación y mejora continua.

3.3.2. Arquitectura general de la solución

La arquitectura propuesta está basada en una serie de componentes conectados entre sí mediante flujos automatizados y acceso mediante APIs. A nivel funcional, la solución está compuesta por:

- **Fuentes de desviaciones.** Prisma Cloud (como principal Cloud Security Posture Management (CSPM)), herramientas internas como SEGCLD, y entradas manuales puntuales.
- **Motor de automatización.** Power Automate, encargado de orquestar el flujo de clasificación, asignación, control de estado y actualización.
- **Repositorio de datos.** Listas estructuradas en SharePoint, que almacenan todas las desviaciones, campos técnicos asociados, trazabilidad de acciones y responsables.
- **Visualización e informes.** Power BI, que se conecta al repositorio y genera paneles interactivos para seguimiento y análisis.
- **Comunicación.** Notificaciones a responsables mediante Microsoft Teams o correo, según la criticidad o los cambios de estado.

3.3.3. Modelo de datos y trazabilidad

Cada desviación almacenada en SharePoint contiene los siguientes campos técnicos, definidos previamente en la Tabla 3.1, entre los que se incluyen: identificador, proveedor, criticidad, estado, responsable y otros metadatos. Este modelo permite establecer relaciones entre desviaciones, priorizarlas, asignar responsables y aplicar filtros dinámicos.

La trazabilidad está garantizada mediante los registros automáticos de cambios, fechas de creación/modificación y el control de versiones que proporciona la plataforma.

3.3.4. Flujo de trabajo actual

El flujo mostrado en la Figura 3.1, compuesto por las siguientes etapas, representa la operativa actual que se lleva con las desviaciones:

- **Ingesta.** Recolección automatizada o manual de desviaciones. Prisma Cloud actúa como fuente principal, mediante exportación de datos en formato `.csv` o mediante la API, alineándose con la estructura empleada en los informes de *KPI* y de seguimiento.
- **Registro.** Los datos recopilados se almacenan tanto en hojas de cálculo como en la base de datos de SEGCLD, donde se normalizan e integran con metadatos clave como estado, proveedor o criticidad.
- **Clasificación.** Las desviaciones se categorizan según su **severidad**, número de ocurrencias y simplicidad de resolución. Esta clasificación permite priorizar el tratamiento y se realiza mediante reglas automáticas y entradas manuales cuando es necesario.
- **Asignación.** En paralelo a la clasificación, un sistema basado en inteligencia artificial genera correos o SAIs dirigidos automáticamente al responsable técnico correspondiente en función de la naturaleza de la desviación, agilizando el proceso de asignación.
- **Análisis y excepción.** Cada desviación es evaluada por los equipos responsables. Puede clasificarse como:
  - *Falso Positivo.* Se gestiona y reporta, documentando la causa para evitar reincidencias mediante medidas preventivas.
  - *Excepción:* Puede estar aprobada por otro equipo (lo que conlleva su cierre y reporte) o rechazada, en cuyo caso se considera como una desviación real.
  - *Desviación real.* Requiere la creación de una solicitud de remediación con ayuda de la IA para ser enviado al equipo técnico correspondiente. Se asigna un Service Level Agreement (SLA) (30/90/120 días) en función de la criticidad.
- **Remediación y validación.** Transcurrido el plazo establecido, se verifica si la remediación ha sido implementada correctamente. En caso afirmativo, se cierra la desviación; de lo contrario, se retrocede al paso anterior para continuar con el seguimiento y se escala al comité de riesgos de la empresa u organización.
- **Cierre y reporte.** Una vez validada o justificada la desviación, esta se cierra y pasa al informe de seguimiento. La información se integra en Power BI para visualización y análisis.
- **Mejora continua.** El reporte final no solo permite documentar y comunicar el estado actual, sino que también aporta retroalimentación al sistema, facilitando la

optimización de flujos, ajustes de umbrales y reasignación de responsables cuando sea necesario.

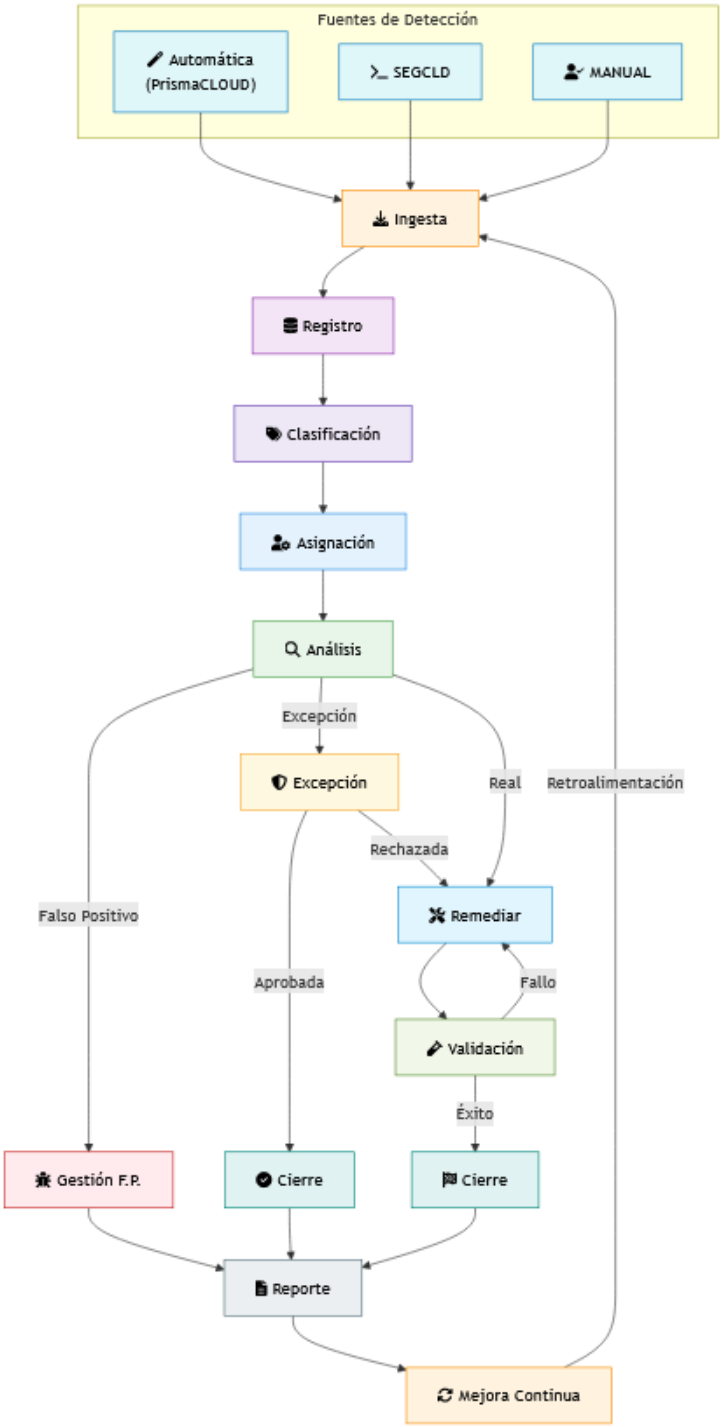


Figura 3.1. Flujo Principal de una Desviación.

3.3.5. Integración entre componentes

La solución conecta los distintos sistemas mediante conectores nativos de Power Platform, que interactúan con APIs públicas. Por ejemplo:

- Power Automate: automatización de procesos y generación de alertas.
- SharePoint: almacenamiento estructurado y permisos controlados.
- Outlook: envío de correos generados automáticamente.

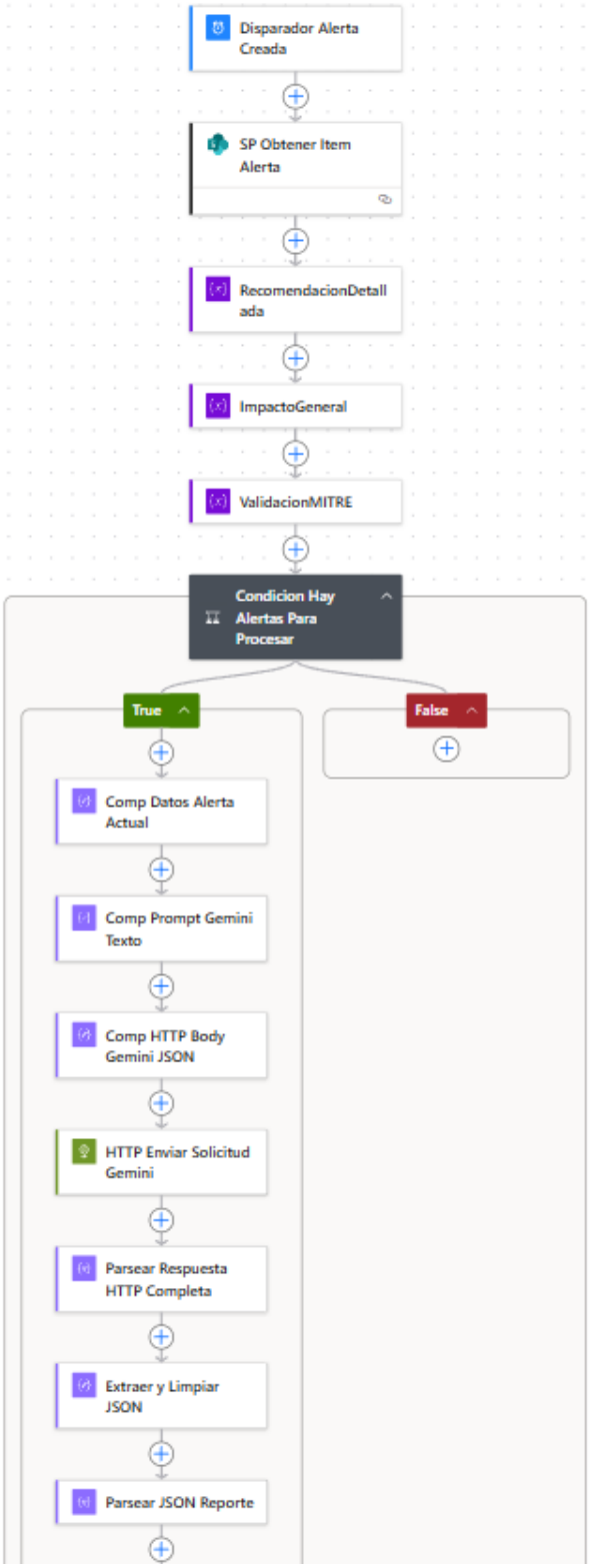
3.4. Desarrollo e implementación

Esta sección describe el proceso completo seguido para llevar a cabo el desarrollo de la solución propuesta.

3.4.1. Flujo principal

En la Figura 3.2 podemos observar el flujo completo desarrollado en Power Automate de las desviaciones, que contempla desde la detección de alertas asociadas a las desviaciones hasta la notificación a los equipos responsables.

Este flujo se ejecuta diariamente a primera hora y tiene como objetivo la detección de los cambios de estado de las desviaciones. Una vez identificados, actualiza la base de datos con los nuevos valores y envía la notificación al equipo responsable de la desviación.


Disparador Alerta Creada
SP Obtener Item Alerta
RecomendacionDetallada
ImpactoGeneral
ValidacionMITRE
Condicion Hay Alertas Para Procesar
True
False
Comp Datos Alerta Actual
Comp Prompt Gemini Texto
Comp HTTP Body Gemini JSON
HTTP Enviar Solicitud Gemini
Parsear Respuesta HTTP Completa
Extraer y Limpiar JSON
Parsear JSON Reporte

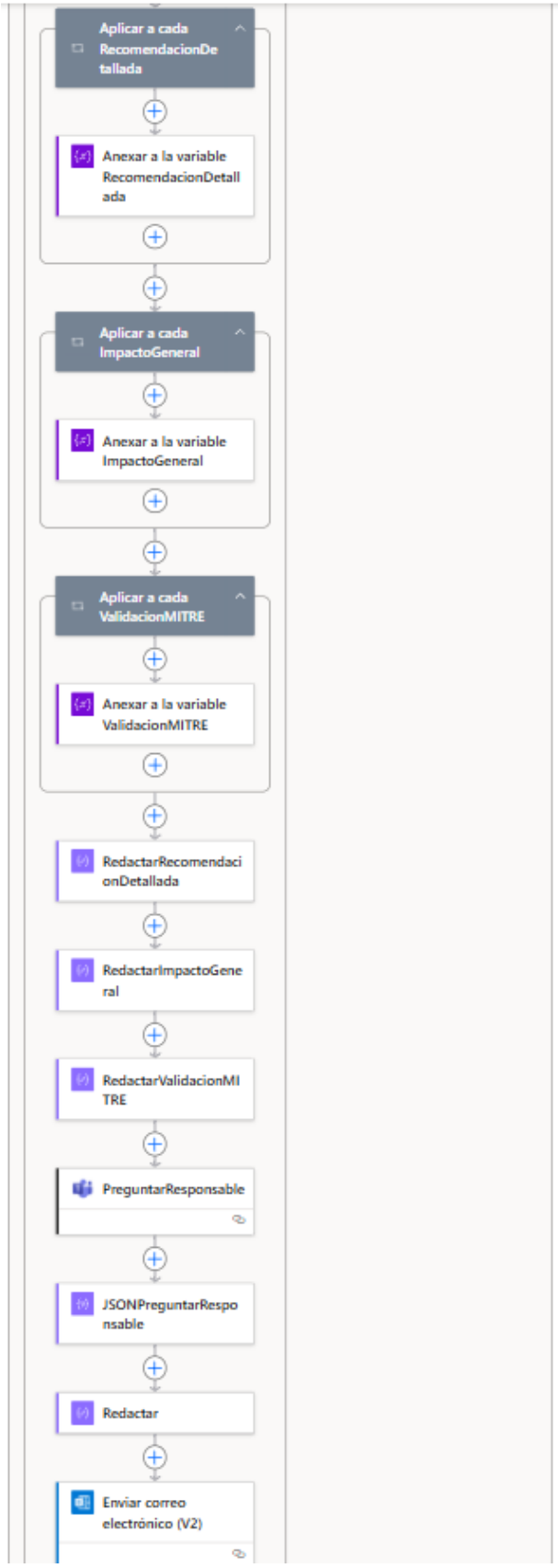


Figura 3.2. Flujo Principal desarrollado.

1. Inicialización del flujo

El flujo se inicia mediante un disparador manual o programado (*Scheduled Trigger*) que permite ejecutar el proceso de forma controlada. En este primer paso, el sistema realiza una solicitud a la API de SharePoint con el objetivo de obtener la lista de desviaciones existentes registradas en la plataforma. En la Figura 3.3 podemos ver la organización que deberían tener todas las tablas de desviaciones.

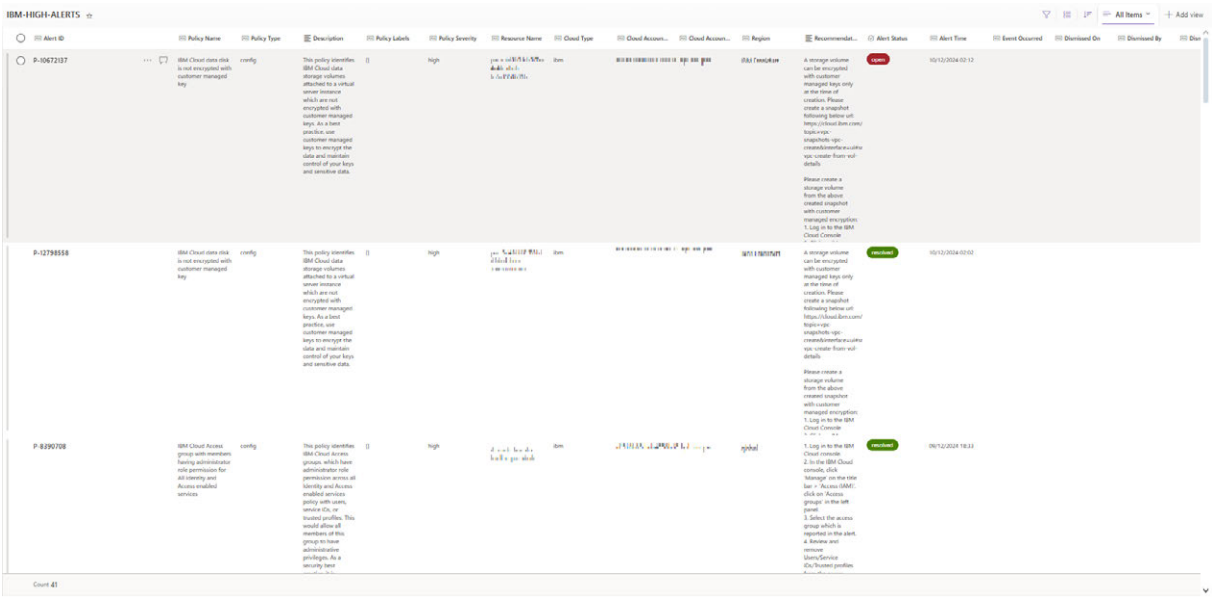


Figura 3.3. Lista de básica de organización de desviaciones.

Para ello, como podemos ver en la Figura 3.4, se emplea el conector oficial de SharePoint disponible en Power Automate. La llamada se realiza sobre una lista específica (en este caso sobre la lista de IBM-HIGH-ALERTS) donde se almacena el histórico de desviaciones, aplicando filtros (*field_12 eq 'open'*) para recuperar únicamente aquellas que están activas y aún pendientes de tratamiento.

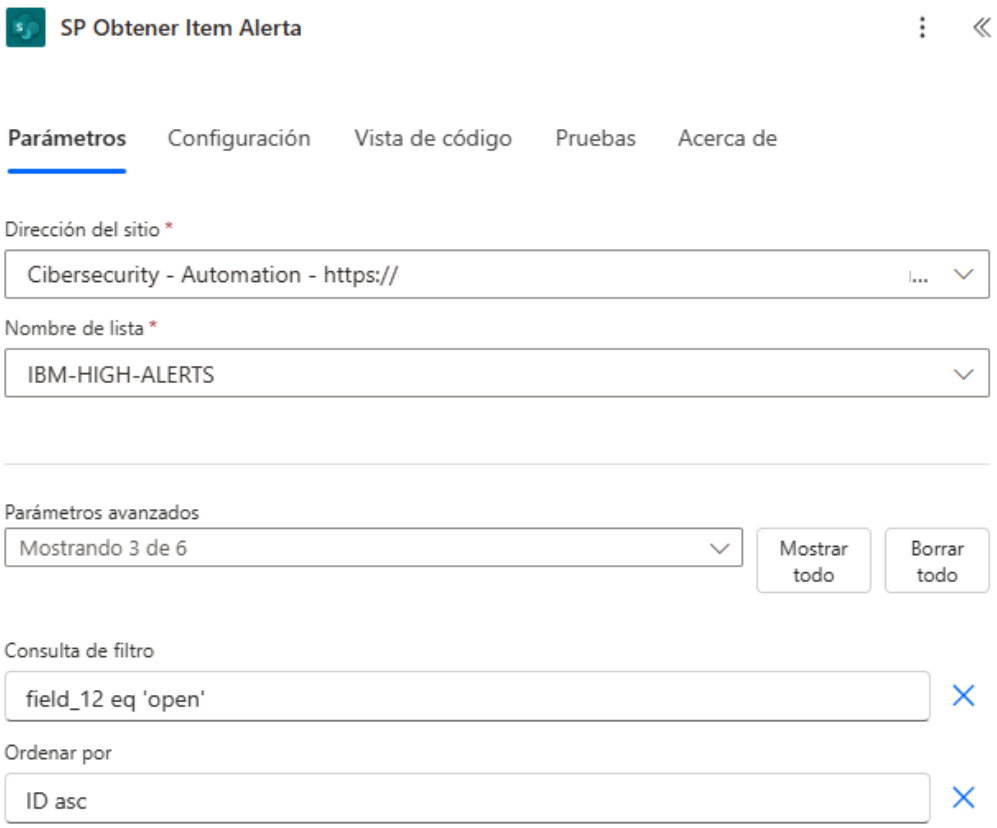


Figura 3.4. Obtención de alertas de SharePoint.

Los datos recuperados se almacenan en una variable estructurada en memoria que se utilizará a lo largo del flujo para comparar, actualizar o enriquecer información según el estado actual de cada desviación.

2. Creación de variables

Tras la obtención de datos desde SharePoint, el flujo procede a declarar e inicializar un conjunto de variables globales que nos servirán desde el punto de vista del diseño funcional, y que se utilizarán a lo largo de la ejecución para almacenar temporalmente información crítica derivada del análisis automatizado.

En concreto, se definen las siguientes variables, todas de tipo `String`:

- **RecomendacionDetallada**: utilizada para almacenar una descripción técnica enriquecida sobre la remediación de la desviación detectada, generada posterior-

mente por el modelo de IA.

- **ImpactoGeneral**: recoge un resumen textual del impacto que tendría la desviación si no es corregida, considerando aspectos como el tipo de control afectado, criticidad y entorno.
- **ValidacionMITRE**: variable donde se almacena una referencia cruzada con la matriz MITRE (si aplica), indicando la técnica o táctica que se vería facilitada por la desviación.

Estas variables permanecen disponibles a lo largo de todo el flujo, permitiendo que sus valores sean definidos o sobrescritos dinámicamente a medida que se procesan los datos extraídos y se generan respuestas desde el Modelo de lenguaje grande (LLM).

3. Comprobación de existencia de alertas

Antes de procesar datos, se comprueba si existen alertas nuevas o alertas reabiertas después del período de excepcionado. Si no se detectan entradas nuevas, el flujo se detiene automáticamente para optimizar recursos.

Una vez recuperadas las desviaciones almacenadas en la lista de SharePoint, el flujo procede a iterar sobre cada elemento para comprobar si es necesario procesarlo. Esta verificación inicial permite optimizar el rendimiento del flujo y evitar operaciones redundantes sobre elementos que ya han sido tratados previamente.

La lógica de comprobación evalúa principalmente los siguientes criterios:

- El estado de la desviación no debe ser “Resuelta”, “Falso positivo” ni “Excepción aceptada”, solo ”Open”.
- La desviación no puede estar duplicada respecto a otra ya analizada ya que cada alerta tiene un identificador único y no cambia si se encuentra en la situación de reapertura.
- Debe contar con los campos mínimos requeridos: severidad, proveedor y nombre del control.

Este paso es clave para asegurar que la ejecución del flujo se limita exclusivamente a desviaciones activas, mejorando la eficiencia operativa y reduciendo la carga innecesaria sobre los conectores y recursos externos.

4. Composición de datos de alerta actual

Se selecciona y estructura la información relevante de la alerta o desviación actual y se agrupan en variables para su uso posterior.

Variables principales estructuradas

- **ID_alerta**
- **Nombre de la politica**
- **Tipo de politica**
- **Descripcion problema (original)**
- **Severidad**
- **Nombre del recurso**
- **Tipo de nube**
- **Region**
- **Recomendacion original (Prisma Cloud)**
- **Fecha de la alerta**

Estandarizar y estructurar la información de la desviación nos facilitará su uso en las siguientes fases, como la elaboración del prompt para Gemini o la construcción del mensaje de notificación.

5. Composición de prompt para Gemini

Se ha construido un texto en lenguaje natural que servirá como entrada para el modelo de lenguaje Gemini. En este prompt, se le proporciona a la IA los datos de la alerta a analizar como vemos en la Figura 3.5 y se solicita por salida un JSON puro sin texto adicional con una serie de claves como las siguientes:

- **"RiesgoResumen"**: resumen ejecutivo que sintetiza el riesgo principal, incluyendo amenaza, vulnerabilidad y posible impacto inmediato.

- **"AnalisisRiesgoEstructurado"**: objeto anidado con las claves:
  - **"Amenaza"**: tipo de actor o evento potencial que podría explotar la desviación.
  - **"Vulnerabilidad"**: debilidad técnica exacta que permite la desviación.
  - **"Probabilidad"**: evaluación cualitativa de explotación (Alta, Media o Baja) con justificación técnica.
  - **"ImpactoConfidencialidad"**: consecuencias si se vulnera la confidencialidad de los datos.
  - **"ImpactoIntegridad"**: consecuencias sobre la integridad de la información o sistemas.
  - **"ImpactoDisponibilidad"**: consecuencias si se compromete la disponibilidad del recurso.
- **"ControlCISViolado"**: referencia al control de seguridad del estándar CIS que se incumple, con justificación.
- **"RecomendacionDetallada"**: array de pasos técnicos claros y ejecutables para mitigar la desviación, incluyendo comandos, rutas o configuraciones.
- **"ImpactoGeneral"**: array que enumera consecuencias más amplias, cada una categorizada como *Operativo*, *Financiero*, *Cumplimiento* o *Reputación*, seguido de una explicación profesional.
- **"ValidacionMITRE"**: array de técnicas MITRE ATT&CK (`T-ID`) que se relacionan con la desviación, si las hay.
- **"DescripcionOriginal_ES"**: traducción precisa al español de la descripción técnica original de la alerta.
- **"RecomendacionOriginal_ES"**: traducción fiel al español de la recomendación de Prisma Cloud.

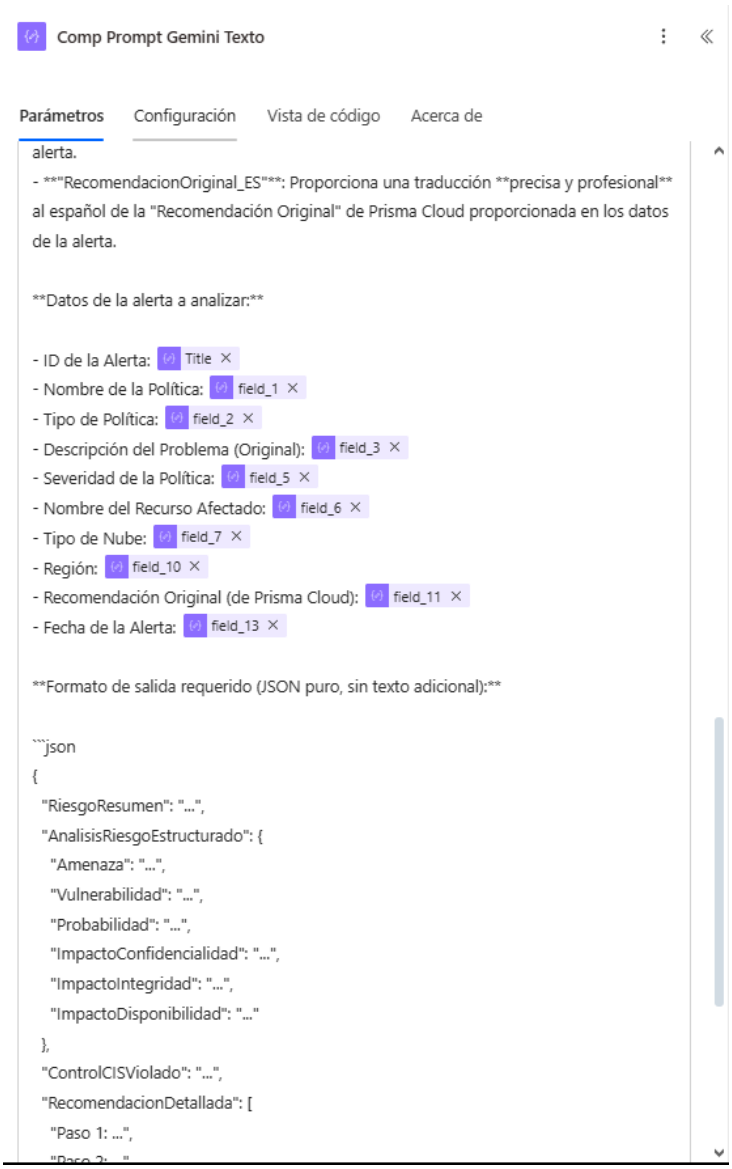


Figura 3.5. Composición del prompt de Gemini.

Este diseño de prompt garantiza uniformidad en las respuestas, facilita su parseo automático y asegura que el análisis generado sea reutilizable, auditable y trazable dentro del flujo automatizado.

6. Composición del cuerpo HTTP (JSON) para Gemini

A partir del texto generado en el paso anterior, se construye el cuerpo de la solicitud HTTP en formato `JSON`, que será enviado al endpoint del modelo Gemini.

El objeto JSON contiene las siguientes claves:

- **"temperature"**= 0.6. Parámetro de control de aleatoriedad.
- **"maxOutputTokens"**= (1500,2000). Número máximo de tokens permitidos en la respuesta.
- **"text"**: incluye el `prompt` generado en el paso anterior.

Este cuerpo está preparado para su envío posterior mediante una acción HTTP POST.

7. Envío de solicitud HTTP a Gemini

Una vez compuesto el cuerpo de la solicitud en formato `JSON`, el flujo procede a realizar la llamada al modelo Gemini-2.0-flash como podemos ver en la Figura 3.6 mediante una acción HTTP configurada con los siguientes elementos:

- **Método:** `POST`
- **Encabezados:**
  - `Content-Type: application/json`
- **body:** el objeto `JSON` generado en el paso anterior, que contiene la alerta de seguridad y el prompt con las instrucciones detalladas para el análisis.

La respuesta esperada de Gemini es un objeto `JSON` estructurado que contiene las claves definidas en el esquema.

Este paso es fundamental, ya que permite delegar el análisis técnico de la alerta a un LLM especializado, reduciendo la carga analítica del equipo de ciberseguridad y estandarizando la calidad de los informes generados.

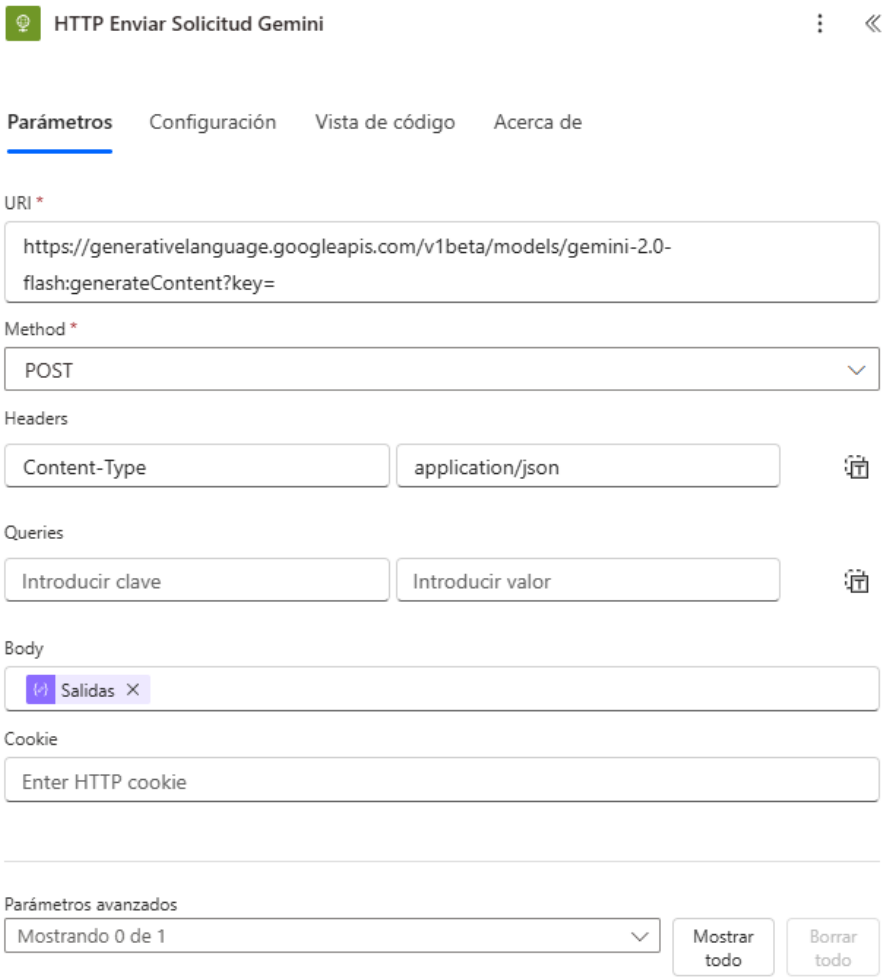


Figura 3.6. Solicitud HTTP Gemini.

8. Parsing y limpieza de la respuesta de Gemini

Una vez enviada la solicitud HTTP al modelo Gemini, se lleva a cabo un proceso en tres etapas para extraer, limpiar y estructurar la información contenida en la respuesta:

1. **Parseo inicial del cuerpo de la respuesta:** se realiza una acción *Parse JSON* sobre el cuerpo de la solicitud para obtener el texto completo generado por el modelo.

2. **Extracción y limpieza del contenido JSON:** mediante una acción `Compose`, se aplica una expresión que localiza el primer carácter "{" y el último "}" del bloque de texto generado. A partir de estos índices, se extrae únicamente el fragmento del texto que representa el objeto JSON, eliminando cualquier contenido adicional no

estructurado que haya sido devuelto por el modelo. También se hace uso de `trim` para asegurar que no queden espacios en blanco alrededor del texto extraído.

3. **Parseo del objeto JSON limpio:** finalmente, se aplica un segundo `Parse JSON` sobre la salida limpia anterior,Figura 3.7, utilizando un esquema predefinido que incluye todas las claves necesarias: `RiesgoResumen`, `AnalisisRiesgoEstructurado`, `ControlCISViolado`, etc... Esto permite acceder a cada uno de estos valores como variables independientes dentro del flujo.

Este enfoque garantiza la integridad del objeto JSON recibido y permite que los pasos posteriores del flujo puedan operar sobre datos estructurados y validados sin riesgo de errores por formato incorrecto.

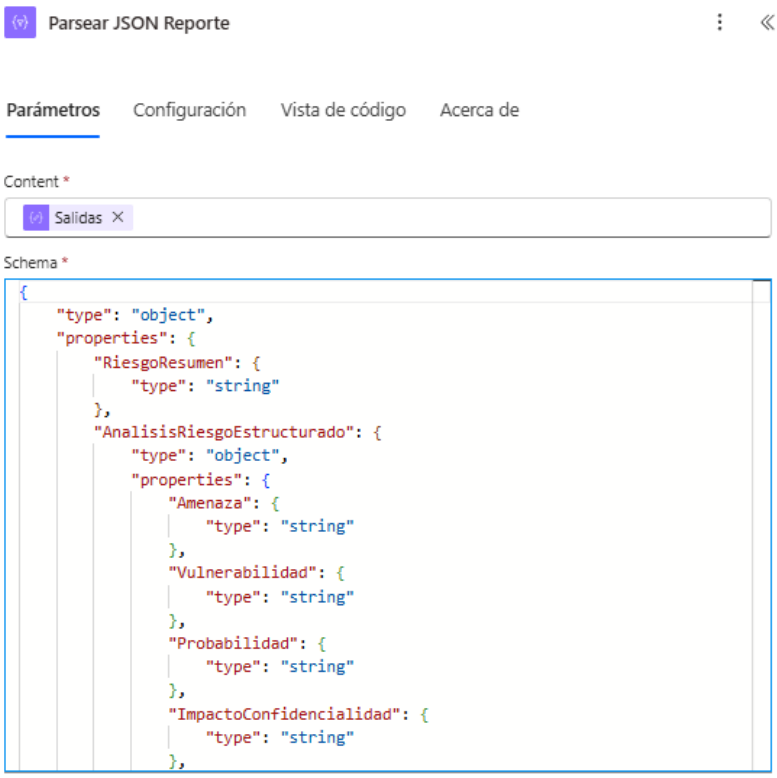


Figura 3.7. Parse del JSON.

9. Anexado y redacción de variables

Una vez parseada correctamente la respuesta generada por Gemini, el flujo procede a anexar a variables individuales los valores de las claves más relevantes del objeto JSON: `RecomendacionDetallada`, `ImpactoGeneral` y `ValidacionMITRE`.

Aunque estos datos ya están presentes dentro del objeto JSON, Power Automate requiere que la información clave para la redacción final se almacene en variables separadas para facilitar su reutilización en pasos posteriores. Al tratarse de contenido que será insertado directamente en mensajes, reportes o registros, resulta más eficiente y seguro acceder a ellos desde variables locales que desde estructuras anidadas de un objeto complejo.

A continuación, el flujo procede a llenar esas variables con el contenido técnico obtenido de las interacciones anteriores. Para ello, se emplean acciones de tipo `Compose`, que permiten ensamblar texto dinámico y coherente con un formato adaptado al destinatario técnico. El resultado es una redacción lista para ser incluida directamente en el mensaje automatizado del siguiente paso.

10. Solicitud de Responsable

En este paso, el flujo automatizado utiliza un conector de Microsoft Teams para enviar una tarjeta adaptativa al canal del equipo de ciberseguridad. Esta tarjeta contiene un resumen de los principales datos técnicos de la desviación detectada, como el ID de alerta, la política afectada, el recurso implicado, la severidad o la región, con el objetivo de facilitar una revisión rápida y contextualizada por parte del equipo técnico.

Además de los campos informativos, y como podemos ver en la Figura 3.8, la tarjeta incluye un campo editable donde se solicita explícitamente a los miembros del equipo que introduzcan el correo electrónico del responsable técnico del recurso afectado. Este valor será utilizado en pasos posteriores del flujo para asignar tareas, generar notificaciones personalizadas y registrar la trazabilidad del tratamiento de la desviación.

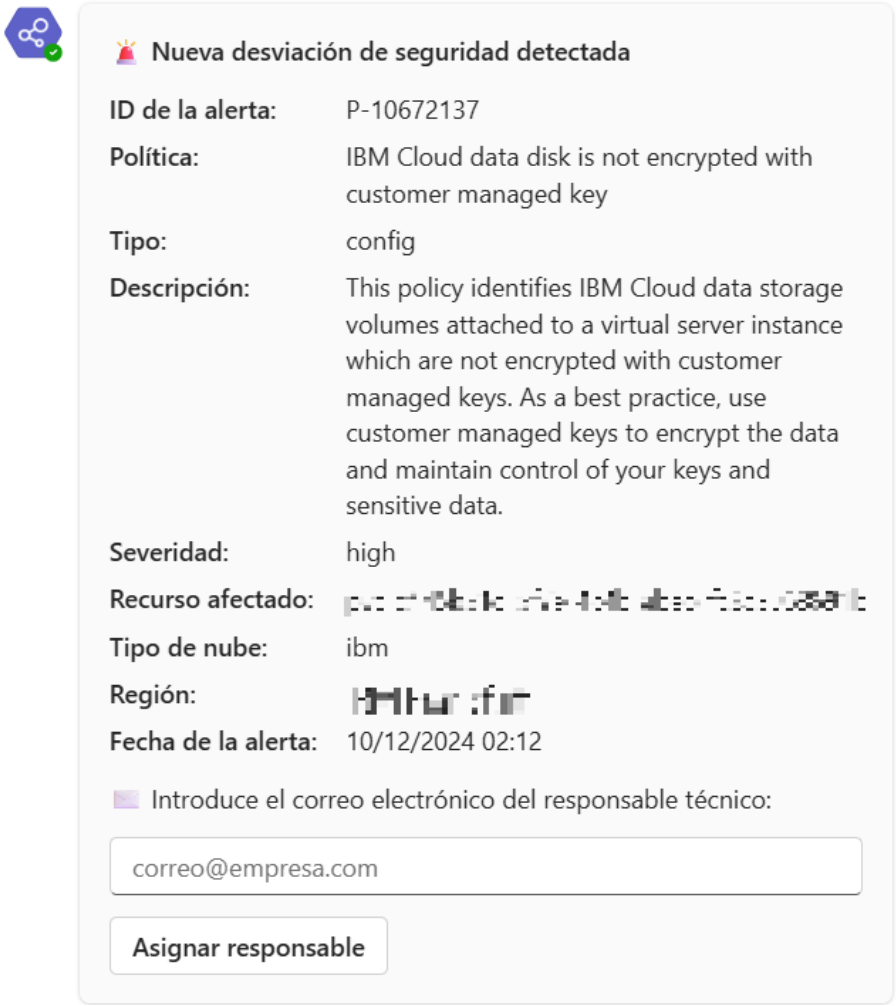


Figura 3.8. Ejemplo de tarjeta recibida por el equipo.

El uso de tarjetas adaptativas permite integrar de forma natural la interacción humana dentro del flujo automatizado, sin necesidad de abandonar la herramienta colaborativa. Una vez enviada la tarjeta, el flujo queda a la espera de la respuesta y extrae la información introducida mediante una operación de análisis `Parse JSON`, asegurando que el campo `responsableCorreo` esté presente y correctamente estructurado para su reutilización posterior.

11. Redacción y envío del correo final

En esta fase final del flujo, se compone un mensaje de correo electrónico técnico que resume de forma estructurada y clara toda la información procesada previamente sobre la desviación detectada. El cuerpo del mensaje incluye los datos clave obtenidos desde

SharePoint, así como el análisis técnico enriquecido generado por la IA y las recomendaciones detalladas para su remediación.

La acción de envío de correo se implementa como se ve en la Figura 3.9 mediante el conector de Outlook en Power Automate, configurando los siguientes elementos:

- **Destinatario:** el responsable técnico asignado a la desviación, determinado en pasos anteriores en función del tipo de control y proveedor.
- **Asunto:** incluye el identificador de la alerta y el nombre.
- **Cuerpo del mensaje:** contiene la redacción técnica que se ha generado, incluyendo la evaluación de riesgo, los controles violados, la validación MITRE ATT&CK y los pasos recomendados para la remediación.

También es posible especificar la importancia del correo que saldría reflejada en Outlook pero, al tener ya la severidad de nuestro control, no nos es necesario.

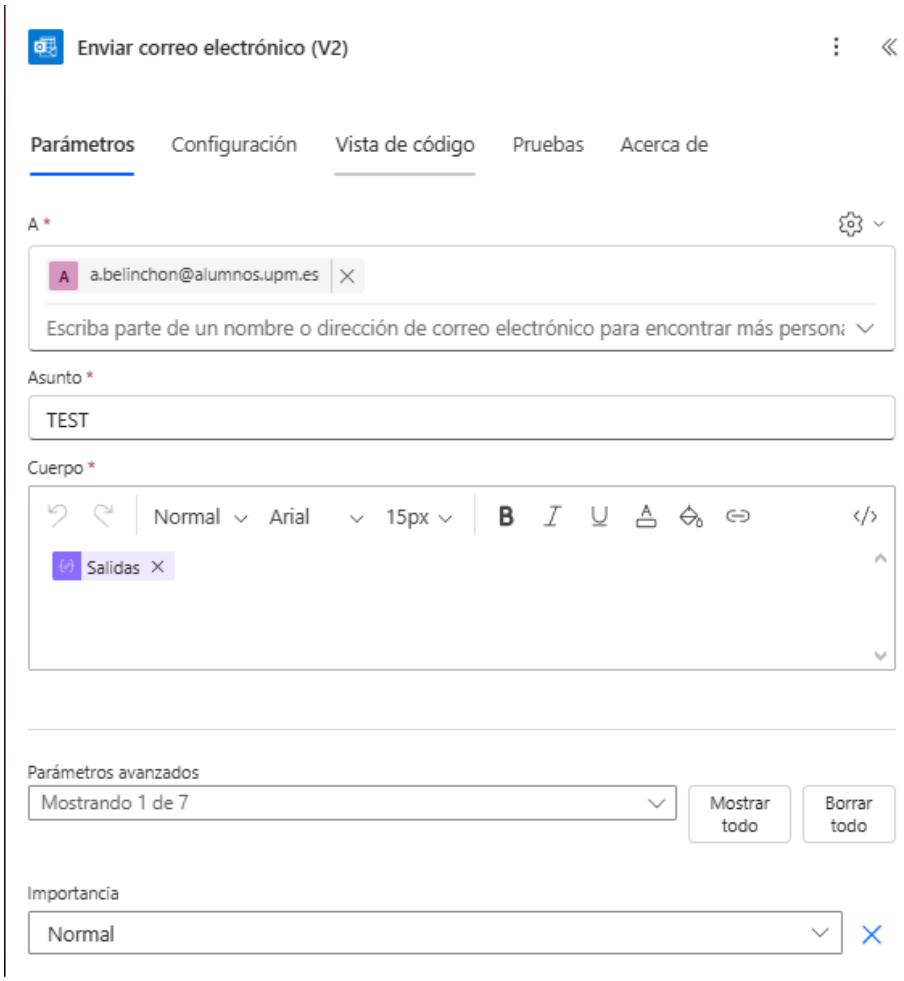


Figura 3.9. Envio de Correo.

Este correo automatizado permite notificar de forma inmediata a los responsables, manteniendo la trazabilidad y acelerando la respuesta ante desviaciones de seguridad críticas.

4. Resultados

Este capítulo presenta los principales resultados obtenidos tras el desarrollo y validación de la solución automatizada para la gestión de desviaciones de seguridad en entornos Cloud. Se evalúa su funcionamiento, eficacia y beneficios observados durante las pruebas en un entorno simulado.

4.1. Evaluación funcional

Durante las pruebas realizadas, se comprobó el correcto funcionamiento del flujo completo, abarcando todas las etapas desde el disparador del flujo y la obtención de las alertas, hasta la comunicación final. En particular, se validaron los siguientes aspectos:

- Registro normalizado y actualizado en listas de SharePoint.
- Generación dinámica de mensajes con análisis enriquecido por LLM.
- Clasificación automática de alertas según criticidad y frecuencia.
- Envío de notificaciones mediante correo electrónico.

4.2. Impacto técnico y operativo

La implementación de la solución ha demostrado una serie de mejoras cuantificables en la operativa de gestión de seguridad:

- **Reducción del tiempo medio de procesamiento:** el tiempo necesario para clasificar y notificar una desviación se ha reducido de horas a minutos.
- **Disminución de errores humanos:** gracias a la automatización, se evita la omisión de registros o errores en la priorización.

- **Mejora de la trazabilidad:** cada paso del flujo queda registrado con fecha, origen y estado, facilitando auditorías y revisiones.
- **Mayor capacidad de respuesta:** los responsables reciben análisis técnicos completos y contextualizados, acelerando la remediación.

4.3. Validación práctica

Los casos de prueba reflejaron una alta estabilidad y precisión en el funcionamiento del sistema. Se verificó su capacidad para:

- Procesar múltiples desviaciones en una sola ejecución.
- Adaptarse a diferentes tipos de alertas y proveedores cloud.
- Recuperarse ante errores puntuales de red o autenticación con reintentos automáticos.
- Registrar correctamente todos los eventos y resultados.

En la Figura 4.1 se muestra una evidencia del correcto envío automatizado de correos electrónicos durante una de las ejecuciones programadas del flujo. Estos mensajes fueron generados por el sistema tras procesar las desviaciones, e incluían toda la información técnica relevante, permitiendo validar la correcta integración con Outlook y la generación dinámica del contenido.

Reporte de Análisis de Desviación de Seguridad

Detalles de la Alerta Original

SEVERIDAD: HIGH

Identificador de Alerta:
P-10672137

Fecha de Registro:
10/12/2024 02:12

Política Aplicada:
IBM Cloud data disk is not encrypted with customer managed key

Tipo de Política:
config

Plataforma Cloud:
ibm

Región/Ubicación:

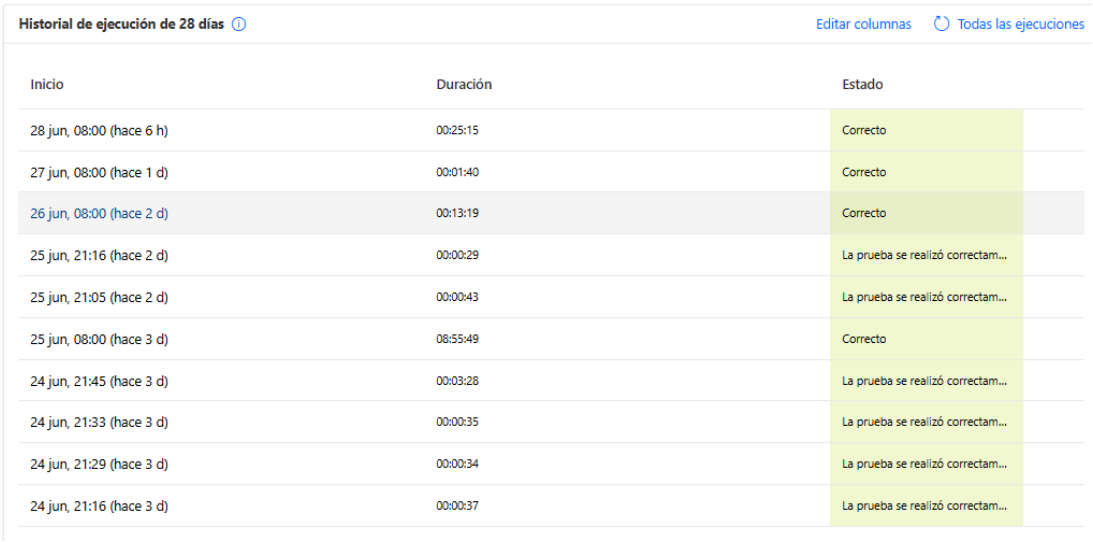
Recurso Afectado:

Descripción del Incidente (Original):
Esta política identifica los volúmenes de almacenamiento de datos de IBM Cloud conectados a una instancia de servidor virtual que no están encriptados con claves gestionadas por el cliente. Como práctica recomendada, utilice claves gestionadas por el cliente para encriptar los datos y mantener el control de sus claves y datos sensibles.

Recomendación Inicial (Plataforma de Seguridad):
Un volumen de almacenamiento solo se puede encriptar con claves gestionadas por el cliente en el momento de la creación. Por favor, cree una instantánea siguiendo la siguiente URL: https://cloud.ibm.com/docs/vpc?topic=vpc-snapshots-vpc-create&interface=ui#snapshots-vpc-create-from-vol-details Por favor, cree un volumen de almacenamiento a partir de la instantánea creada anteriormente con encriptación gestionada por el cliente: 1. Inicie

Figura 4.1. Test de correos.

Asimismo, en la Figura 4.2 se presenta una captura que demuestra la ejecución periódica del flujo, donde puede observarse su funcionamiento constante a lo largo de los días (8:00 am) y algunas pruebas manuales realizadas. Podemos observar que las distintas ejecuciones programadas y pruebas presentan tiempos de ejecución muy dispares. Esta variabilidad se debe principalmente al paso del flujo en el que se solicita la intervención del ingeniero de seguridad, quien debe proporcionar información adicional respecto al responsable del recurso afectado. Al tratarse de una tarea manual que depende de la disponibilidad y coordinación entre distintos equipos, este punto introduce una incertidumbre significativa en los tiempos de respuesta globales.



Historial de ejecución de 28 días ⓘ

Editar columnas | Todas las ejecuciones

Inicio	Duración	Estado
28 jun, 08:00 (hace 6 h)	00:25:15	Correcto
27 jun, 08:00 (hace 1 d)	00:01:40	Correcto
26 jun, 08:00 (hace 2 d)	00:13:19	Correcto
25 jun, 21:16 (hace 2 d)	00:00:29	La prueba se realizó correctam...
25 jun, 21:05 (hace 2 d)	00:00:43	La prueba se realizó correctam...
25 jun, 08:00 (hace 3 d)	08:55:49	Correcto
24 jun, 21:45 (hace 3 d)	00:03:28	La prueba se realizó correctam...
24 jun, 21:33 (hace 3 d)	00:00:35	La prueba se realizó correctam...
24 jun, 21:29 (hace 3 d)	00:00:34	La prueba se realizó correctam...
24 jun, 21:16 (hace 3 d)	00:00:37	La prueba se realizó correctam...

Figura 4.2. Historial de ejecuciones periódicas del flujo automatizado y pruebas.

Por último, la Figura 4.3 muestra parte del panel de seguimiento construido en Power BI, donde se representan métricas clave sobre las ejecuciones del flujo automatizado. Entre los elementos visualizados se incluyen:

- El número total de ejecuciones por día, permitiendo observar la frecuencia de uso y su evolución temporal. Más avanzado en la Sección 6.1.
- Una gráfica de tendencias que distingue entre ejecuciones exitosas, fallidas y canceladas, para destacar los errores y facilitar su resolución. Como podemos ver, los últimos días solo se realizaron las ejecuciones programadas, lo que indica que el flujo funciona correctamente.
- Una distribución porcentual que refleja la proporción de ejecuciones según su resultado.

Estas visualizaciones evidencian tanto la estabilidad general del sistema como los puntos críticos en los que pueden producirse fallos, lo que facilita su depuración y mejora continua.

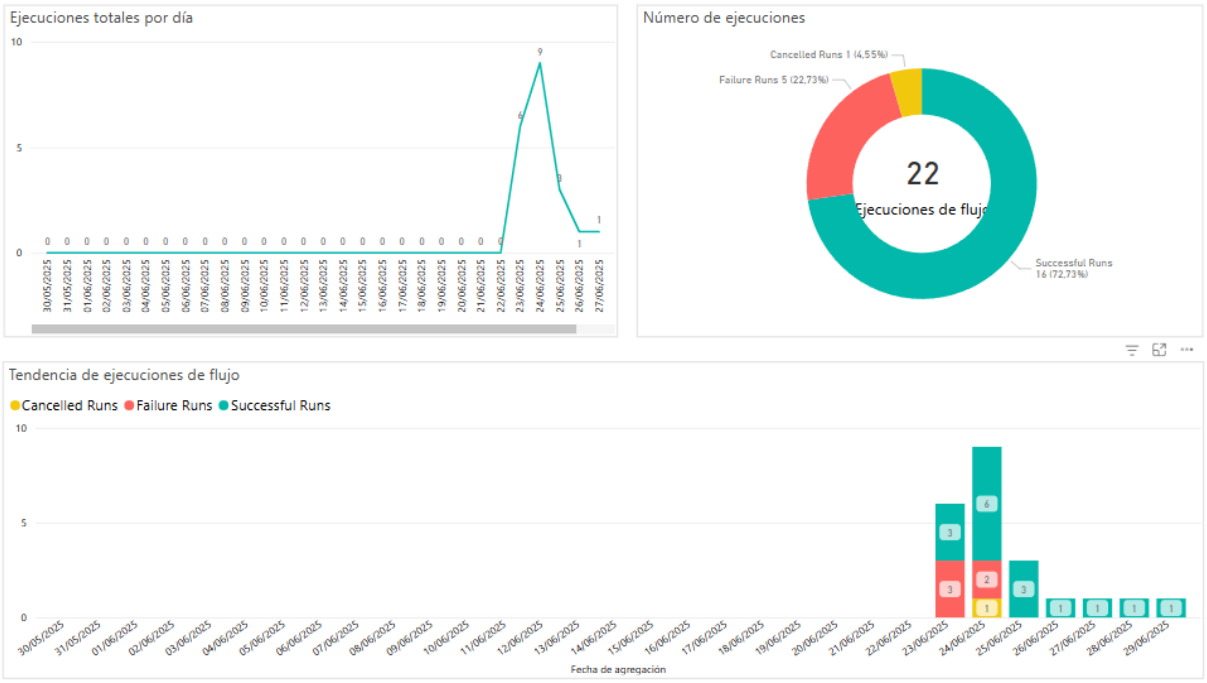


Figura 4.3. Panel de resultados de Power BI generado con datos reales.

Los resultados observados en estas pruebas respaldan la aplicabilidad de la solución al contexto y la capacidad para adaptarse a diferentes niveles de complejidad y volumen de alertas.

5. Análisis de sostenibilidad e implicaciones éticas

Este capítulo aborda las implicaciones del proyecto desde una perspectiva de sostenibilidad y ética profesional. Se analizan los impactos medioambientales y económicos asociados a la solución propuesta, así como los principios éticos que han guiado su desarrollo y despliegue. El objetivo es demostrar que, además de su viabilidad técnica, la propuesta responde a criterios responsables en cuanto al uso de recursos, protección de datos y equidad en el tratamiento de la información.

5.1. Impacto medioambiental, económico y sostenibilidad del proyecto

Este apartado evalúa el uso de recursos tecnológicos implicados en el desarrollo del sistema, así como el consumo energético estimado, el impacto económico asociado y consideraciones generales de sostenibilidad. Se analizan tanto los costes directos como el uso eficiente de herramientas digitales, con el fin de valorar la viabilidad y responsabilidad del proyecto desde una perspectiva técnica y ambiental.

5.1.1. Uso de recursos tecnológicos

El desarrollo de este proyecto se ha apoyado principalmente en tecnologías cloud y herramientas digitales que no requieren infraestructura física local, lo que contribuye a reducir el consumo energético asociado a centros de datos propios y a minimizar la obsolescencia de hardware. La mayor parte de los procesos se han realizado mediante entornos virtualizados ofrecidos por plataformas CSPs como AWS, Azure o GCP, así como mediante soluciones colaborativas como Microsoft Teams y SharePoint.

Además, se ha hecho uso de herramientas como Prisma Cloud para la supervisión de seguridad, Power Automate para la automatización de flujos de trabajo, y Power BI para la visualización de datos. Todas estas herramientas operan sobre entornos escalables y compartidos, que optimizan la utilización de recursos en función de la demanda.

Desde un punto de vista sostenible, este enfoque reduce la necesidad de disponer de equipos locales de alto rendimiento, disminuyendo la huella de carbono derivada de la fabricación, el transporte y el consumo energético de hardware tradicional. El uso de plataformas SaaS, PaaS y otras soluciones basadas en la nube permite aprovechar infraestructuras ya existentes, mejor gestionadas y energéticamente más eficientes que las locales.

5.1.2. Optimización y reducción del consumo

Uno de los pilares fundamentales de la sostenibilidad tecnológica es la capacidad para optimizar el uso de los recursos disponibles, evitando el sobredimensionamiento y reduciendo el consumo innecesario. En este proyecto, se han adoptado prácticas que promueven la eficiencia operativa a través del modelo de computación en la nube.

La automatización de procesos mediante Power Automate y la integración de múltiples fuentes de datos ha permitido reducir tareas manuales repetitivas, lo que conlleva una menor demanda de recursos computacionales y humanos. Además, el uso de servicios cloud con escalado dinámico garantiza que los recursos se consuman únicamente cuando son necesarios, evitando el gasto energético asociado a infraestructuras sobredimensionadas o infrautilizadas.

Por otro lado, la consolidación de datos en herramientas como SharePoint y su visualización optimizada en Power BI contribuyen a una toma de decisiones más ágil, evitando duplicidades, mejorando el rendimiento de los análisis y disminuyendo la necesidad de ejecutar múltiples sistemas en paralelo.

Estas prácticas no solo optimizan el uso de tecnología, sino que también tienen un impacto positivo directo en la sostenibilidad, al reducir el consumo energético, minimizar la huella de carbono digital y prolongar la vida útil de los recursos informáticos.

5.1.3. Sostenibilidad del modelo cloud

El modelo de Cloud computing introduce ventajas significativas en términos de sostenibilidad frente a la infraestructura On-premise tradicional. Al externalizar los recursos tecnológicos a centros de datos especializados y compartidos, se obtiene una mayor eficiencia energética y una reducción de la huella ambiental asociada.

Los principales CSPs, como AWS, Azure y GCP, han invertido ampliamente en infraestructuras optimizadas para el consumo energético, empleando tecnologías avanzadas de refrigeración, consolidación de cargas de trabajo, energías renovables y arquitecturas *serverless*. Estas estrategias permiten alcanzar ratios de eficiencia energética muy superiores a los de centros de datos locales, donde la infraestructura suele estar sobredimensionada o subutilizada.

Además, la virtualización y el uso de contenedores permiten un aprovechamiento más eficiente del hardware físico, reduciendo el número de máquinas necesarias para ejecutar una misma carga de trabajo. Esto se traduce en un menor uso de materiales, menor generación de residuos electrónicos y una reducción considerable del impacto ambiental global del sistema.

5.1.4. Impacto económico de la automatización

La automatización del flujo de gestión de desviaciones no solo ha supuesto mejoras operativas y de trazabilidad, sino también un impacto económico significativo. En el modelo manual, tareas como la extracción de datos, el análisis en hojas de cálculo y la actualización en Confluence consumían varias horas semanales de trabajo por parte de distintos perfiles técnicos. La nueva solución reduce drásticamente este esfuerzo, permitiendo una redistribución del tiempo hacia tareas de mayor valor añadido.

Consumo energético durante el desarrollo

Desde el punto de vista energético, el desarrollo del proyecto implicó un consumo limitado de recursos, ya que se realizó sobre entornos de oficina utilizando equipos convencionales. Tomando como referencia un consumo estimado de 70 W por equipo durante unas 540 horas de desarrollo activo, el gasto energético asociado se estima como:

Consumo durante el desarrollo activo: Estimando un consumo de 70 W por equipo durante unas 540 horas de trabajo:

$$E_{\text{desarrollo}} = 70\ \text{W} \times 540\ \text{h} = 37{,}8\ \text{kWh} \tag{5.1}$$

Consumo por pruebas de ejecución: Realizadas 22 pruebas de unos 15 minutos cada una en un equipo de 70 W:

$$E_{\text{tests}} = 70\ \text{W} \times \left(\frac{22 \times 15}{60}\right)\ \text{h} = 0{,}385\ \text{kWh} \tag{5.2}$$

Consumo total durante el desarrollo:

$$E_{\text{total desarrollo}} = E_{\text{desarrollo}} + E_{\text{tests}} = 37{,}8 + 0{,}385 = 38{,}185\ \text{kWh} \tag{5.3}$$

Considerando un factor de emisión medio en Europa de 0.231 kg CO_2/kWh, el impacto en emisiones se calcula como:

$$\text{CO}_2^{\text{desarrollo}} = 38{,}185\ \text{kWh} \times 0{,}231\ \frac{\text{kg CO}_2}{\text{kWh}} = 8{,}82\ \text{kg CO}_2 \tag{5.4}$$

Después de estos cálculos, podemos resumir el impacto medioambiental del desarrollo en la Tabla 5.1 como:

	Consumo (kWh)	**Emisiones CO_2 (kg)**
Desarrollo activo	37.8	8.73
Pruebas de ejecución	0.385	0.089
Total desarrollo	**38.185**	**8.82**

Tabla 5.1. Consumo energético y emisiones estimadas del desarrollo

Consumo mensual durante la ejecución

Durante la ejecución continua del flujo automatizado, la mayor parte de los procesos se ejecutan sobre infraestructura Cloud computing, y localmente solo se consume energía

en los accesos esporádicos al sistema. Suponiendo una carga promedio de 15 minutos diarios de uso local por parte de un solo usuario, con un consumo medio de 50 W por equipo:

$$E_{\text{operación mensual}} = \frac{70\ \text{W} \times 15\ \text{min} \times 30}{60} = 0{,}525\ \text{kWh/mes} \tag{5.5}$$

El impacto en emisiones se calcula como:

$$\text{CO}_2^{\text{operación}} = 0{,}525\ \text{kWh} \times 0{,}231\ \frac{\text{kg CO}_2}{\text{kWh}} = 0{,}121\ \text{kg CO}_2\text{/mes} \tag{5.6}$$

Este impacto es considerablemente bajo, especialmente en comparación con los beneficios indirectos obtenidos por la reducción de errores, la optimización del tiempo de trabajo, la mejora de la calidad del análisis y la disminución del uso de recursos innecesarios. Además, al ejecutarse en entornos Cloud computing, parte de la carga operativa se deriva a CSPs que operan con infraestructuras energéticamente optimizadas y con compromiso medioambiental.

En conjunto, la automatización no solo mejora la eficiencia económica del proceso, sino que también contribuye a una operación más sostenible y responsable desde el punto de vista energético.

Impacto económico

Como vemos en la Figura 5.2, se llevó a cabo el diseño, implementación, pruebas y documentación de la solución automatizada. Siendo el esfuerzo total de aproximadamente 540 horas y asumiendo una retribución simbólica de 10 €/h (acorde a prácticas universitarias), el coste en recursos humanos asciende a 5400 €.

Por otro lado, el consumo energético total estimado durante esta fase fue de 43,05 kWh, incluyendo sesiones de trabajo, ejecución de scripts, pruebas e iteraciones de carga. Con un precio medio de la electricidad en España de 0,101 €/kWh[1], el coste eléctrico se sitúa en torno a 4,10 €.

Además, se consideraron las licencias de software necesarias durante el desarrollo. En particular, se utilizaron Power Automate, SharePoint y Power BI en sus versiones de

[1]Fuente: Red Eléctrica de España. Datos de 2024.

pago, con un coste mensual por usuario estimado en 9,4 €, 5,6 € y 14 € respectivamente, durante 5 meses.

Tipo de coste	Coste/Unidad (€)	Nº de unidades	Unidad	Coste total (€)
Recursos humanos	10	540	Hora	5 400
Energía eléctrica	0,101	40,5	kWh	4,10
Power BI Pro	9,4	5	Mes	47
Power Automate Premium	14	5	Mes	70
Microsoft 365 (SharePoint)	5,6	5	Mes	28
			Total	**5 549,10**

Tabla 5.2. Coste total estimado del desarrollo del proyecto

Coste de la ejecución y mantenimiento. En cuanto al ciclo de vida operativo del sistema, se estima un coste mensual de mantenimiento de aproximadamente 8 horas al mes, correspondientes a revisión de alertas, ajustes menores en los flujos o visualizaciones y resolución de incidencias técnicas. Este mantenimiento se complementa con el consumo energético asociado a esas 8 horas (con un consumo promedio de 75 W por equipo).

Asimismo, se mantiene la necesidad de licencias activas para el entorno Microsoft (Power BI, Power Automate y SharePoint), sumando un coste fijo mensual de 29 €.

$$\text{Coste mensual} = (8 \times 10)\,€ + (8 \times 0{,}070 \times 0{,}101)\,€ + 29\,€ \approx 109{,}06\,€$$

5.2. Implicaciones éticas y sociales

El desarrollo e implementación de soluciones automatizadas para la gestión de desviaciones de seguridad en entornos Cloud computing conlleva una serie de implicaciones éticas y sociales que deben ser consideradas para asegurar una adopción responsable y alineada con los principios fundamentales de privacidad, equidad y transparencia.

Privacidad y protección de datos

Uno de los aspectos más relevantes es la protección de la información sensible tratada en el sistema. Dado que las desviaciones pueden implicar recursos que contienen datos personales o confidenciales, es fundamental aplicar el principio de *Privacy by Design* durante todo el ciclo de vida del proyecto. Esto incluye el uso de medidas técnicas como el cifrado, el control de accesos y la anonimización de datos, así como el cumplimiento con normativas como el RGPD.

Transparencia y trazabilidad

La solución desarrollada incorpora mecanismos de trazabilidad mediante el registro de cambios, la asignación de responsables y la validación de acciones. Esta transparencia no solo fortalece la confianza en los procesos de seguridad, sino que también facilita auditorías internas y externas, garantizando que las decisiones tomadas puedan justificarse con evidencia técnica.

Responsabilidad en la toma de decisiones

El uso de sistemas automatizados y el apoyo de inteligencia artificial para la generación de alertas, correos y clasificación de desviaciones implica una delegación parcial de decisiones a mecanismos automáticos. Aunque estos procesos mejoran la eficiencia, es importante mantener la supervisión humana en etapas críticas para evitar sesgos, errores no detectados y consecuencias no deseadas sobre la operación o los usuarios.

Impacto social y accesibilidad

Desde un punto de vista social, este tipo de soluciones contribuyen a mejorar la ciberseguridad organizacional, protegiendo no solo los activos tecnológicos sino también a los empleados, clientes y otras partes interesadas. Además, la visualización de datos mediante herramientas como Power BI permite que tanto perfiles técnicos como no técnicos participen en la toma de decisiones, promoviendo una cultura de seguridad más inclusiva y accesible.

Ética del desarrollo

Finalmente, se ha tenido en cuenta la ética del desarrollo tecnológico. Las herramientas que se emplearon fueron seleccionadas por su compatibilidad con buenas prácticas, licencias adecuadas y bajo impacto ambiental. Asimismo, el proyecto ha sido ejecutado sin emplear datos personales reales, respetando los principios éticos asociados al tratamiento de la información y al desarrollo de soluciones en entornos reales de empresa.

5.3. Cumplimiento normativo y estándares

El desarrollo de soluciones en entornos Cloud computing exige un compromiso firme con el cumplimiento normativo y la alineación con estándares reconocidos internacionalmente. En este proyecto, se han integrado mecanismos de control y supervisión que permiten verificar la conformidad con marcos regulatorios y de buenas prácticas ampliamente aceptados.

Normativas de seguridad y protección de datos

Uno de los principales marcos considerados es el RGPD, que establece directrices claras para la protección de datos personales dentro del ámbito europeo. Aunque el sistema no gestiona directamente Información Personal Identificable (PII), se han aplicado medidas técnicas y organizativas que refuerzan los principios de minimización, integridad y confidencialidad.

Además, se han considerado marcos los explicados en Solutions [36] e *Cumplimiento de ISO/IEC 27017* [37], que orientan sobre la gestión de la seguridad de la información y controles específicos para servicios en la nube, respectivamente. La herramienta Prisma Cloud y los controles verificados mediante Cloud Security Posture Management (CSPM) han sido alineados con estas normas para asegurar la solidez del sistema.

Controles de seguridad (CIS Controls)

La referencia principal empleada para evaluar el estado de seguridad de los recursos ha sido el conjunto de CIS Controls. Estos controles proporcionan una lista priorizada de prácticas recomendadas, que permiten reducir la superficie de ataque y mitigar riesgos comunes. En particular, se han automatizado procesos para detectar desviaciones respecto a dichos controles, facilitando el seguimiento y la mejora continua.

Relación con los Objetivos de Desarrollo Sostenible (ODS)

Este proyecto contribuye activamente a varios Objetivos de Desarrollo Sostenible definidos por Naciones Unidas en la Agenda 2030 [38]:

- **ODS 9 - Industria, innovación e infraestructura.** La solución desarrollada impulsa la modernización de los sistemas de seguridad mediante el uso de tecnologías digitales innovadoras, fomentando infraestructuras resilientes y sostenibles.
- **ODS 12 - Producción y consumo responsables.** Al promover la automatización y el uso eficiente de los recursos tecnológicos, se optimizan los flujos de trabajo y se minimiza el uso innecesario de recursos computacionales.
- **ODS 13 - Acción por el clima.** El análisis del consumo energético del sistema y la consideración de su impacto ambiental refleja una preocupación activa por la reducción de emisiones de CO2 vinculadas al desarrollo tecnológico.
- **ODS 16 - Paz, justicia e instituciones sólidas.** El refuerzo de la ciberseguridad y el cumplimiento normativo favorece instituciones digitales más seguras, transparentes y fiables, mejorando la gobernanza tecnológica.

Adaptabilidad y evolución normativa

La arquitectura de la solución ha sido diseñada para adaptarse a futuras actualizaciones regulatorias o cambios en los estándares del sector. Gracias al uso de herramientas flexibles y configurables, el sistema puede evolucionar sin necesidad de rediseños estructurales, garantizando la sostenibilidad normativa a medio y largo plazo.

6. Conclusiones y líneas futuras

Este Trabajo de Fin de Grado ha desarrollado una solución automatizada orientada a la mejora de la visibilidad y la gestión de desviaciones de seguridad en entornos Cloud. A través de la integración de herramientas corporativas como Prisma Cloud, Power Automate, SharePoint, Power BI y Microsoft Teams, se ha conseguido transformar un proceso manual, disperso y poco trazable en un flujo estructurado, eficiente y auditable.

Entre los principales logros del proyecto, cabe destacar:

- La automatización de la operativa reduciendo enormemente la carga de trabajo diaria.
- La normalización, categorización y priorización de desviaciones en base a criterios técnicos y operativos.
- La integración de un módulo de análisis mediante LLM, que enriquece el contexto técnico de cada hallazgo, alineándolo con marcos como MITRE o los controles CIS.
- La generación automática de notificaciones a responsables técnicos, reduciendo los tiempos de respuesta.

El sistema resultante mejora de forma significativa la trazabilidad, la eficiencia operativa y la capacidad de reacción ante riesgos de seguridad, aportando valor tanto en términos de cumplimiento como de gobernanza de la seguridad.

6.1. Líneas futuras

Aunque el sistema desarrollado es plenamente funcional y ha demostrado su utilidad en entornos de prueba, existen múltiples oportunidades de mejora y ampliación que podrían llevar la solución hacia una plataforma más integral y automatizada de gestión de riesgos en entornos Cloud. Las líneas futuras más destacables son:

- **Activación reactiva del flujo.** En la versión actual, el flujo se ejecuta de forma periódica cada día a las 8:00 mediante un disparador temporal. Aunque este enfoque garantiza regularidad, no permite una respuesta inmediata ante nuevas alertas. Una mejora clave consistiría en activar el flujo automáticamente en el momento en que se detecte un nuevo registro o cambio en la lista de desviaciones en SharePoint. Esta activación reactiva podría implementarse mediante conectores o flujos desencadenados por eventos, reduciendo el tiempo de reacción ante incidentes y aumentando la eficiencia operativa del sistema.

- **Escalado multicloud completo.** Aunque el flujo está diseñado de forma modular y adaptable, todavía no se ha automatizado la ingesta desde otras plataformas cloud como AWS, Azure, GCP u OCI. Una línea futura de trabajo consistiría en extender el sistema a estas nubes públicas mediante la creación de listas específicas en SharePoint para cada proveedor, manteniendo una estructura de campos homogénea que permita la integración con el flujo actual. Esto permitiría ampliar el alcance de la solución hacia una gestión verdaderamente multicloud, sin alterar el diseño base del sistema.

- **Unificación de procesos de ingesta.** Actualmente, la recopilación de desviaciones se realiza desde tres fuentes distintas, pero algunos pasos requieren aún intervención manual (como exportaciones en formato `.csv`). Se plantea unificar la ingesta bajo un único flujo automatizado centralizado, reduciendo la dependencia del factor humano y mejorando la coherencia en el almacenamiento de registros.

- **Asignación automática del responsable.** Una mejora significativa sería automatizar la identificación del responsable técnico de cada recurso afectado. Esto podría lograrse mediante la integración con un sistema de inventario o *asset management* corporativo, donde se mantenga actualizada la relación entre recursos y responsables. De este modo, se eliminaría la necesidad de consultas manuales o participación directa del equipo de ciberseguridad en esta fase.

- **Mejora de la interacción post-alerta.** Actualmente, la comunicación hacia los responsables se limita al envío de un correo técnico. En versiones futuras, se propone añadir una tarjeta adaptativa interactiva mediante Microsoft Teams, permitiendo a los destinatarios responder directamente con información clave como la fecha prevista de reconducción, solicitud de excepción o justificación documentada. Esta interacción estructurada facilitaría la trazabilidad y la automatización de las siguientes etapas del flujo.

- **Integración con sistemas de ticketing externos.** Incluir herramientas como Jira,

ServiceNow o SAI corporativos permitiría escalar la solución a entornos empresariales complejos, permitiendo una gestión más fluida y trazable de tareas de remediación a través de plataformas ya adoptadas por las organizaciones.

- **Uso de modelos avanzados de IA.** A largo plazo, se podrían entrenar modelos personalizados de lenguaje sobre desviaciones históricas específicas de la organización para mejorar la precisión del análisis técnico, la propuesta de mitigaciones y la categorización contextual de riesgos.
- **Refuerzo del módulo de auditoría.** La inclusión de mecanismos adicionales para registrar todas las decisiones manuales, las excepciones justificadas y la trazabilidad de las acciones permitiría mejorar la gobernanza del proceso y facilitar auditorías internas o externas.
- **Automatización del cierre y validación de remediaciones.** Finalmente, una evolución lógica del flujo sería incorporar validaciones automáticas mediante las APIs de los proveedores cloud, que permitan verificar si una desviación ha sido corregida efectivamente, eliminando así la necesidad de confirmaciones manuales y mejorando la eficiencia del ciclo de remediación.

Estas mejoras no solo optimizarían el rendimiento y la escalabilidad de la solución, sino que avanzarían hacia una gestión proactiva y continua de la seguridad en la nube, reforzando la postura de ciberseguridad organizacional y reduciendo la exposición a riesgos críticos.

Referencias

[1] *Prisma Cloud Documentation*, en. dirección: https://docs.prismacloud.io/en (visitado 03-06-2025).

[2] v-aangie, *Official Microsoft Power Automate documentation - Power Automate*, en-us. dirección: https://learn.microsoft.com/en-us/power-automate/ (visitado 03-06-2025).

[3] samanro, *Documentación de SharePoint*, es-es. dirección: https://learn.microsoft.com/es-es/sharepoint/ (visitado 03-06-2025).

[4] kfollis, *Documentación de Power BI - Power BI*, es-es. dirección: https://learn.microsoft.com/es-es/power-bi/ (visitado 03-06-2025).

[5] AkJo, *Documentación para desarrolladores de Microsoft Teams - Teams*, es-es. dirección: https://learn.microsoft.com/es-es/microsoftteams/platform/ (visitado 03-06-2025).

[6] *¿Qué es la seguridad en la nube?* es-419. dirección: https://cloud.google.com/learn/what-is-cloud-security (visitado 26-04-2025).

[7] P. Jogi, *What is Cloud Security and Computing? Its Challenges, Mitigation and Penetration Testing*, en-US, abr. de 2022. dirección: https://www.ssl2buy.com/cybersecurity/cloud-security-computing (visitado 03-06-2025).

[8] C. for Internet Security, *CIS Resources and Downloads*, 2025. dirección: https://downloads.cisecurity.org/#/all.

[9] *Welcome to AWS Documentation*. dirección: https://docs.aws.amazon.com/ (visitado 05-06-2025).

[10] JnHs, *Azure documentation*, en-us. dirección: https://learn.microsoft.com/en-us/azure/ (visitado 05-06-2025).

[11] *Documentación de Google Cloud | Documentation*, es-419-x-mtfrom-en. dirección: https://cloud.google.com/docs?hl=es-419 (visitado 05-06-2025).

[12] *IBM Documentation*, en-US. dirección: https://www.ibm.com/docs/www.ibm.com/docs/en (visitado 05-06-2025).

[13] *Oracle Cloud Infrastructure Documentation*. dirección: https://docs.oracle.com/en-us/iaas/Content/home.htm (visitado 05-06-2025).

[14] *Nube Pública, Privada o Híbrida, ¿con cuál te quedas?* es, nov. de 2021. dirección: https://blog-es.islonline.com/2021/11/24/nube-publica-vs-nube-privada/ (visitado 03-06-2025).

[15] *Multicloud: Conoce las características de esta tecnología*, abr. de 2025. dirección: https://impactotic.co/tecnologia/cloud/multicloud-conoce-las-caracteristicas-y-oportunidades-de-esta-tecnologia/ (visitado 03-06-2025).

[16] *Google Kubernetes Engine (GKE)*, es-419. dirección: https://cloud.google.com/kubernetes-engine (visitado 05-06-2025).

[17] *Servicio de Kubernetes administrado: Amazon EKS: AWS*, es-ES. dirección: https://aws.amazon.com/es/eks/ (visitado 05-06-2025).

[18] *Azure Kubernetes Service (AKS) | Microsoft Azure*, es-ES. dirección: https://azure.microsoft.com/es-es/products/kubernetes-service (visitado 05-06-2025).

[19] *Red Hat OpenShift enterprise application platform*, en. dirección: https://www.redhat.com/en/technologies/cloud-computing/openshift (visitado 05-06-2025).

[20] *AWS | Lambda - Gestión de recursos informáticos*, es-ES. dirección: https://aws.amazon.com/es/lambda/ (visitado 05-06-2025).

[21] *Funciones de Cloud Run*, es. dirección: https://cloud.google.com/functions (visitado 05-06-2025).

[22] *Azure Functions: Funciones sin servidor en informática | Microsoft Azure*, es-ES. dirección: https://azure.microsoft.com/es-es/products/functions (visitado 05-06-2025).

[23] *Using Cloud Functions | IBM Cloud Docs*, es. dirección: https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-functions (visitado 05-06-2025).

[24] *Microsoft 365 - Suscripción para aplicaciones de productividad | Microsoft 365*, es-ES. dirección: https://www.microsoft.com/es-es/microsoft-365 (visitado 05-06-2025).

[25] G. Workspace, *Soluciones de colaboración y optimización para empresas*, es. dirección: https://workspace.google.com/intl/es/business/ (visitado 05-06-2025).

[26] *El CRM número uno del mundo*, es. dirección: https://www.salesforce.com/es/ (visitado 05-06-2025).

[27] *dropbox.com*, es-419. dirección: https://www.dropbox.com/es/ (visitado 05-06-2025).

[28] Slack, *Gestión del trabajo mediante IA y herramientas de productividad*, es-ES. dirección: https://slack.com/intl/es-es (visitado 05-06-2025).

[29] *Convierte los correos electrónicos en ingresos*, es. dirección: https://mailchimp.com/es/ (visitado 05-06-2025).

[30] *PaaS, IaaS y SaaS: ¿en qué se diferencian? Google Cloud*, es. dirección: https://cloud.google.com/learn/paas-vs-iaas-vs-saas (visitado 19-04-2025).

[31] *Terraform | HashiCorp Developer*, en. dirección: https://developer.hashicorp.com/terraform (visitado 05-06-2025).

[32] *checkov*. dirección: https://www.checkov.io/ (visitado 05-06-2025).

[33] *KICS - Keeping Infrastructure as Code Secure*, en-US. dirección: https://kics.io/./ (visitado 05-06-2025).

[34] *Administración de la posición de seguridad en la nube (CSPM) - AWS Security Hub - AWS*, es-ES. dirección: https://aws.amazon.com/es/security-hub/ (visitado 05-06-2025).

[35] *Microsoft Defender for Cloud | Seguridad de Microsoft*, es-ES. dirección: https://www.microsoft.com/es-es/security/business/cloud-security/microsoft-defender-cloud (visitado 05-06-2025).

[36] G. Solutions, *¿Qué es la norma ISO 27001 y para qué sirve?* es-ES, mar. de 2023. dirección: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/ (visitado 27-05-2025).

[37] *Cumplimiento de ISO/IEC 27017*, es. dirección: https://cloud.google.com/security/compliance/iso-27017 (visitado 27-05-2025).

[38] *La Asamblea General adopta la Agenda 2030 para el Desarrollo Sostenible*, es, sep. de 2015. dirección: https://www.un.org/sustainabledevelopment/es/2015/09/la-asamblea-general-adopta-la-agenda-2030-para-el-desarrollo-sostenible/ (visitado 02-07-2025).

[39] *¿Qué es la nube? | Conceptos esenciales*, es-es. dirección: https://www.cloudflare.com/es-es/learning/cloud/what-is-the-cloud/ (visitado 18-04-2025).

[40] *¿Qué es el cloud computing? | IBM*, es-es, abr. de 2023. dirección: https://www.ibm.com/es-es/topics/cloud-computing (visitado 18-04-2025).

[41] *Ventajas de la computación en la nube*, es-419. dirección: https://cloud.google.com/learn/advantages-of-cloud-computing (visitado 19-04-2025).

[42] M. J. Gamez, *Objetivos y metas de desarrollo sostenible*, es. dirección: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/ (visitado 25-05-2025).

[43] *Intensidad de CO2 | Mapa mundial de intensidad de CO2 por región | Enerdata*, es. dirección: https://datos.enerdata.net/co2/intensidad-mundial-CO2.html (visitado 27-05-2025).

[44] *Cloud Computing Deployment Models Explained*, es-mx. dirección: https://trailhead.salesforce.com/es-MX/content/learn/modules/aws-cloud/understand-the-different-cloud-computing-deployment-models (visitado 03-06-2025).

[45] *Comparar planes y precios de Microsoft 365 para empresas | Microsoft 365*, es-ES. dirección: https://www.microsoft.com/es-es/microsoft-365/business/compare-all-microsoft-365-business-products (visitado 03-06-2025).

[46] *Power BI: Plan de precios | Microsoft Power Platform*, es-ES. dirección: https://www.microsoft.com/es-es/power-platform/products/power-bi/pricing (visitado 03-06-2025).

[47] *Precios de Power Automate | Microsoft Power Platform*, es-ES. dirección: https://www.microsoft.com/es-es/power-platform/products/power-automate/pricing (visitado 03-06-2025).

[48] *Microsoft 365 - Suscripción para aplicaciones de productividad | Microsoft 365*, es-ES. dirección: https://www.microsoft.com/es-es/microsoft-365 (visitado 05-06-2025).

Índice de términos

Glosario

AES-256 Algoritmo de cifrado simétrico de 256 bits ampliamente utilizado para proteger datos en reposo. 19

Algoritmo de Shor Algoritmo cuántico desarrollado por Peter Shor que permite factorizar números enteros de forma eficiente, representando una amenaza para los sistemas de cifrado basados en RSA y ECC. 22

Amazon Elastic Kubernetes Service (EKS) Servicio de AWS para ejecutar aplicaciones basadas en contenedores usando Kubernetes. 15

AWS Lambda Plataforma de Amazon Web Services que permite ejecutar funciones bajo demanda sin gestionar servidores. 16

AWS Security Hub Servicio de AWS que proporciona una vista integral del estado de seguridad en las cuentas y recursos de AWS, integrando hallazgos de múltiples servicios de seguridad. 26

Azure Functions Plataforma de Microsoft Azure para ejecutar código en respuesta a eventos con modelo sin servidor. 16

Azure Key Vault Servicio de Microsoft Azure para almacenar y gestionar secretos, claves de cifrado y certificados digitales. 19

Azure Kubernetes Service (AKS) Plataforma de Microsoft Azure para gestionar entornos de contenedores con Kubernetes. 15

Backup Proceso de copia y almacenamiento de datos para prevenir su pérdida y permitir su recuperación en caso de incidentes. 20

Business Continuity Capacidad de una organización para mantener sus funciones críticas o restablecerlas rápidamente tras una interrupción, garantizando la resiliencia operativa y la mínima pérdida de servicio. 12

Checkov Herramienta de análisis estático de código que escanea archivos de infraestructura como código (por ejemplo, Terraform o CloudFormation) en busca de errores de configuración y vulnerabilidades antes de su despliegue. 21

Cloud Entorno de computación en la nube que permite acceso remoto a recursos tecnológicos. 1–4, 8, 11, 12, 15, 19, 21, 24, 26, 30, 52, 66

Cloud bursting Técnica utilizada en entornos de nube híbrida que permite redirigir automáticamente cargas de trabajo desde una infraestructura privada a una pública cuando se supera la capacidad. 12

Cloud computing Modelo de computación que permite acceder bajo demanda a recursos informáticos a través de Internet, sin necesidad de infraestructura local. 2, 9, 10, 17, 18, 59–62, 64

Cloud Security Posture Management (CSPM) Herramienta para evaluar y supervisar la configuración de seguridad en infraestructuras cloud, detectando desviaciones y riesgos. 20, 25–27, 30, 33, 64, 75

Compute Engine Servicio de Google Cloud que permite el uso de máquinas virtuales como parte del modelo IaaS. 14

Confluence Herramienta colaborativa desarrollada por Atlassian para crear, organizar y compartir documentación entre equipos de trabajo. 27

Contenedor Unidad de software ligera que empaqueta código, bibliotecas y dependencias necesarias para ejecutar una aplicación de forma aislada. 14

Disaster Recovery (DR) Conjunto de políticas, herramientas y procedimientos diseñados para restaurar servicios y sistemas críticos tras un incidente que interrumpa la operativa normal, como fallos técnicos, ciberataques o desastres naturales. 17, 20, 24

Dropbox Servicio de almacenamiento en la nube basado en el modelo SaaS que permite sincronizar y compartir archivos entre dispositivos. 16

EDR *Endpoint Detection and Response*. Herramienta de seguridad que supervisa y analiza las actividades en los endpoints (dispositivos finales) para detectar, investigar y responder a amenazas en tiempo real. 25

Elastic Compute Cloud (EC2) Servicio de máquinas virtuales de Amazon Web Services (AWS) que forma parte del modelo IaaS. 14

Gemini Modelo de lenguaje avanzado desarrollado por Google DeepMind, diseñado para tareas de procesamiento de lenguaje natural (PLN), generación de texto, análisis contextual y razonamiento complejo.. 44–47

Google App Engine Plataforma de desarrollo en la nube de Google que permite desplegar aplicaciones web sin necesidad de gestionar la infraestructura. 15

Google Cloud Functions Servicio de Google Cloud que permite ejecutar funciones sin servidor en respuesta a eventos. 16

Google Kubernetes Engine (GKE) Servicio de Google Cloud que permite desplegar y gestionar clústeres de Kubernetes como parte del modelo CaaS. 15

Google Workspace Conjunto de aplicaciones colaborativas de Google, como Gmail, Google Drive, Docs, Sheets y Meet. 16

Heroku Plataforma en la nube que permite construir, ejecutar y escalar aplicaciones de forma sencilla usando varios lenguajes de programación. 15

IBM Cloud Functions Servicio basado en Apache OpenWhisk que permite ejecutar funciones en la nube bajo el modelo FaaS. 16

Infraestructura heredada Sistemas tecnológicos existentes, normalmente locales, que han sido desplegados con anterioridad a la adopción de soluciones en la nube. 11, 12

Infrastructure as Code (IaC) Modelo de provisión de infraestructura mediante archivos de configuración que pueden versionarse y automatizarse como código. 21, 77

Mailchimp Plataforma SaaS de automatización de marketing y envío masivo de correos electrónicos. 16

Microsoft 365 Suite de productividad de Microsoft basada en la nube que incluye herramientas como Word, Excel, Outlook, Teams y OneDrive. 16

Microsoft Azure App Service Servicio de plataforma como servicio (PaaS) de Azure que permite alojar aplicaciones web, APIs REST y backends móviles en un entorno escalable. 15

Microsoft Defender for Cloud Herramienta de Azure que proporciona capacidades de Cloud Security Posture Management (CSPM) y protección de cargas de trabajo para mejorar la postura de seguridad en entornos híbridos y multicloud. 26

Microsoft Teams Plataforma de comunicación y colaboración empresarial de Microsoft que permite chats, videollamadas, trabajo en equipo y la integración de múltiples herramientas en un entorno corporativo. 2–4, 48, 57, 66, 67

Middleware Software que actúa como capa intermedia entre el sistema operativo y las aplicaciones, facilitando la comunicación y gestión de datos entre componentes distribuidos. 15

MITRE Organización sin ánimo de lucro que gestiona centros de investigación y desarrollo financiados por el gobierno de Estados Unidos. Es conocida por su mantenimiento del framework ATT&CK, una base de conocimientos de técnicas utilizadas por atacantes en el mundo real. 41, 43, 50, 66

On-premise Infraestructura tecnológica alojada y gestionada físicamente dentro de las instalaciones de una organización. 1, 10, 11, 18, 59

OpenStack Plataforma de código abierto para la gestión de infraestructuras como servicio (IaaS) en nubes públicas y privadas. 14

Outlook Herramienta de correo electrónico y calendario desarrollada por Microsoft, ampliamente utilizada en entornos corporativos.. 31, 50, 53

Power Automate Herramienta de Microsoft para crear flujos de trabajo automatizados. 2–4, 22, 23, 30, 31, 36, 39, 48, 58, 61, 66

Power BI Herramienta de Microsoft para visualización de datos e informes interactivos. 2–4, 20, 22, 23, 25, 29, 31, 32, 58, 61, 63, 66

Principio de menor privilegio Modelo de seguridad que establece que cada usuario, sistema o proceso debe tener únicamente los permisos mínimos necesarios para realizar sus funciones, reduciendo así el riesgo de accesos no autorizados o uso indebido. 19

Prisma Cloud Herramienta de seguridad en la nube que permite supervisar configuraciones, vulnerabilidades y cumplimiento. 2–4, 20, 23, 25–30, 33, 34, 43, 58, 64, 66

Red Hat OpenShift Plataforma empresarial basada en Kubernetes que permite desarrollar, desplegar y escalar aplicaciones de forma automatizada bajo un modelo PaaS o CaaS. 15

Salesforce Plataforma en la nube para gestión de relaciones con clientes (CRM), ventas, atención al cliente y automatización de marketing. 16

SEGCLD Base de datos centralizada para la gestión de controles de seguridad y cumplimiento en entornos cloud, utilizada para registrar, almacenar y consultar desviaciones, estados y métricas relevantes del sistema. 33, 34

SharePoint Plataforma colaborativa de Microsoft utilizada para almacenamiento, gestión de datos y documentación. 2–4, 22, 23, 31, 32, 39–41, 50, 52, 57, 58, 61, 66, 67

SIEM Sistema para la gestión de eventos e información de seguridad que permite recopilar, analizar y correlacionar eventos de múltiples fuentes. 20, 21, 25

Slack Plataforma de mensajería y colaboración empresarial basada en canales, ofrecida como servicio SaaS. 16

Tenencia múltiple Modelo de uso en la nube en el que múltiples clientes comparten recursos físicos gestionados por un proveedor, manteniendo entornos virtualizados aislados. 10

Terraform Herramienta de infraestructura como código (Infrastructure as Code (IaC)) desarrollada por HashiCorp que permite definir, aprovisionar y gestionar recursos de infraestructura a través de archivos de configuración declarativos. 21

Time-to-market Tiempo que transcurre desde la concepción de un producto o servicio hasta su disponibilidad en el mercado. Su reducción es clave para aumentar la competitividad. 18

Zero Trust Modelo de seguridad que asume que ninguna entidad, interna o externa a la red, es confiable por defecto. Requiere autenticación y validación continua para cada acceso a recursos. 19

Siglas

API Application Programming Interface. 15, 30, 33, 34, 36

APT Advanced Persistent Threat. 21

AWS Amazon Web Services. 10, 12, 14, 28, 29, 57, 59, 67, 73

Azure Microsoft Azure. 10, 12, 14, 28, 29, 57, 59, 67, 75

BaaS Backend as a Service. 14, 15

CaaS Container as a Service. 14

CIS Center for Internet Security Controls. 1, 2, 19, 20, 23, 24, 26, 30, 43, 65, 66

CSP Cloud Service Provider. 9, 17, 18, 26, 57, 59, 61

FaaS Function as a Service. 14, 16

GCP Google Cloud Platform. 10, 12, 14, 28, 29, 57, 59, 67

IaaS Infrastructure as a Service. 13–15, 20, 30

IAM Identity and Access Management. 18, 19

IBM Cloud Infraestructura y servicios cloud de International Business Machines. 10, 12, 14

IoT Internet of Things. 18

ISO Organización Internacional de Normalización. 19, 20

KICS . 21

KMS Key Management Service. 19

LLM Modelo de lenguaje grande. 41, 45, 52, 66

ML Machine Learning. 21

NIST National Institute of Standards and Technology. 19, 20, 22

OCI Oracle Cloud Infrastructure. 10, 12, 14, 67

PaaS Platform as a Service. 13–15

PII Información Personal Identificable. 64

RBAC Role-Based Access Control. 19

RGPD Reglamento General de Protección de Datos. 1, 20, 24, 63, 64

SaaS Software as a Service. 14, 16

SAI Sistema de Atención de Incidencias. 30, 34

SLA Service Level Agreement. 34

TI Tecnologías de la Información. 9, 17

TLS Transport Layer Security. 19

VPC Virtual Private Cloud. 11