

Cloud Security Posture Management (CSPM)

Alumno: Rubén Vázquez González
Máster universitario de Ciberseguridad y Privacidad
Seguridad Empresarial

Consultor: Manuel Jesús Mendoza Flores
Profesor responsable: Víctor García Font
Fecha Entrega: junio de 2021



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

FICHA DEL TRABAJO FINAL

Título del trabajo:	<i>Cloud Security Posture Management (CSPM)</i>
Nombre del autor:	<i>Rubén Vázquez González</i>
Nombre del consultor/a:	<i>Manuel Jesús Mendoza Flores</i>
Nombre del PRA:	<i>Victor Garcia Font</i>
Fecha de entrega (mm/aaaa):	06/2021
Titulación:	<i>Máster universitario de Ciberseguridad y Privacidad</i>
Área del Trabajo Final:	<i>Seguridad Empresarial</i>
Idioma del trabajo:	<i>Castellano</i>
Palabras clave	<i>CSPM; Nube; Seguridad</i>
Resumen del Trabajo	
<p>La finalidad de este trabajo final de máster es comprender cuales son las principales amenazas a las que se somete el cloud computing y que justifican la aparición de un tipo de herramientas denominadas Cloud Security Posture Management (CSPM), que nos ayudan a corregir las malas configuraciones de nuestros despliegues en la nube, además de facilitar el cumplimiento normativo.</p> <p>Se ha seguido una metodología de tres fases, en la que primero, se realiza una fase teórica de documentación, en la que se identifican las amenazas y controles más habituales del cloud computing, y se describe la hoja de ruta a seguir en las organizaciones para conseguir un entorno cloud seguro, donde se listan los diferentes tipos de herramientas para conseguirlo, entre las que se encuentran las CSPM.</p> <p>Posteriormente, se revisan algunas soluciones de este tipo herramientas de código abierto, propietarias y nativas para finalmente implementarlas en un entorno de laboratorio y realizar pruebas de corrección de configuraciones y adaptación a un determinado estándar de cumplimiento, que nos ayudará a comprender mejor su funcionamiento y características.</p>	
Abstract:	
<p>The purpose of this final master's thesis is to understand which are the main threats to which cloud computing is subjected and which justify the appearance of a type of tools called Cloud Security Posture Management (CSPM), which help</p>	

us to correct bad configurations of our cloud deployments, in addition to facilitating regulatory compliance.

A three-phase methodology has been followed. The first one is a theoretical documentation phase, in which the most common threats and controls of cloud computing are identified, and the roadmap to be followed in organizations to achieve a secure cloud environment, where the different types of tools to achieve this are listed, among which are the CSPM's.

Subsequently, some open source, proprietary and native solutions of this type of tools are reviewed, to finally implement them in a laboratory environment and carry out tests of remediation of misconfigurations and compliance with a certain standard, which will help us to better understand their operation and features.

Índice

1. Introducción: Plan de trabajo	1
1.1. Contexto y justificación	1
1.2. Objetivos	3
1.3. Metodología	3
1.4. Recursos necesarios.....	4
1.5. Listado de tareas.....	4
1.6. Planificación.....	6
1.7. Productos obtenidos	7
2. Computación en la nube: riesgos en la seguridad de la información y cumplimiento normativo	8
2.1. Computación en la nube	8
2.2. Controles de seguridad más habituales en computación en la nube	11
2.3. Cumplimiento normativo en la nube.....	17
3. Seguridad en nubes públicas	18
3.1. Estrategia y habilidades	18
3.2. Diseño y arquitectura	19
3.3. Implementación.....	20
3.4. Operacionalizar	27
4. Herramientas Cloud Security Posture Management.....	29
4.1. Herramientas propias.....	29
4.2. Herramientas Open Source	33
4.3. Herramientas propietarias	35
5. Fase práctica	39
5.1. Selección de proveedores cloud y despliegue de entorno de prueba	39
5.2. Prueba de herramientas CSPM	46
6. Conclusiones	77
7. Glosario	79
8. Bibliografía.....	81

Índice de ilustraciones

Figura 1: Grupos de herramientas seguridad Cloud	2
Figura 2: Modelo de seguridad compartida en Azure.....	2
Figura 3: Listado de tareas.....	5
Figura 4: Diagrama de Gantt.....	6
Figura 5: Ruta para implementación de seguridad en nubes públicas.....	18
Figura 6: Arquitectura de seguridad SABSA	19
Figura 7: Cobertura herramientas cloud.....	21
Figura 8: Arquitectura CASB	23
Figura 9: Tipos de herramientas CWPP, y capacidades mínimas	24
Figura 10: Caso de uso típicos para CSPM	25
Figura 11: Arquitectura lógica para seguridad en la nube	27
Figura 12: Funcionamiento de AWS Security Hub	29
Figura 13: Mapa de red creado por Azure Security Center	32
Figura 14: Cuadrante mágico de Gartner de proveedores cloud públicos	39
Figura 15: Laboratorio	40
Figura 16: Creación de MV en GCP.....	41
Figura 17: Reglas Firestore	41
Figura 18: Configuración Cloud Storage	42
Figura 19: Configuración cuenta de almacenamiento Azure.....	43
Figura 20: Creación de función en Azure	44
Figura 21: Azure Security Center, inventariado.....	44
Figura 22: Conexión a máquina virtual de AWS por SSH	45
Figura 23: Función de AWS	45
Figura 24: Configuración insegura S3.....	46
Figura 25: Configuración AWS Security Hub	47
Figura 26: AWS Security Hub, resumen.....	48
Figura 27: AWS Security Hub, estándares de seguridad	48
Figura 28: AWS Security Hub, observaciones	48
Figura 29: AWS Security Hub, resultados	49
Figura 30: AWS Config, inventariado	49
Figura 31: AWS Config, HIPAA no conforme	50
Figura 32: AWS Config, regla no conforme.....	51
Figura 33: AWS Config, regla conforme.....	51
Figura 34: Regla con severidad alta.....	52
Figura 35: Detalles y corrección de la regla	52
Figura 36: Regla aplicada	53
Figura 37: Detalle de la regla	53
Figura 38: Botón de "Solucionar" hallazgo y solución del incidente	53
Figura 39: Cumplimiento PCI DSS v3.2.1	54
Figura 40: Detalle cumplimiento PCI DSS.....	54
Figura 41: Security Center, conectores de nube	55
Figura 42: Security Center. resumen.....	55



Figura 43: Detalle de inventario	56
Figura 44: Security Center, recomendaciones	56
Figura 45: Detalle del control	57
Figura 46: Recurso afectado	57
Figura 47: Grupo de seguridad de red	58
Figura 48: Recurso en estado correcto	58
Figura 49: Security Center, cumplimiento	59
Figura 50: Detalle cumplimiento ISO 27001:2013	60
Figura 51: Controles criptográficos	60
Figura 52: Detalle control no conforme de cumplimiento	61
Figura 53: Prueba de Quick Fix	61
Figura 54: Corregir hallazgo	62
Figura 55: Solución del hallazgo	62
Figura 56: Fichero config.js	63
Figura 57: CloudSploit, resultado TLSVersionCheck	65
Figura 58: CloudSploit, AWS, resultado encriptación de bucket	65
Figura 59: CloudSploit, AWS, re-comprobación	65
Figura 60: Cifrado de bucket antes y después, vía panel de AWS	66
Figura 61: GCP, una VPC por región	66
Figura 62: Hub de aplicaciones de Palo Alto para nube	68
Figura 63: Script Terraform para la creación del usuario	69
Figura 64: Panel lateral de Prisma Cloud	69
Figura 65: Dashboard de Prisma Cloud	70
Figura 66: Inventario de activos en la nube	70
Figura 67: Prisma Cloud, recurso S3 de AWS afectado	71
Figura 68: Prisma Cloud, S3 con acceso publico	71
Figura 69: Prisma Cloud, guía de remediación manual	71
Figura 70: Comando CLI para remediación automática	72
Figura 71: Recurso afectado y remediación de la política	72
Figura 72: Acceso denegado al fichero del bucket de S3	72
Figura 73: Listado de alertas de Prisma Cloud	73
Figura 74: Motor de reglas de Prisma Cloud	73
Figura 75: Cobertura de cumplimiento general (izquierda) y específico del ISO 27001:2013 (derecha)	74
Figura 76: Estándares de cumplimiento disponibles	74

Índice de tablas

Tabla 1. Controles cloud más habituales	16
Tabla 2: Herramientas CSPM de código abierto	34
Tabla 3: Herramientas CSPM propietarias.....	36
Tabla 4: CloudSploit, controles por CSP	63
Tabla 5: CloudSploit, órdenes y descripción	64
Tabla 6: CloudSploit, TLSVersionCheck	64
Tabla 7: CloudSploit, AWS, comprobar encriptación de bucket.....	65
Tabla 8: CloudSploit, AWS, remediación	65
Tabla 9: CloudSploit, GCP, compliance en PCI DSS	66
Tabla 10: Resultado VPC GCP	67
Tabla 11: Listado de estándares de cumplimiento por CSP y políticas aplicadas....	75

1. Introducción: Plan de trabajo

1.1. Contexto y justificación

Cada vez son más las organizaciones que deciden mover sus cargas computacionales a la nube. Esto es debido a sus interesantes propiedades como la alta disponibilidad, elasticidad, agilidad y tolerancia a fallos, que permiten a las organizaciones ofrecer un mejor servicio a sus clientes independientemente de muchos factores que pudieran ocurrir, con una importante reducción en sus costos de operación. Según la consultora Gartner [1], se espera que durante el 2021 el gasto destinado a nubes públicas aumente un 18%, mientras que para 2024, y acelerado por la situación actual de pandemia por la COVID-19, se espera que la nube represente el 14.2% del gasto total de las tecnologías de la información (TI) de las empresas.

Esta nueva forma de gestionar las TI de las organizaciones, sumado muchas veces con la falta de experiencia del personal y la continua evolución de la nube, hacen que las empresas desconozcan los riesgos en la seguridad de la información a los que están expuestos, suponiendo muchas de las veces que la responsabilidad total de la seguridad recae sobre el proveedor de nube. Al mismo tiempo, la necesidad de cumplir y mantener la conformidad con requisitos normativos y marcos regulatorios pueden convertir la nube en un verdadero quebradero de cabeza para las organizaciones.

A partir de esta nueva problemática, han surgido una serie de herramientas tanto nativas como de terceras partes que buscan solventar los problemas de seguridad de la información y cumplimiento normativo que nos presenta la nube. Gartner definió una taxonomía de este tipo de herramientas, distinguiendo tres tipos principales [2]; Cloud Access Security Brokers (CASB), que son un grupo de herramientas encargadas de realizar de intermediario en los procesos de autenticación y autorización con la nube; Cloud Workload Protection Platforms (CWPP), que es la adaptación de las soluciones on-premises a entornos cloud para la protección de las cargas de trabajo; y por último, Cloud Security Posture Management (CSPM), que son un conjunto de herramientas que, automáticamente, evalúan los entornos en la nube contra las mejores prácticas en seguridad de la información, facilitando el cumplimiento normativo y ofreciendo facilidades o automatismos para solventar todos los hallazgos. Cada una de estas herramientas tiene un caso de uso concreto en función del modelo de nube utilizado (IaaS/PaaS/SaaS), tal y como se observa en Figura 1, que se comprende tras ver el modelo de responsabilidad compartida (ver Figura 2) definido por un proveedor de nube público (Cloud Service **Proveedor**, CSP), donde se marcan los límites de responsabilidad de ambas partes.

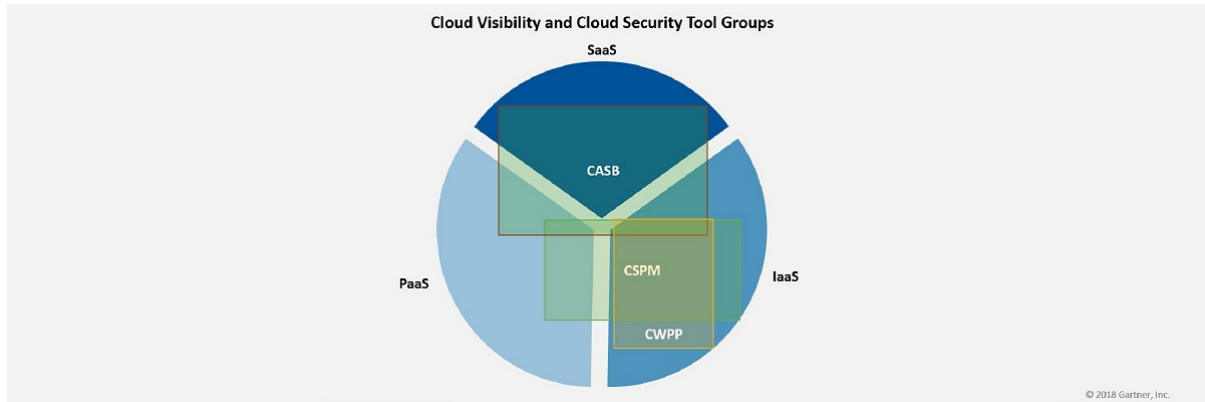


Figura 1: Grupos de herramientas seguridad Cloud

Este modelo de responsabilidad compartida muestra quién es el responsable (proveedor de nube, cliente, o compartido) en cada una de las capas, según el modelo de nube implementado. Si analizamos la Figura 2, vemos como en los modelos IaaS, PaaS y SaaS, el proveedor de nube (Microsoft en este caso), es el responsable de todos los elementos físicos de la red, y por tanto, de la correcta implementación de los controles de seguridad física, a diferencia de las infraestructuras on-premises, en la que la responsabilidad recae en el lado del cliente.



Figura 2: Modelo de seguridad compartida en Azure

A medida que cambiamos entre modelos de nube desde IaaS hasta SaaS, observamos como cada vez más responsabilidades se van cediendo al proveedor de nube. Para las capas de responsabilidad relacionadas con la gestión de identidades y datos mostradas en la figura (capas superiores), vemos como siempre es el cliente final el que está obligado a la correcta implementación de los controles de seguridad y configuraciones apropiados. Para casos particulares, como el mostrado en la Figura 2 para los controles de aplicación en un PaaS, vemos como se trata de

responsabilidades compartidas, ya que el proveedor de nube gestionará parte de la infraestructura mientras que es el cliente el que debe proveer su propia implementación de controles (administración de parches, configuraciones, etc). Por ejemplo, siguiendo con el caso de los controles de aplicación en un PaaS, si tenemos una pequeña aplicación web ejecutándose sobre un modelo PaaS, y dicha aplicación web tiene un fallo de seguridad debido a una configuración incorrecta, será nuestra responsabilidad el detectar y remediar dicho fallo, y nunca del proveedor de nube, mientras que si el modelo usado para ejecutar la aplicación fuera un SaaS, sería el proveedor de nube el responsable de dicha incidencia.

El presente trabajo de fin de máster pretende identificar cuáles son los principales riesgos en la seguridad de la información a los que se enfrenta la nube pública, así como analizar las diferentes herramientas del grupo CSPM presentes en el mercado para este tipo de nubes. Por último, se espera crear un pequeño laboratorio con las principales nubes públicas para la puesta en marcha y prueba de algunas de estas herramientas.

Para la elección de las herramientas CSPM a utilizar, se analizan aspectos como: el número de nubes públicas compatibles, (multi-cloud); soluciones nativas o de terceras partes; licencia gratuita o modo demo disponible, entre otros.

Para la elección de qué nubes públicas usar para las pruebas de las herramientas, se ha consultado el cuadrante mágico de Gartner del 2020 sobre infraestructura cloud y plataforma como servicios [3], eligiendo a los 3 proveedores públicos de nube líderes, que son, Amazon Web Services (AWS), Microsoft Azure (AZ) y Google Cloud Platform (GCP).

1.2. Objetivos

Los objetivos principales de este trabajo de fin de máster son los siguientes:

- Identificar cuáles son los principales riesgos de la seguridad de la información presentes en nubes públicas.
- Listar las diferentes soluciones CSPM presentes en el mercado, identificando sus principales características.
- Diseñar e implementar un entorno de pruebas con las principales nubes públicas en los que probar algunas herramientas seleccionadas.

1.3. Metodología

La metodología a seguir para dar cumplimiento a los objetivos marcados en el presente trabajo de fin de máster viene definida por las siguientes fases o etapas:

Fase teórica

En esta primera fase, se identifican los diferentes riesgos de seguridad de la información a los que están sometidos los entornos cloud, se buscan los mecanismos

de mitigación existentes y se centra en un conjunto de herramientas específico, donde se indica la oferta actual de soluciones disponibles y sus principales características.

Fase práctica

En esta segunda fase, se crea un laboratorio con un conjunto de clouds públicos específicos y se prueban una serie de herramientas seleccionadas partiendo del estudio del listado anterior.

Conclusiones

A partir de las pruebas y estudios realizados, se muestran las conclusiones obtenidas y se identifican posibles líneas de trabajo futuras.

1.4. Recursos necesarios

Para llevar a cabo las fases descritas en el punto anterior, necesitaremos los siguientes recursos:

- Un computador personal con conexión a Internet que disponga de: un software de procesador de textos para elaborar el documento final entregable del proyecto; un navegador web con el que conectarnos al portal de los proveedores cloud elegidos; cualquier otro software necesario para conectarnos a dichos entornos cloud por otra vía distinta al navegador
- Cuentas de usuario, suscripciones o similar, en los proveedores cloud elegidos
- Licencias o demos de las herramientas empleadas, si aplica.

1.5. Listado de tareas

En la Figura 3 se detallan las tareas a tratar en cada una de las etapas indicadas en el apartado anterior:

































		Nombre	Duración	Inicio	Fin	Predecesoras	Recursos
1		☐ Trabajo de Fin de Máster	37 días	17/02/2021	17/06/2021		Rubén Vázquez (autor)
2		☐ Planificación	10 días	17/02/2021	02/03/2021		Rubén Vázquez (autor)
3		Documentación previa	4 días	17/02/2021	22/02/2021		Rubén Vázquez (autor)
4		Objetivo del trabajo	1 día	23/02/2021	23/02/2021	3	Rubén Vázquez (autor)
5		Ámbito del trabajo	1 día	24/02/2021	24/02/2021	4	Rubén Vázquez (autor)
6		Tareas, recursos y planificación	2 días	25/02/2021	26/02/2021	5	Rubén Vázquez (autor)
7		Redacción PEC1	1 día	02/03/2021	02/03/2021	6	Rubén Vázquez (autor)
8		PEC1. Plan de trabajo	0 día	02/03/2021	02/03/2021	7	Rubén Vázquez (autor)
9		☐ Fase teórica	20 días	03/03/2021	30/03/2021		Rubén Vázquez (autor)
10		Documentación sobre cloud	6 días	03/03/2021	10/03/2021	8	Rubén Vázquez (autor)
11		Identificar riesgos sobre cloud	1 día	15/03/2021	15/03/2021	10	Rubén Vázquez (autor)
12		Búsqueda de soluciones de seguridad y cumplimiento en cloud	3 días	16/03/2021	18/03/2021	11	Rubén Vázquez (autor)
13		Búsqueda de herramientas CSPM	1 día	25/03/2021	25/03/2021	12	Rubén Vázquez (autor)
14		Elección de proveedores cloud y herramientas CSPM para parte práctica	2 días	26/03/2021	29/03/2021	13	Rubén Vázquez (autor)
15		Redacción PEC2	1 día	30/03/2021	30/03/2021	14	Rubén Vázquez (autor)
16		PEC2. Entrega de seguimiento	0 día	30/03/2021	30/03/2021	15	Rubén Vázquez (autor)
17		☐ Fase práctica	20 días	31/03/2021	27/04/2021		Rubén Vázquez (autor)
18		Creación de cuentas e instancias en cloud seleccionadas	2 días	31/03/2021	01/04/2021	16	Rubén Vázquez (autor)
19		Instalación de herramientas CSPM	4 días	02/04/2021	07/04/2021	18	Rubén Vázquez (autor)
20		Configuración de herramientas	6 días	08/04/2021	15/04/2021	19	Rubén Vázquez (autor)
21		Pruebas de herramientas	7 días	16/04/2021	26/04/2021	20	Rubén Vázquez (autor)
22		Toma de capturas y conclusiones	7 días	16/04/2021	26/04/2021	19	Rubén Vázquez (autor)
23		Redacción PEC3	1 día	27/04/2021	27/04/2021	22	Rubén Vázquez (autor)
24		PEC3. Entrega de seguimiento	0 día	27/04/2021	27/04/2021	23	Rubén Vázquez (autor)
25		☐ Presentación	37 días	28/04/2021	17/06/2021		Rubén Vázquez (autor)
26		Conclusiones y trabajo futuro	8 días	28/04/2021	07/05/2021	24	Rubén Vázquez (autor)
27		Redacción PEC4 / Memoria	16 días	10/05/2021	31/05/2021	26	Rubén Vázquez (autor)
28		PEC4. Memoria final. Redacción	0 día	01/06/2021	01/06/2021	27	Rubén Vázquez (autor)
29		Preparación PEC5	4 días	02/06/2021	07/06/2021	28	Rubén Vázquez (autor)
30		PEC5. Presentación en video	0 día	08/06/2021	08/06/2021	29	Rubén Vázquez (autor)
31		Defensa del trabajo de fin de máster	0 día	17/06/2021	17/06/2021	30	Rubén Vázquez (autor)

Figura 3: Listado de tareas

1.6. Planificación

Se muestra en la Figura 4 la planificación temporal del proyecto mediante un diagrama de Gantt:

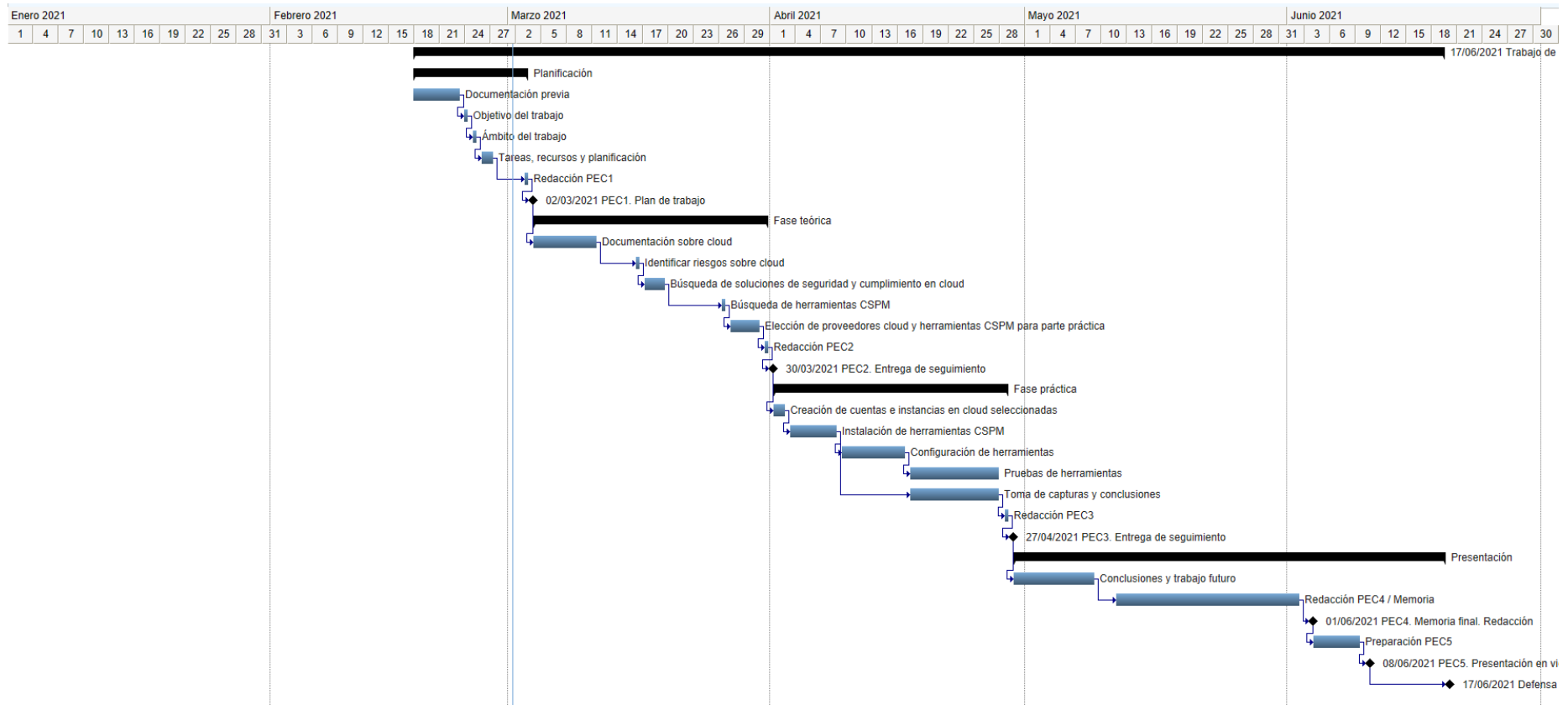


Figura 4: Diagrama de Gantt

1.7. Productos obtenidos

Este trabajo de fin de máster se divide en los siguientes entregables, que formarán parte de la memoria final del proyecto:

PEC1. Plan de trabajo. Entregable explica cuál es el problema a resolver con el presente trabajo y el estado del arte de la tecnología actual, se muestran los objetivos que se quieren alcanzar, mediante qué metodología y con qué recursos, definiendo una planificación temporal con las tareas a realizar.

PEC2. Entrega de seguimiento 1. Se entrega un documento con las tareas realizadas hasta el momento según la planificación, ajustándola en caso necesario según los avances., y un breve resumen sobre el estudio teórico realizado, mostrando las diferentes herramientas CSPM encontradas.

PEC3. Entrega de seguimiento 2. Al igual que el anterior, se trata de un entregable donde se muestran los avances realizados, y se ajusta la planificación en caso necesario. En este documento, se muestran los avances de la fase práctica, mostrando qué proveedores de cloud públicos y herramientas CSPM se han elegido. Se dan detalles sobre su implementación y principales características.

PEC4. Memoria final. Se sintetiza en un documento el trabajo realizado durante el trabajo de fin de máster y se muestran las conclusiones obtenidas, así como otra posible información (Anexos, bibliografía, etc.).

PEC5. Presentación en video. En este entregable se realiza una presentación resumen con diapositivas sobre el proyecto y se elabora un pequeño video narrado por el autor describiendo el trabajo realizado.

2. Computación en la nube: riesgos en la seguridad de la información y cumplimiento normativo

2.1. Computación en la nube

La computación en la nube, o cloud computing, consiste en la entrega de servicios computacionales a través de Internet. Entre esos servicios, encontramos servidores, bases de datos, almacenamiento, red, software, analíticas e inteligencia. La computación en la nube ofrece una mayor rapidez en la innovación, flexibilidad en los recursos y la ventaja significativa de las economías de escala.

La nube o cloud (refiriéndonos siempre a computación en la nube) generalmente funciona usando una estructura pay-as-you-go, donde se paga por lo que se usa, lo que permite una reducción considerable en los costes de operación (OpEx) y un uso más eficiente de la infraestructura, pudiéndose adaptar dinámicamente a las condiciones de negocio necesarias en cada momento. Por otro lado, es el proveedor de nube el encargado del mantenimiento de toda la infraestructura subyacente, con todo lo que ello supone.

Además de lo anterior, las aplicaciones desplegadas en la nube ofrecen una serie de beneficios adicionales sobre las desplegadas en entornos on-premises convencionales, entre ellas, destacan:

- Alta disponibilidad, lo que permite que la aplicación desplegada esté el mayor tiempo posible en funcionamiento y sea accesible por los usuarios finales. Este factor viene determinado por el acuerdo de nivel de servicio del servicio cloud contratado (o Service Level Agreement, SLA)
- Escalabilidad, lo que permite a la aplicación o servicio cloud aumentar o disminuir su poder de cómputo en todo momento. Se distinguen dos tipos de escalabilidad; vertical, en la que la capacidad de computación se incrementa añadiendo más memoria RAM o CPU a una máquina virtual (MV) o servicio en general; y horizontal, donde lo que se hace es añadir más instancias de un recurso a la solución, como, por ejemplo, añadiendo más máquinas virtuales y balanceando la carga entre las diferentes máquinas.
- Elasticidad, que permite a las aplicaciones escalarse de forma automática de manera que puedan seguir estando disponibles a pesar de los picos de mayor demanda. Esta característica permite a las soluciones cloud adaptarse a las situaciones cambiantes de negocio y regular automáticamente los recursos necesarios para satisfacer los picos de demanda, volviendo a su estado original cuando estos picos lleguen a su fin.
- Agilidad, en lo que se refiere a rapidez en el despliegue y configuración de los recursos.

- Distribución en múltiples localizaciones, generalmente, los proveedores de nube disponen de múltiples centros de datos en diferentes regiones alrededor del mundo
- Recuperación ante desastres, es posible hacer uso de la computación en la nube para el almacenamiento de copias de respaldo, o simplemente almacenar los datos generados por las aplicaciones desplegadas en la nube. Además, es posible apoyarse en la ventaja de la distribución en múltiples localizaciones y tener todos estos datos replicados, lo que hace que la recuperación ante desastres se pueda llevar a cabo de una forma efectiva llegado el caso

Por otro lado, la computación en la nube ofrece una serie de modelos de computación que se diferencian de los modelos tradicionales de infraestructura física on-premises, alojadas en algún centro de procesamiento de datos de la empresa en cuestión. Estos modelos de computación se dividen generalmente en tres:

- Infraestructura como servicio o IaaS, Infrastructure-as-a-Service: Este modelo de servicio cloud es el que más se asemeja al modelo on-premises donde se gestionan los servidores físicos directamente. El proveedor de nube es el encargado de gestionar y actualizar el hardware de los equipos, pero es el usuario final (cloud tenant) el encargado de gestionar el sistema operativo (SO) y la configuración de la red, así como todos los elementos que funcionen sobre ellos (runtime, aplicaciones, etc.). Un ejemplo claro de IaaS, es una máquina virtual desplegada en la nube.
- Plataforma como servicio o PaaS, Platform-as-a-Service: En este modelo, a diferencia del anterior, es el proveedor de la nube el que gestiona tanto el sistema operativo como la configuración de red. Es lo que se conoce como un entorno de hosting gestionado, aunque también suele denominarse entorno sin servidor (serverless), ya que no gestionamos nada relacionado con los servidores físicos, ni SO. El cloud tenant es el encargado de administrar las aplicaciones que en él se despliegan, teniendo en cuenta que el runtime empleado sea el correcto. Un ejemplo de PaaS son los hosting's usados en despliegues de aplicaciones webs como Wordpress. Nosotros simplemente debemos añadir mediante un portal web el código necesario para su ejecución en función del runtime necesario, y ya estaría listo para funcionar. Cualquier error en el código, sería nuestra responsabilidad, mientras que el proveedor de hosting es el encargado de gestionar el SO y mantener actualizados los runtimes necesarios.
- Software como servicio o SaaS, Software-as-a-Service: Este modelo se diferencia del PaaS en que la ejecución de la aplicación en sí es responsabilidad del proveedor de nube, junto con todos los elementos subyacentes que dependan de ella. El cloud tenant es el responsable de la gestión de los datos generados por la aplicación y, parcialmente, de la gestión de las identidades que permiten acceder a la aplicación. Un ejemplo claro es

la suite ofimática de Google (Docs, Sheets, Slides, etc.), la aplicación, sistema operativo e infraestructura es gestionada por Google, mientras que los datos añadidos en esa aplicación son nuestra responsabilidad, así como parte de la gestión de los accesos. Google protege contra accesos indeseados a esos datos, pero nosotros podemos hacerlos completamente públicos o concederles acceso a usuarios específicos.

Como se puede observar, existe una clara distinción de la responsabilidad por parte del proveedor de nube y del cloud tenant en cada caso, tal y como se muestra en la Figura 2. Aunque estos son los tres modelos de servicios más comunes, existen otros, que pueden entenderse como un subgrupo de los anteriores. Entre ellos encontramos; la “base de datos como servicio” o DBaaS (DataBase as a Service); el “escritorio como servicio”, o DaaS (Desktop as a Service); o “copia de respaldo como servicio” o BaaS (Backup as a Service), entre otros.

A su vez, dentro de estos modelos de servicio en la nube, podemos hacer una distinción según el tipo de nube utilizada, también conocidos como modelos de despliegue. Encontramos nubes públicas, privadas e híbridas:

- Nube pública: Los servicios se ofrecen a través de la Internet pública y están disponibles para cualquier persona que desee adquirirlos. Los recursos en la nube, como los servidores y el almacenamiento, son propiedad y están operados por un proveedor de servicios en la nube externo y se entregan a través de Internet.
- Nube privada: Una nube privada consta de recursos informáticos utilizados exclusivamente por usuarios de una empresa u organización. Una nube privada puede estar ubicada físicamente en el centro de datos de una organización, o puede estar alojada por un proveedor de servicios externo.
- Nube híbrida: Una nube híbrida es un entorno informático que combina una nube pública y una nube privada al permitir que los datos y las aplicaciones se compartan entre ellos.

Como es lógico pensar, estos nuevos paradigmas de servicios computacionales y modelos de despliegue en la nube han supuesto la aparición de nuevas amenazas y riesgos para la seguridad de la información y, consecuentemente, el surgimiento de una serie de controles específicos para mitigar dichos riesgos. Por otro lado, la adopción del cloud en organizaciones donde se requiera el cumplimiento normativo de acuerdo con una norma generalmente se complica o malinterpreta, al suponer que el proveedor es el encargado de llevar a cabo muchos de los controles que dicta la norma, o también debido a disponer de varios entornos en la nube de diferentes proveedores.

2.2. Controles de seguridad más habituales en computación en la nube

El Instituto de Tecnologías de la Comunicación (INTECO), que en 2014 pasó a denominarse Instituto Nacional de Ciberseguridad de España (INCIBE), realizó una publicación en 2011 [4] donde se recopilaron los riesgos y amenazas más habituales en el cloud computing partiendo del análisis de tres organismos, el Cloud Security Alliance (CSA), la consultora Gartner, y la National Institute of Standards and Technology (NIST). Aunque el documento de INTECO parezca anticuado, muchos de los riesgos y amenazas recopilados se siguen manteniendo a día de hoy sin prácticamente ninguna actualización.

De las tres instituciones mencionadas, la que más actividad ha mantenido en este campo y está más orientada a ello es la CSA, una organización internacional sin ánimo de lucro que promueve las mejores prácticas para garantizar la seguridad en la nube. Dicha organización dispone de varios grupos de trabajo encargados de cubrir los diferentes puntos de seguridad en la computación en la nube [5].

Entre esos grupos de trabajo, los más relevantes para este trabajo de fin de máster son: el “Thread Intelligence”, encargado de mantener actualizado y recopilados los riesgos, amenazas y vulnerabilidades en entornos cloud más habituales en una publicación denominada “Top Threads”; y el “Assesments and Audits”, encargado de elaborar y mantener la matriz de controles de nube (CCM, o “Cloud Controls Matrix”), un documento que mapea los controles con los riesgos más habituales, realizando a su vez análisis diferenciales entre los descritos en la CCM y otros estándares aceptados de la industria, regulaciones y frameworks de control como ISO 27001/27002, ISACA COBIT, PCI y NIST, entre otros.

En la última versión de la publicación “Top Threads”, publicada en septiembre de 2020 [6], se recopilaban a través de unos casos de estudio las brechas de seguridad sufridas en entornos cloud por nueve empresas de diversos sectores, entre las que se encuentran Github, Tesla y Zoom. Con cada caso de estudio, se analizaban cuáles eran las amenazas, vulnerabilidades e impacto técnico en cada caso, enlazando los controles de la CCM que podrían aplicar. Con cada caso analizado, se hace patente que las once amenazas más habituales en el cloud son las siguiente, en orden de mayor a menor magnitud:

1. Filtraciones de datos
2. Configuración incorrecta y control de cambios inadecuado
3. Falta de estrategia y arquitectura de seguridad en la nube
4. Gestión insuficiente de identidades, credenciales, acceso y claves
5. Secuestro de cuentas o (Account Hijacking)
6. Amenazas internas
7. Interfaces y API's inseguras
8. Falta de control
9. Fallas en la metaestructura y la estructura de aplicaciones

- 10. Visibilidad limitada del uso de la nube
- 11. Abuso y uso nefasto de los servicios en la nube.

Para cada una de las amenazas dentro de cada caso de estudio, se enlazan una serie de controles de la matriz de controles cloud del CSA en su versión 3.0.1. La CCM más actual en el momento de redacción de estas líneas corresponde con la versión 4.0. Cada control de la matriz está agrupado dentro de un cierto dominio y dispone de un título, un identificador numérico y una especificación ampliada. A su vez, cada control tiene asignado un “propietario” del control, según el modelo de responsabilidad compartido anteriormente mostrado, cuyos valores pueden ser CSP, CSC (Cloud Service Client o Cloud tenant) y compartido. Por otro lado, cada control dispone de un componente de aplicación (red, computo, almacenamiento, dato, aplicación o físico) y un departamento interno de la organización para el que es más relevante (auditoría interna, desarrollo, recursos humanos, operaciones, etc).

La última versión de la CCM incluye un apartado de mapeos con los controles de la antigua versión (v3.0.1) y con los controles de las normas ISO, concretamente las ISO/IEC 27001/02: 2013, ISO/IEC 27017: 2015 e ISO/IEC 27018: 2019, incluyendo un análisis diferencial con los controles de dicha norma.

Partiendo de las once amenazas listadas anteriormente y de la publicación del “Top Threads” con los casos de estudio, podemos extraer cuales son los controles cloud de la CCM más habituales, ver Tabla 1.

Como se puede observar, y según indica Gartner [7] con su previsión para el 2025, muchos de esos controles buscan crear una serie de políticas y procedimientos, y con ello, favorecer el cumplimiento normativo y evitar fallas de configuración por parte del CSC.

ID del control	Dominio	Especificación del control
SEF-02	Gestión de incidentes de seguridad, descubrimiento electrónico y análisis forense en la nube Gestión de incidentes	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la gestión oportuna de incidentes de seguridad.
TVM-02	Gestión de amenazas y vulnerabilidades Gestión de vulnerabilidades / parches	Se establecerán políticas y procedimientos, y se implementarán procesos de apoyo y medidas técnicas, para la detección oportuna de vulnerabilidades dentro de las aplicaciones de propiedad o administradas por la organización, la red de infraestructura y los componentes del sistema para garantizar la eficiencia de los controles de seguridad implementados.
IAM-02	Gestión de identidad y acceso Ciclo de vida de credenciales / Gestión de aprovisionamiento	Se establecerán políticas y procedimientos de acceso de usuario, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para asegurar su identidad apropiada, el derecho y la gestión de acceso para todos los usuarios corporativos y clientes internos (inquilino), con acceso a los datos.
AAC-02	Garantía de auditoría y cumplimiento Auditorías independientes	Se deben realizar revisiones y evaluaciones independientes al menos una vez al año para asegurar que la organización aborde las no conformidades de las políticas, estándares, procedimientos y obligaciones de cumplimiento establecidos.
CCC-03	Control de cambios y gestión de la configuración Pruebas de calidad	Las organizaciones deben seguir un proceso de prueba y control de cambio de calidad definido (por ejemplo, ITIL Service Management) con líneas de base, pruebas y estándares de publicación establecidos que se centran en la disponibilidad del sistema, la confidencialidad y la integridad de los sistemas y servicios.
HRS-09	Recursos humanos Entrenamiento / Conciencia	Se establecerá un programa de formación de conciencia de seguridad para todos los contratistas, terceros usuarios y empleados de la organización y el mandato cuando sea apropiado.

IVS-01	Seguridad de infraestructura y virtualización Registro de auditoría / Detección de intrusiones	Se requieren niveles más altos de garantía para la protección, la retención y la gestión del ciclo de vida de los registros de auditoría, adhiriéndose a las obligaciones de cumplimiento legales, reglamentarias o reglamentarias aplicables y proporcionando responsabilidad de acceso de usuario única para detectar comportamientos de red potencialmente sospechosos y / o anomalías en la integridad de archivos, y para respaldar las capacidades de investigación forense en caso de una violación de seguridad.
IVS-06	Seguridad de infraestructura y virtualización Seguridad de la red	Los entornos de red y las instancias virtuales deben diseñarse y configurarse para restringir y monitorear el tráfico entre conexiones confiables y no confiables.
STA-08	Gestión de la cadena de suministro, transparencia y rendición de cuentas Evaluación de terceros	Los proveedores garantizarán una seguridad de la información razonable en toda su cadena de suministro de información mediante la realización de una revisión anual. La revisión incluirá a todos los socios / proveedores externos de los que depende su cadena de suministro de información.
IAM-07	Gestión de identidad y acceso Acceso de terceros	La identificación, evaluación y priorización de los riesgos planteados por los procesos de negocio que requieren el acceso de terceros a los sistemas y datos de información de la organización deberán ser seguidos por la aplicación coordinada de los recursos para minimizar, monitorear y medir la probabilidad y el impacto del acceso no autorizado o inapropiado.
SEF-03	Gestión de incidentes de seguridad, descubrimiento electrónico y análisis forense en la nube Informe de incidentes	Los eventos de seguridad de la información se informarán a través de canales de comunicación predefinidos de manera oportuna, cumpliendo con las obligaciones de cumplimiento legales, reglamentarias o reglamentarias aplicables.
STA-02	Gestión de la cadena de suministro, transparencia y rendición de cuentas Informe de incidentes	El proveedor pondrá la información sobre incidentes de seguridad a disposición de todos los clientes y proveedores afectados periódicamente a través de métodos electrónicos

STA-09	Gestión de la cadena de suministro, transparencia y rendición de cuentas Auditorías de terceros	Los proveedores de servicios de terceros deberán demostrar el cumplimiento de la seguridad y la confidencialidad de la información, el control de acceso, las definiciones de servicio y los acuerdos de nivel de entrega incluidos en los contratos de terceros.
AAC-01	Garantía de auditoría y cumplimiento Planificación de auditorías	Se deben desarrollar y mantener planes de auditoría para abordar las interrupciones de los procesos comerciales. Los planes de auditoría se centrarán en revisar la eficacia de la implementación de las operaciones de seguridad.
DSI-02	Seguridad de datos y gestión del ciclo de vida de la información Inventario / Flujos de datos	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para inventariar, documentar y mantener los flujos de datos dentro de las aplicaciones distribuidas geográficamente
EKM-03	Cifrado y gestión de claves Protección de datos sensibles	Se establecerán políticas y procedimientos, y el apoyo a los procesos de negocio y medidas técnicas implementadas, para el uso de protocolos de cifrado para la protección de los datos sensibles en el almacenamiento, los datos de utilización (memoria) y datos en transmisión según las obligaciones de cumplimiento legal, reglamentario y reglamentario aplicables.
GRM-02	Gobernanza y gestión de riesgos Evaluaciones de riesgos de enfoque de datos	Las evaluaciones de riesgo asociadas con los requisitos de gobernanza de datos deben realizarse a intervalos planificados
HRS-07	Recursos humanos Roles y responsabilidades	Los roles y responsabilidades de los contratistas, empleados y usuarios externos deben documentarse en lo que respecta a los activos de información y la seguridad.
IVS-13	Seguridad de infraestructura y virtualización Arquitectura de red	Se implementarán medidas técnicas y se aplicarán técnicas de defensa en profundidad para la detección y respuesta oportuna a los ataques basados en la red asociados con patrones de tráfico de entrada o salida anómalos

SEF-04	Gestión de incidentes de seguridad, descubrimiento electrónico y análisis forense en la nube Preparación legal de respuesta a incidentes	Se requieren procedimientos forenses adecuados, incluida la cadena de custodia, para la presentación de pruebas para respaldar una posible acción legal sujeta a la jurisdicción pertinente después de un incidente de seguridad de la información.
--------	---	---

Tabla 1. Controles cloud más habituales

2.3. Cumplimiento normativo en la nube

El cumplimiento normativo o compliance consiste en establecer políticas y procedimientos adecuados y suficientes para garantizar que toda la empresa (incluyendo a directivos, empleados y agentes vinculados) cumple con el marco normativo aplicable. Compliance no deja de ser el resultado de que una organización cumple con sus obligaciones. Se diferencian principalmente dos tipos de obligaciones: las de obligado cumplimiento, regidas por los poderes públicos; y las de voluntario cumplimiento, como códigos de buenas prácticas a los que la sociedad se ha adherido [8].

El compliance implica, en mayor o menor medida, una serie de controles informáticos que las organizaciones deben llevar a cabo, además de otros controles de caracteres más jurídico y/o organizativo. Entre las regulaciones a las que puede tener que enfrentarse una empresa, encontramos, el Esquema Nacional de Seguridad (ENS), la ISO/IEC 27001, el PCI-DSS en materia de pagos con tarjeta, el Reglamento General de Protección de Datos (RGPD), y un largo etcétera. En las infraestructuras on-premises convencionales, es la propia organización la encargada de implementar todos los controles necesarios para el correcto cumplimiento normativo, pero cuando dicha organización usa de alguna manera la computación en la nube, la cosa varía en función del modelo de servicio utilizado y el esquema de responsabilidad compartida mostrado anteriormente. Por otro lado [9], el uso de arquitecturas multi-cloud, con varios CSP diferentes, o el uso de nubes híbridas puede dificultar en gran medida la visibilidad que la organización tiene sobre toda la infraestructura de TI, y, por tanto, la correcta aplicación de estos controles.

Un error común en cumplimiento normativo en la nube es asumir que como el proveedor de nube está certificado en la misma norma que aplica a mi organización (por ejemplo, en el Esquema Nacional de Seguridad), directamente implica que el servicio que tengo contratado con ese proveedor está en cumplimiento con esa norma por herencia, pero eso es completamente erróneo, de ahí que la matriz de controles cloud del CSA aclare qué control es de aplicación para el proveedor, cuál para el cliente y cual es compartido entre ambos.

Por todo lo anteriormente descrito es por lo que han surgido una serie de herramientas que nos facilitan llevar a cabo un control y desarrollo del cumplimiento normativo en entornos cloud. En los próximos capítulos se indican los pasos a seguir para conseguir un entorno en la nube seguro, haciendo hincapié en este tipo de herramientas que nos facilitan un correcto cumplimiento en la nube, así como la revisión de controles de configuración en general.

3. Seguridad en nubes públicas

Una vez vistas cuales son las amenazas y controles más habituales en el cloud computing podemos suponer que ya tenemos todos los elementos necesarios para desplegar soluciones en la nube pública de forma segura, pero no es así. La implementación de controles es solo una fase en el proceso de securización de la nube, y como veremos en este capítulo y los siguientes, adaptar los controles manualmente requiere de una serie de habilidades y conocimientos actualizados de las que pocas organizaciones disponen, y puedo suponer un dolor de cabeza en compañías donde se empleen múltiples proveedores de nube.

Según Gartner [10], en los últimos años las organizaciones han pasado de cuestionarse si mover o no sus cargas computacionales a la nube, a preguntarse cómo poder mantener la agilidad que ofrece la nube pero asegurando siempre la seguridad. Es por ello, la consultora propuso una guía de cuatro pasos de cómo y qué implementar para cumplir con este objetivo. Esta guía puede resumirse en la Figura 5.

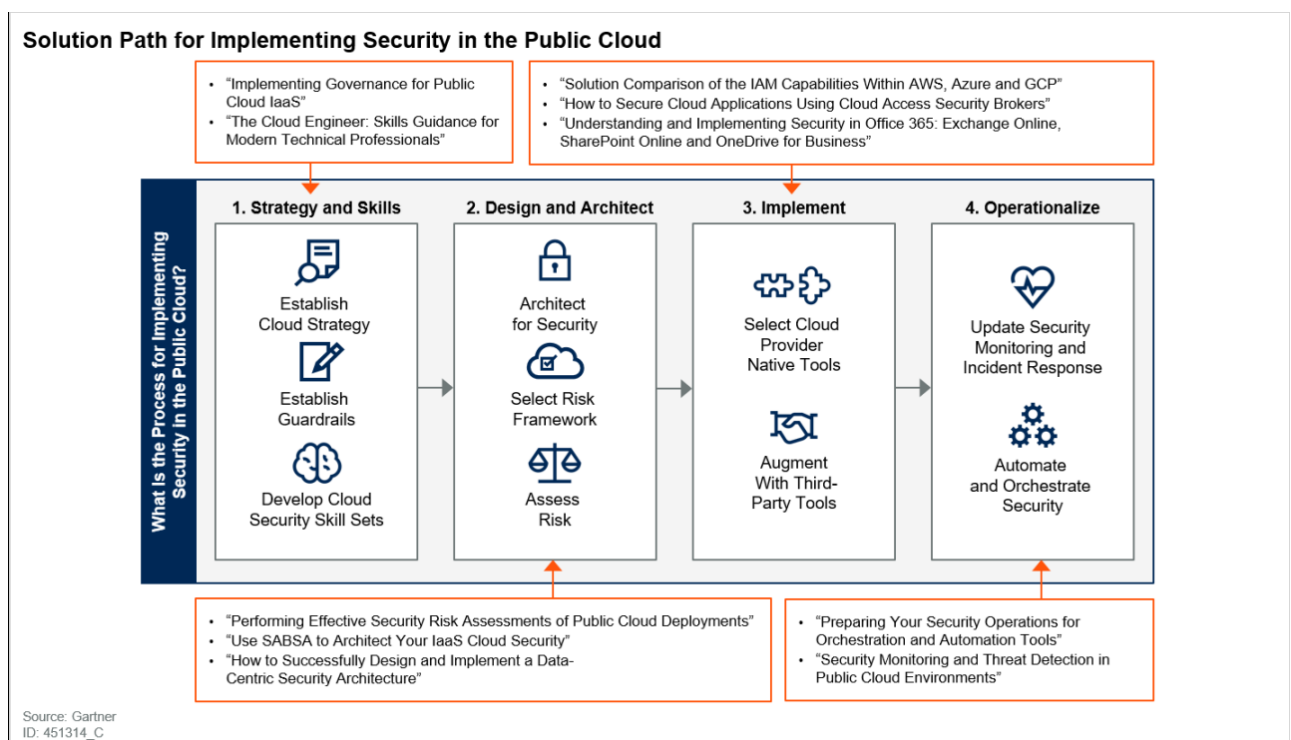


Figura 5: Ruta para implementación de seguridad en nubes públicas

3.1. Estrategia y habilidades

La primera fase trata de "Estrategia y habilidades". La organización, con el apoyo de la alta dirección y haciendo uso de políticas internas, debe desarrollar un documento de estrategia en la nube que sea entendible y seguido por toda la organización, donde se definan cuáles son los objetivos, riesgos y otros principios clave para la adopción

de la nube. También se deben establecer controles de supervisión que garanticen el correcto cumplimiento de este documento interno, y, por otro lado, asegurar el desarrollo de habilidades y conocimientos del personal en materia de seguridad en la nube.

3.2. Diseño y arquitectura

La segunda fase, entra en el terreno del “Diseño y arquitectura”. Como todo en informática, la seguridad comienza desde la fase del diseño, y en la nube no es diferente. Para desplegar una arquitectura segura en la nube se han desarrollado metodologías como SABSA (Sherwood Applied Business Security Architecture), propuesto por el NIST. Las diferentes capas de diseño y aspectos de seguridad cloud de SABSA se pueden ver en la Figura 6. En esta fase, la consultora recomienda adoptar un framework para la gestión de riesgos en nuestra organización. Puede ser un framework propio, o emplear otros ya existentes en el mercado (ISO 27001, NIST Risk Management Framework, etc.), todo dependiendo de la legislación o necesidades aplicables al sector de la organización. Estos frameworks implican una serie de catálogos de controles a implementar (ISO 27002, NIST SP 800-53, respectivamente), cuya aplicabilidad por parte del proveedor de nube o cliente depende del modelo de nube empleado, y, de nuevo, del modelo de responsabilidad compartida visto en la Figura 2.

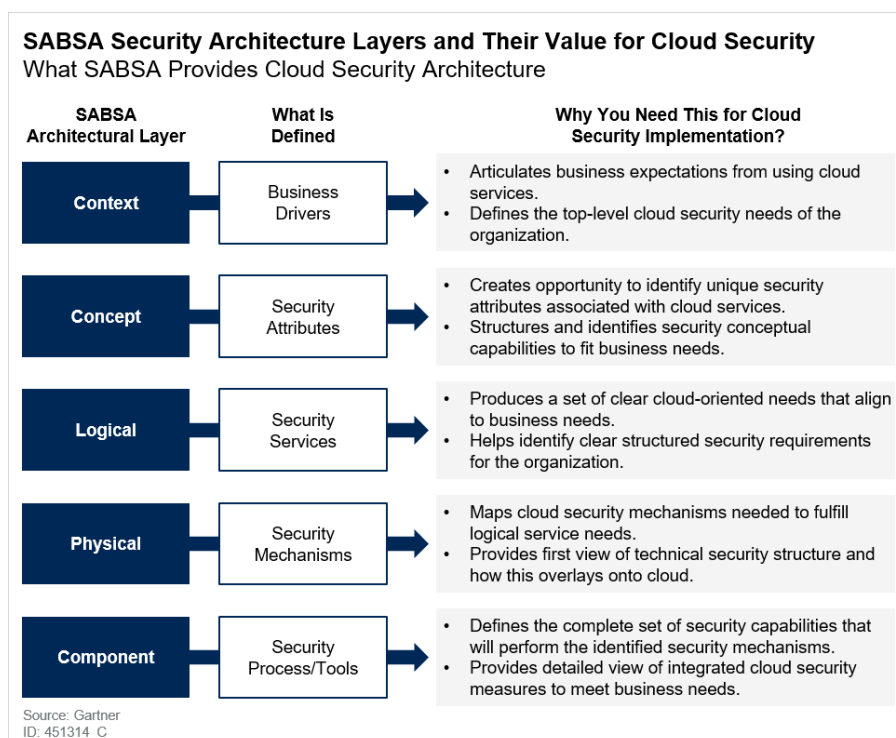


Figura 6: Arquitectura de seguridad SABSA

Una vez y hemos conseguido identificar los riesgos que afectan a nuestra organización, debemos realizar una evaluación de dichos riesgos, de manera que podamos identificar aquellos más relevantes que afecten a la organización, o

simplemente por motivos regulatorios. Este proceso de evaluación de riesgos suele consumir bastante tiempo, por lo que Gartner realizó una agrupación de proveedores de nube en tres niveles de acuerdo al nivel requerido de evaluación de riesgos de seguridad por parte de las organizaciones. Tenemos proveedores de nube:

- Tier 1: Son proveedores globales hiper escalables. Ofrecen servicios de, al menos, dos modelos de nube (IaaS, PaaS, SaaS) con un amplio catálogo de servicios genéricos para todas las verticales de negocio, de cualquier tamaño. Su público objetivo es todo el mundo. Tienen la experiencia de muchos años en el sector tecnológico.
- Tier 2: Puede ofrecer servicios de múltiples modelos de nube, pero se concentra principalmente en uno de esos modelos. Suelen estar limitados geográficamente, o a ciertas verticales de negocio. No compiten en precio con las Tier-1 pero ofrecen otras características de valor añadido como amplio soporte.
- Tier 3: Proveedores pequeños, que ofrecen generalmente SaaS, desplegados la mayor parte de las veces sobre proveedores Tier 1. Cualquiera con conocimientos básicos de programación puede ofrecer una solución SaaS básica, por lo que esta Tier es la que dispone de una mayor tasa de fallos

Es decir, una organización puede determinar los niveles de riesgo de su despliegue en la nube simplemente observando: qué modelo de nube emplea; qué tier ocupa su proveedor público de nube; cómo de importantes son los datos o servicios que en ellos se ejecutan; y qué certificaciones dispone el CSP.

3.3. Implementación

Los proveedores de nube de tipo Tier-1 están continuamente evolucionando, ampliando y mejorando sus opciones de seguridad. Que una organización se mantenga al día en estos cambios para poder seguir considerando el entorno seguro, le quita agilidad a la nube. Por ello, han surgido una serie de herramientas, tanto nativas como de terceras partes, que buscan ampliar la seguridad en un entorno tan cambiante como este.

3.3.1. Herramientas nativas

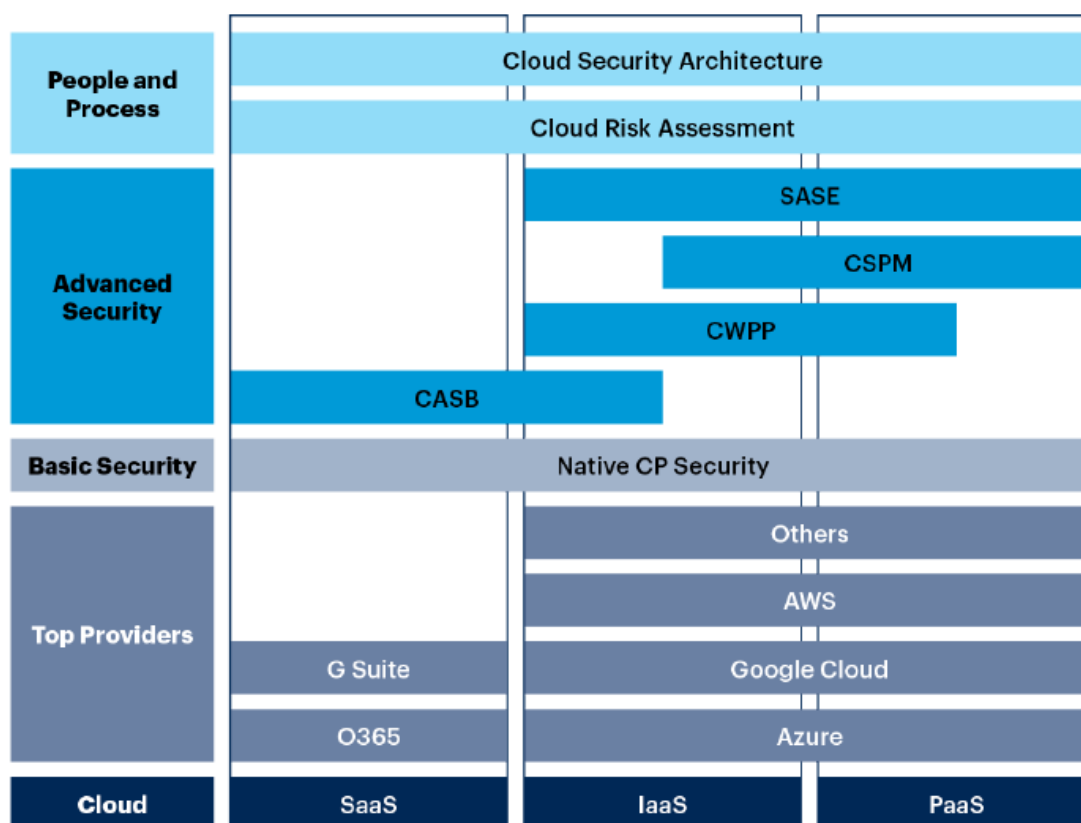
El primer paso para implementar medidas de seguridad en la nube es mediante el uso de las herramientas nativas que nos facilita el proveedor cloud. Estas herramientas cuentan siempre con el respaldo en actualizaciones y soporte del propio proveedor, ofreciendo mayores niveles de control y visibilidad en su implementación. Por otro lado, también dispone de opciones de control más detalladas para las aplicaciones, servicios, y datos alojados, además de ser soluciones que, por lo general, están incluidas en la suscripción empleada con el proveedor cloud, por lo que son más rentables. Como desventaja, estas herramientas suelen estar destinadas a un proveedor cloud específico (el que dispone la herramienta), por lo que su uso en entornos con múltiples nubes requeriría aprender y mantener tantas herramientas nativas como de proveedores disponga nuestro despliegue. Por otro lado, estas

herramientas están orientadas a todo el público en general, pudiendo haber casos de uso no contemplados por estas herramientas, pero habituales en ciertos sectores.

3.3.2. Herramientas de terceras partes

Debido a las dos últimas desventajas comentadas, surgieron las herramientas creadas por terceras partes, más orientadas a negocio, con casos de uso no contemplados por las herramientas nativas, y con soporte para la mayor parte de los proveedores de nube líderes en el mercado [11]. Estas soluciones van desde la implementación de contrafirewalls de aplicaciones web (Web Application Firewalls, WAF), y pasarelas web seguras (Secure Web Gateways, SWG), hasta otras más específicas como las descritas a continuación. Hay que tener en cuenta que muchos vendedores que ofrecen estas soluciones han combinado diferentes funcionalidades de estos conjuntos de herramientas para abarcar un mayor número de clientes al cubrir una mayor cobertura entre los diferentes modelos de cloud (ver Figura 7)

GTP Cloud Security Core Topic Coverage



Source: Gartner
720923_C

Figura 7: Cobertura herramientas cloud

Cloud Access Security Broker (CASB)

Este conjunto de herramientas están enfocadas para modelos de servicio SaaS, asegurando la protección del acceso y la seguridad de los datos para los servicios en

la nube. Ofrecen visibilidad, cumplimiento y protección contra amenazas y seguridad de los datos. Este conjunto de herramientas ofrece cuatro modelos diferentes de despliegue [12]:

- Modo API, en el que la herramienta CASB y el servicio cloud se integran directamente mediante la API del proveedor, permitiendo ver la actividad, el contenido y realizar las acciones oportunas. Usando esta técnica, se permite que las herramientas se conecten por otra vía con la nube y se permita identificar datos confidenciales, haciendo uso de diversas técnicas de inspección de contenido, eliminar el uso compartido externo que suponga cierto riesgo, cifrar archivos o revocar conexiones riesgosas de nube a nube.
- Proxy de reenvío: implementación en línea entre el dispositivo final y el servicio en la nube en la que el dispositivo o la red enrutan el tráfico al proxy CASB. El modo de proxy de reenvío proporciona controles de acceso granulares sensibles al contexto para aplicaciones en la nube aprobadas y no aprobadas
- Proxy inverso: implementación en línea entre el dispositivo final y el servicio en la nube en la que el servicio en la nube o el proveedor de identidades enrutan el tráfico al proxy CASB. Esto nos permite un control de acceso adaptativo basado en riesgos, prevención de pérdida de datos basado en inspección de contenidos en tiempo real y mayor protección frente a la descarga de archivos sensibles
- Recolector de logs: Análisis de logs desde diferentes infraestructuras (firewalls, SWG, SIEMs, ...). Generalmente se analizan los registros de actividad del usuario, pero no el contenido.

Estos modelos de despliegue pueden verse en la Figura 8.

Las características clave de las herramientas CASB, incluyen:

- Descubrimiento de aplicaciones en la nube y clasificación del riesgo
- Control de acceso adaptativo
- Protección de datos (DLP, clasificación y cifrado de datos)
- Análisis de comportamiento de usuarios y entidades.
- Protección contra amenazas
- Cifrado orientado al cliente (incluida la integración con la gestión de derechos digitales)
- Cifrado y tokenización pre-cloud
- Seguimiento y gestión de registros

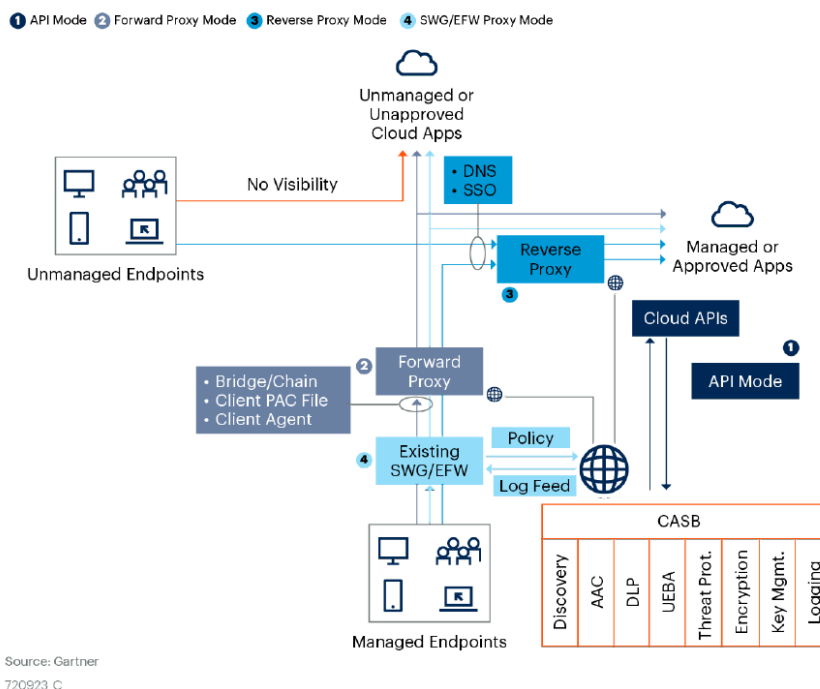
Overview of CASB Capabilities and Architecture Integration Modes


Figura 8: Arquitectura CASB

Cloud Workload Protection Platform (CWPP)

Este conjunto de herramientas está orientadas a los modelos de IaaS y PaaS, y se centran en el análisis de las cargas de trabajo, algunas de carácter más general, y otras más enfocadas a ciertas soluciones como los contenedores o modelos serverless. Estas herramientas funcionan de manera similar a las herramientas on-premises habituales, pero en la nube. En la Figura 9, Gartner compara las diferentes variantes de las herramientas CWPP.

CWPP Types and Their Minimum Capabilities

■ Attack Surface Reduction ■ Pre-Execution Protection ■ Post-Execution Protection

CWPP's "DNA Markers"/Capabilities	CWPP Variants						
	Broad Spectrum	Container-Focused	Serverless-Focused	Memory, Process Integrity Protection	Network and Micro-segmentation	EDR-Focused	Vulnerability, Hardening and Config. Compliance
Hardening and Configuration							
Host-Based Network Firewalling							
Microsegmentation							
Exploit Prevention and Memory Protection							
Vulnerability Management							
Application Control							
Privileged Account Management							
Antivirus							
Vulnerability Shielding							
Integrity Control							
User Behavior Monitoring							
Intrusion Detection/Prevention							
Workload EDR							
Autoremediation							

Figura 9: Tipos de herramientas CWPP, y capacidades mínimas

Cloud Security Posture Management (CSPM)

El último conjunto de herramientas a comentar son las CSPM, enfocadas a los modelos IaaS y PaaS. Aunque todas las herramientas citadas tienen su caso de uso concreto y se pueden complementar unas con otras, lo cierto es que las CSPM son las que más sentido tienen a la hora de asegurar un entorno cloud, pues atacan directamente a la amenaza más típica en estos entornos: los errores de configuración, además de disponer de otras muchas funciones. Por esta razón, como veremos en el próximo capítulo, son muchos los fabricantes de herramientas CASB y CWPP propietarias que han decidido integrar funciones CSPM en sus herramientas, ya que, con ello, amplían la cobertura de los modelos cloud cubiertos y constituyen una solución de seguridad más completa para entornos empresariales.

Estas herramientas CSPM se justifican en las organizaciones cuando se emplean IaaS/PaaS en múltiples nubes, o se opera en un sector con altos requisitos de cumplimiento normativo.

Las funcionalidades que ofrecen este conjunto de herramientas van más allá de la evaluación de configuraciones de seguridad. Proporcionan capacidades de gestión y aumentan la visibilidad en la nube que tienen las organizaciones. De forma más extendida, las herramientas CSPM generalmente ofrecen las siguientes características:

- Evaluación de cumplimiento: Estas herramientas se encargan de revisar el entorno cloud desplegado y comparan la configuración respecto a las mejores

prácticas, pudiendo hacer uso de guías de refuerzo como la del CIS [13] o respecto a otros marcos regulatorios.

- **Monitoreo operativo:** se encarga de recopilar logs de los diferentes entornos cloud en tiempo real y alertar en función de ciertos disparadores, lo que facilita la labor de los centros de operaciones de seguridad (SOC) y los equipos de incidentes.
- **Integración DevOps:** Estas herramientas puedes disponer de una API que analice los despliegues realizados y se informe de configuraciones que supongan algún riesgo.
- **Respuesta a incidentes:** proporcionan capacidades para manejar y mitigar incidentes.
- **Identificación de riesgos:** Partiendo de la información de monitoreo y cumplimiento, es capaz de identificar y priorizar los riesgos más relevantes en el entorno desplegado
- **Automatizar la corrección de determinados riesgos de seguridad:** Estas herramientas pueden realizar las modificaciones necesarias para remediar una configuración incorrecta y mitigar el riesgo producido.

Estas herramientas se integran con las API de los proveedores cloud para obtener los datos de configuración y eventos, permitiendo la escritura/modificación de ciertos parámetros para automatizar la corrección de configuraciones y evitando de esta manera el uso de agentes externos para la conexión [14].

Typical Multicloud Use Case for CSPM

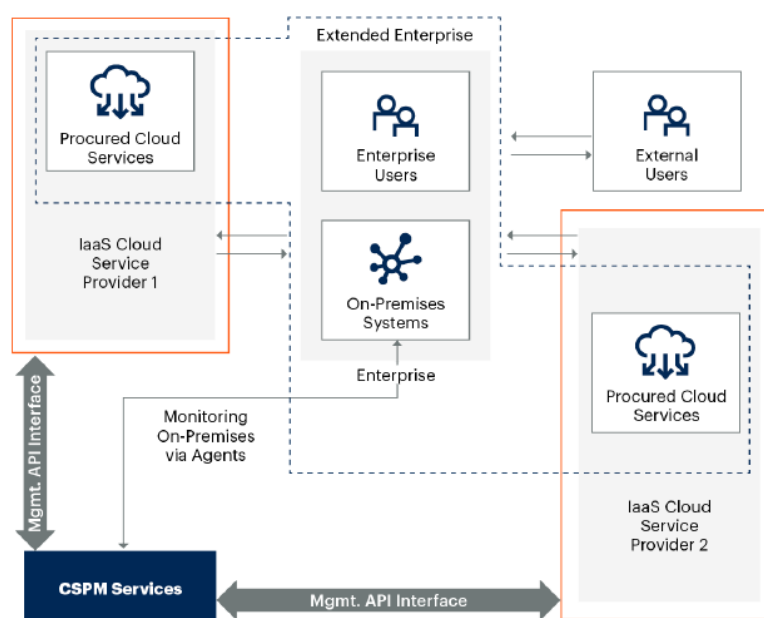


Figura 10: Caso de uso típicos para CSPM

Algunas de las configuraciones erróneas que las herramientas CSPM pueden llegar a detectar, son:

- Cuentas con amplios privilegios y cuentas con ciertos permisos habilitados pero que no hacen uso de ellos. Los desarrolladores a menudo proporcionan cuentas y servicios con más permisos de los necesarios para acelerar el desarrollo y reducir los problemas de ejecución, pero esto aumenta el riesgo.
- Cuentas y servicios donde no se utilizan métodos de autenticación multifactor.
- Conectividad de red excesiva o mal configurada. Las nubes públicas permiten la microsegmentación de forma predeterminada para hacer cumplir el principio de privilegios mínimos. La conectividad de red debe proporcionarse al mínimo necesario (también conocido como red de confianza cero)
- Servicios con conectividad directa a Internet.
- SSH / RDP para gestión remota expuesto directamente a Internet.
- Almacenamiento de datos expuestos directamente a Internet.
- Almacenamiento de datos y archivos compartidos que se comparten de manera no controlada.
- Servicios de almacenamiento de datos / bases de datos no cifradas
- Uso inadecuado de la gestión de claves de cifrado.
- Claves / certificados caducados o próximos a caducar.
- Servidores web externos sin el uso de WAF o balanceador de carga.
- API expuestas directamente a Internet.

Aunque las herramientas CSPM cubren las amenazas más explotadas en la nube, disponen de una serie de limitaciones, como:

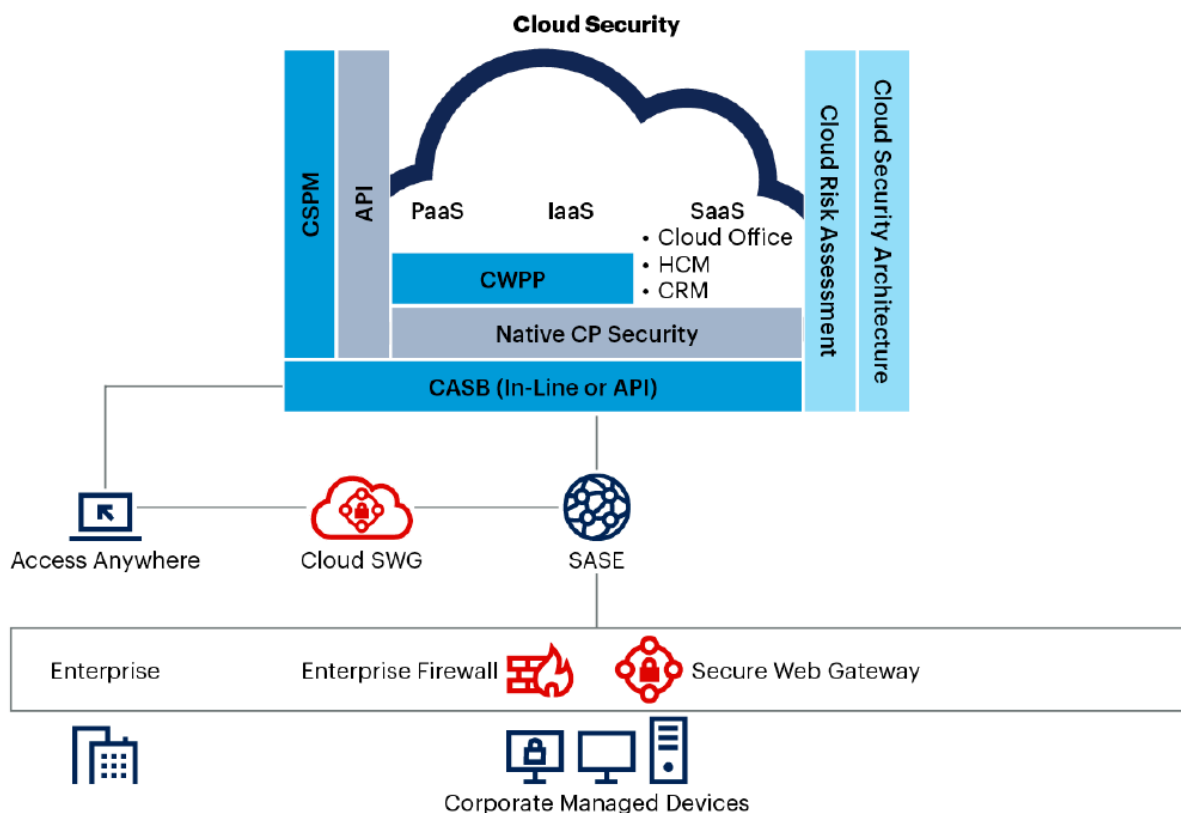
- Visibilidad. No se puede gestionar lo que no se ve. Se debe controlar que las herramientas CSPM tienen visión de toda la infraestructura/suscripciones a cubrir
- Precio excesivo. Debido a la inmadurez del mercado, los modelos de precios son muy variables. A esto se le suma que muchas empresas combinan estos tipos de herramientas con otras como CASB, incrementando el precio del producto, así como sus funcionalidades ofrecidas.
- El CSP líder en el sector empresarial actualmente es AWS, por lo que muchas herramientas propietarias se han centrado en este proveedor, dejando de lado o abordando en menor medida otras grandes como Azure o GCP, y mucho menos Alibaba, Oracle, entre otros. +
- Pueden existir puntos de ciegos que no cubra una solución CSPM y se cree una solución de falsa seguridad
- Falta de contexto de datos. Muchas soluciones de CSPM no comprenden el contexto de los datos, por lo que no se puede determinar correctamente el nivel de riesgo.
- Falta de búsqueda de vulnerabilidades en las cargas de trabajo. Si suponemos que está todo bien configurado, pero a la aplicación que estamos ejecutando le falta un parche de seguridad crítica, esto no será detectado por una herramienta CSPM
- Las CSPM están enfocadas a trabajar cuando ya todo se ha implementado en la nube, lo que origina un pequeño slot no cubierto por la herramienta. Además,

muchas organizaciones son reacias a automatizar la toma de decisiones por estas herramientas, por lo que aumenta la exposición [14].

- Aunque se pudiera automatizar gran parte de las incidencias detectadas por estas herramientas, sigue siendo necesario la supervisión por algún técnico capacitado que analice las alertas y se encargue de remediar aquellas configuraciones que supongan un riesgo.

Tras ver las limitaciones de las CSPM, se comprende como la seguridad en la nube no depende de una única solución, sino de la combinación de varias de estas herramientas, lo que justifica en gran medida las adquisiciones que están llevando a cabo grandes empresas en seguridad, integrando y combinando muchas de estas herramientas y ofreciendo un producto integral que abarque lo máximo posible, con las mínimas limitaciones [15]. En la Figura 11 se muestra cómo quedarían todas estas herramientas funcionando en un despliegue cloud.

Cloud Security Logical Architecture



Source: Gartner
720923 C

Figura 11: Arquitectura lógica para seguridad en la nube

3.4. Operacionalizar

Una vez y tenemos las herramientas que nos ayudarán a prevenir y detectar ataques, debemos monitorizar dichas herramientas, de manera que podamos responder ante

los posibles incidentes cuando ocurran. En general, las soluciones de monitorización orientadas al cloud persiguen los mismos puntos que las soluciones on-premises:

- Detección de amenazas, llevando a cabo monitorización de ataques, revisión de accesos no autorizados y otros problemas de seguridad que pudieran ocurrir.
- Respuesta e investigación ante incidentes de seguridad, facilitando la captura de datos para su posterior análisis ante algún incidente
- Cumplimiento regulatorio, llevando a cabo todos los requerimientos de monitoreo que exija un determinado framework regulatorio (por ejemplo, todas las elevaciones de privilegios a usuarios deben registrarse durante al menos un año).

Estas soluciones de monitorización pueden estar: desplegadas dentro del propio cloud a monitorizar; on-premise; fuera del entorno a monitorizar, pero en el mismo proveedor cloud; o en terceras partes externas al entorno a monitorizar.

El último punto a la hora de operacionalizar el despliegue cloud consiste en la automatización y orquestación de los procesos y procedimientos de seguridad. Dado al gran número de amenazas que sufre la red, cada vez más en aumento, es imposible monitorizar y gestionar todas a mano, por lo que la automatización y orquestación se hacen más que necesarias. Para ello, se pueden implantar soluciones como SOAR (Security orchestration, automation and response), que permiten a las organizaciones recoger las entradas de varias fuentes y aplicar workflows alineados por los procesos y procedimientos de la organización.

4. Herramientas Cloud Security Posture Management

A continuación, se analizan algunas de las diferentes herramientas CSPM que podemos localizar en el mercado, agrupadas en tres grandes grupos: las herramientas propias incorporadas por cada CSP, a las cuales se accede generalmente mediante el propio portal web de cada proveedor y proporcionan una seguridad básica; las herramientas de código abierto disponibles, que suelen requerir de la instalación de la herramienta en alguna máquina on-premise o IaaS en la nube; y por último, las herramientas propietarias, que disponen de algún tipo de pago por suscripción y cuyo código no es accesible al público. Estas últimas herramientas generalmente vienen en formato SaaS, accediendo a ellas a través de un portal web del propio fabricante de la herramienta.

4.1. Herramientas propias

Para el análisis de estas herramientas propias, se han elegido las ofrecidas por los tres CSP líderes del mercado, es decir, las ofrecidas por Amazon Web Services, Microsoft Azure y Google Cloud Platform [3]. Eso no significa que el resto de los proveedores de nube no dispongan de este tipo de herramientas, Alibaba Cloud, por ejemplo, dispone del servicio Security Center, que realiza muchas de las funciones de sus competidores, al igual que Oracle Cloud Infraestructura (OCI), y su herramienta de seguridad.

4.1.1. AWS Security Hub

AWS Security Hub [16] es un servicio en la nube de AWS que nos permite ver de manera integral las alertas de seguridad de alta prioridad y el estado de cumplimiento en todas las cuentas de AWS vinculadas. Permite recopilar en un solo lugar los registros y alertas generados por otros servicios de AWS (AWS Config, Inspector, etc) y visualizar mediante gráficos y tablas los resultados obtenidos. También nos permite monitorizar continuamente nuestra infraestructura desplegada y revisar desviaciones en el cumplimiento respecto a estándares líderes del sector y otras guías de buenas prácticas como el CIS Benchmark para AWS. En la Figura 12, se observa como es el funcionamiento de esta herramienta.



Figura 12: Funcionamiento de AWS Security Hub

Entre las características más importantes, encontramos:

- Consolidación de todos los hallazgos encontrados por los servicios de AWS e integraciones de terceros. Esta herramienta emplea un formato de resultados llamado AWS Security Finding Format (ASFF) que permite el intercambio de hallazgos entre distintas plataformas. Entre dichas plataformas encontramos proveedores como PaloAlto, Aqua Security, entre otros.
- Comprobaciones continuas de seguridad basándose en guías de buenas prácticas o estándares del sector (como PCI DSS). Security Hub nos señala cual es el problema o desviación y los pasos necesarios para remediarlo.
- Se integra con Amazon CloudWatch, y permite crear flujos de respuesta y corrección personalizados, enviando los hallazgos al SIEM, SOAR u otras herramientas. Para crear los flujos de reparación automatizados es necesario programarlos usando otros servicios como AWS System Manager Automation o AWS Lambda.
- Soporte para múltiples cuentas de AWS
- Facilita la revisión de configuraciones erróneas (o mejorables) en materia de seguridad de los servicios vinculados a dicha cuenta
- Permite revisiones de políticas propias contra recursos, basándose en etiquetas. Por ejemplo, si tenemos una IaaS marcada con la etiqueta “producción”, puede conllevar que ciertas medidas de seguridad apliquen a dicho recurso.
- Dashboard para la visualización de los problemas de cumplimiento y configuraciones.

Como podemos observar, este servicio tiene las siguientes desventajas frente a las características de las herramientas CSPM indicadas en el capítulo anterior:

- AWS Security Hub, en su formato standalone, no es compatible con otros proveedores de nube distintos a AWS (sin soporte multicloud), sino que necesita de la integración de herramientas de terceras partes (ver AWS Security Hub Partners [17]) para la revisión de esos otros despliegues.
- Simplemente señala cuales son las configuraciones erróneas o desviaciones en el cumplimiento, indicando los pasos para remediarlo, pero no incorpora herramientas de remediación automatizadas, sino que debemos realizarlas nosotros, o programarlas mediante algún servicio externo.
- El número de estándares de cumplimiento que revisa no es tan alto como el de sus competidores.

4.1.2. Azure Security Center

El Azure Security Center [18] es un sistema unificado de administración de seguridad de la infraestructura, que fortalece la posición de seguridad de los centros de datos y proporciona una protección contra amenazas avanzada para todas las cargas de trabajo híbridas que se encuentran en la nube, estén en Azure o no. Esta herramienta

nos permite proteger la red, servicios, y garantizar el cumplimiento normativo y seguridad en la nube.

Como se observa por su definición, no es una simple herramienta CSPM, sino que incluye otras funcionalidades más típicas de herramientas CWPP como son la protección de las cargas de trabajo.

Entre sus características más notables, tenemos:

- Es compatible con la nube híbrida. Permite monitorizar no solo la infraestructura creada en Azure sino también los equipos on-premises mediante la instalación de un agente propio en las máquinas (Linux/Windows).
- Permite la conexión de otros proveedores de nube como AWS y GCP, sin necesidad de integraciones con software de terceras partes.
- Permite la creación de directivas para reforzar las configuraciones de seguridad, aplicable a todos los elementos bajo su alcance (servicios propios de Azure, on-premises y de otras nubes)
- Facilita la visibilidad en la nube, informando de las suscripciones que están cumpliendo con las políticas de seguridad y cuales están fuera de ellas.
- Permite evaluaciones continuas, detectando los nuevos recursos creados y comprobando las configuraciones realizadas respecto a procedimientos recomendados de seguridad. Entre estas guías, encontramos una propia de Azure (Security Benchmark) y otros marcos de cumplimiento como los propuestos por el NIST y por CIS.
- Creación de un mapa de red visual (Figura 13) donde se contemplan todos los recursos en alcance por la herramienta
- Recomendaciones ante fallas de seguridad o en configuraciones, facilitando las instrucciones detalladas de cómo solucionar cada vulnerabilidad.
- Es capaz de proteger contra amenazas en todos los recursos bajo su alcance, incluidos en los PaaS de Azure
- Se integra con Microsoft Defender
- Permite bloquear los ataques de fuerza bruta habilitando diferentes tipos de acceso como el "just-in-time", solo cuando sea necesario, o limitando las direcciones IP que pueden conectar con ciertos recursos
- Permite clasificar los datos en Azure SQL y Azure Storage de forma automática según su grado de protección (DLP)
- Detecta e incorpora todos los nuevos recursos creados en Azure, aplicando las políticas correspondientes

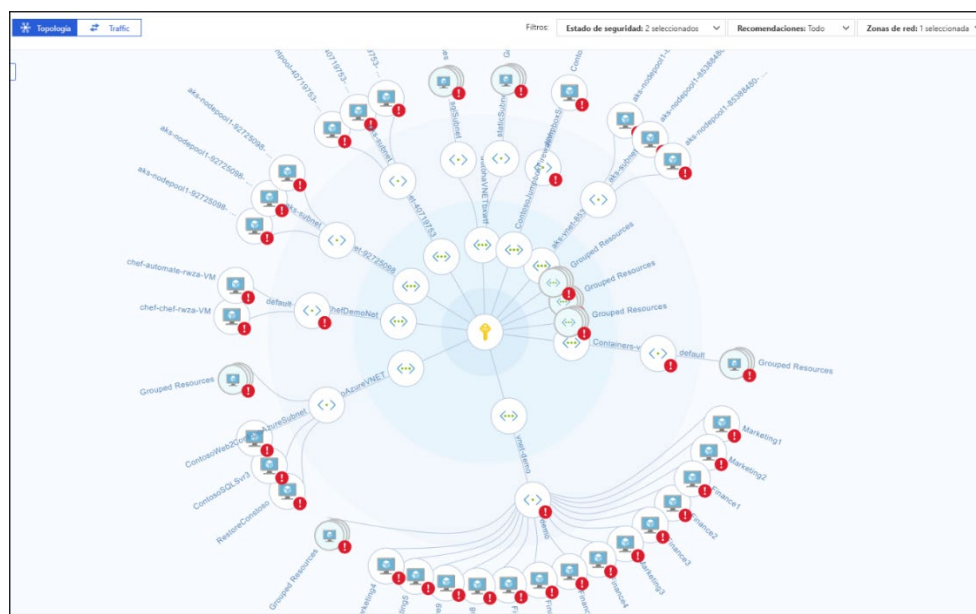


Figura 13: Mapa de red creado por Azure Security Center

4.1.3. Google Cloud Security Command Center

El servicio Google Cloud Security Center se define como una plataforma de gestión de riesgos y seguridad [19] para la nube de Google. Ofrece una mejor visibilidad y control centralizados, detectando errores de configuración y vulnerabilidades y facilitando el cumplimiento normativo, facilitando todas las recomendaciones necesarias para resolver los posibles errores. También es capaz de detectar las amenazas que ponen en riesgo los recursos desplegados, usando incluso herramientas a nivel de kernel, con soporte para contenedores.

Este servicio se ofrece en dos niveles, el estándar y el premium. En función del nivel elegido, habrá unas características u otras. Todas las características del nivel estándar están incluidas en el nivel premium.

Entre las características principales, tenemos:

- Descubrimiento e inventario de recursos, lo que permite conocer en tiempo real los recursos desplegados en la nube de Google, así como los recursos modificados o eliminados
- Prevención de amenazas, detectando las vulnerabilidades más habituales y ayudando a corregir las configuraciones erróneas detectadas y facilitando guías paso a paso para solventar los errores. En el nivel estándar las configuraciones detectadas son las básicas más habituales (puertos SSH/RDP abiertos, instancias SQL abiertas, etc.), pero en el nivel premium incluye otras guías de buenas prácticas y estándares como CIS 1.0, PCI DSS v3.2.1, NIST 800-53 e ISO 27001.
- Detección de amenazas. Utilizando los registros generados por los servicios es capaz de identificar amenazas y de detectar algunos ataques a

contenedores como la ejecución de binarios dañinos, uso de bibliotecas sospechosas y shell's inversos.

- Análisis de los sistemas de almacenamiento en busca de datos sensibles para su clasificación (DLP)
- Detección de anomalías como credenciales filtradas o uso de recursos para minería de datos
- Integración con herramientas de terceras partes (PaloAlto, McAfee, etc.) mediante API.
- Monitoreo continuo y avisos por SMS/email
- Supervisión del control de acceso mediante el uso de políticas.

Por sus características, podemos ver cómo nos encontramos ante una herramienta con funciones CSPM, además de incorporar otras más habituales de las CWPP.

4.2. Herramientas Open Source

En este apartado, se analizan las soluciones CSPM de código abierto disponibles. Estas herramientas, como las propietarias, no son herramientas propias del proveedor de nube, por lo que necesitan de una serie de credenciales para poder acceder a la nube y leer o modificar las configuraciones. Para hacer esta acción, hacen uso del SDK del proveedor que permite acceso de programación a la plataforma. Esas herramientas, por lo general, se pueden ejecutar en infraestructura on-premises, IaaS en la nube, contenedores de Docker e incluso en modo serverless en algunos casos.

En los servicios en la nube que suelen revisar, entran casi todos los productos IaaS y PaaS más habituales de cada proveedor.

Durante la etapa de documentación de este trabajo final de máster, se encontraron las herramientas de código abierto de la Tabla 2.

De entre todas las herramientas descritas, se decidió analizar la solución más madura, CloudSploit. Esta herramienta, como se comenta en la tabla, es compatible con los 3 CSP líderes del mercado y detrás de su desarrollo se encuentra la compañía Aqua Security [20], que dispone de otra herramienta CSPM propietaria en formato SaaS. Además, frente a otras soluciones open source, dispone de guías para el desarrollo de extensiones (o políticas) que nos permiten crear nuestros propios controles a revisar; y guías de remediación, que nos permite indicar paso a paso qué modificaciones debemos realizar, ya sea de manera automática o manual, para solventar los errores de configuración.

Tabla 2: Herramientas CSPM de código abierto

Herramienta	Características principales	Estándares y configuraciones revisados	CSP soportados
CloudSploit	Interacción por CLI Soporte para instancias de AWS gubernamentales y china Amplia variedad de formatos de salida Junit, CSV, entre otros Guía de desarrollo de extensiones y guía de remediación	HIPAA, PCI DSS, CIS Benchmark Level 1 & 2	AWS, GCP, Azure, Oracle Cloud Infrastructure
OpenCSPM	Interfaz web para la gestión y muestra de resultados Creación de políticas propias Sistema de notificaciones en caso de desviaciones en cumplimiento	CIS Benchmarks, NIST 800-53 & 171, FedRAMP, PCI DSS, HIPAA y los propios de cada GCP	AWS, GCP
kube-bench	Testeo de configuraciones de Kubernetes respecto a la guía CIS (no es compatible con otro tipo de servicios)	CIS Kubernetes Benchmark	GCP, AWS, Azure, entre otros.
Prowler	Más de 180 controles disponibles Reports en formato HTML, CSV, ASFF, entre otros. Creación propia de controles	PCI-DSS, ISO27001, FFIEC, SOC2, ENS, HIPAA, GDPR, CIS level 1 & 2	AWS
Cloud Custodian	Gestión de configuraciones en tiempo real en base a políticas Gestión de inventario en la nube y costo Gestión de políticas por etiquetas Amplia comunidad	N/A, análisis en base a políticas. La comunidad puede haber creado políticas estándar en base a requerimientos de estándares	AWS, GCP, Azure

4.3. Herramientas propietarias

Durante la búsqueda de herramientas propietarias CSPM para el desarrollo de este trabajo final de máster, se localizaron unas 30 de diferentes fabricantes/desarrolladores. En la Tabla 3 se puede ver algunas de ellas con enlaces a la web del fabricante y un listado simplificado de todas sus características.

La mayoría de estas herramientas tienen soporte multi-nube, siendo posible su uso con cualquiera de los tres CSP líderes del mercado (AWS, GCP y Azure). Algunas de ellas incluyen soporte para otros CSP como Alibaba Cloud, OCI, con soporte para Kubernetes, e incluso, con soporte para la nube híbrida.

En cuanto a sus características, hay que comprender que muchas de estas herramientas no son simples CSPM, sino que suelen ir integradas en otras soluciones mayores (denominadas Cloud Security Platforms), o integran funcionalidades más propias de un CWPP o CASB. Si no centramos únicamente en las funcionalidades CSPM, vemos que todas facilitan la visibilidad y la gestión de recursos entre las diferentes nubes públicas (inventariado), hacen auditorías o comprobaciones de las configuraciones de seguridad frente a las mejores prácticas del mercado (CIS Benchmak, DISA STIG, etc.) y disponen de plantillas para analizar el cumplimiento normativo de nuestra infraestructura, además de algún tipo de sistema de auto remediación para solventar las configuraciones inseguras o el no cumplimiento.

En varias de las webs de producto analizadas, se ha comprobado que muchas de ellas no disponen de una hoja de producto (datasheet) lo suficientemente detallada, con los servicios de nube analizados y más concretamente, con los controles revisados en cada uno de esos servicios. Este punto es clave, pues es el que determina la precisión de esta herramienta y que se pueda adaptar o no a las necesidades de una organización. Este aspecto influye también en el apartado de cumplimiento normativo, pues las plantillas que analizan el cumplimiento simplemente enlazan un control del estándar a cumplir (como ISO 27001), con una serie de controles en la configuración de esos servicios, por lo que, si el listado de servicios y controles es amplio, mayor será el nivel de detalle y certeza en el cumplimiento de esa norma.

Por tanto, para elegir entre una u otra herramienta, primero se deben analizar bien los requisitos de nuestra organización, y luego, solicitar una prueba a las diferentes fabricantes para asegurar que dicha herramienta cumple con los requisitos. Casi todas las webs (y productos) analizadas disponen de un apartado de solicitud de versión de prueba.

Tabla 3: Herramientas CSPM propietarias

Herramienta	Proveedor	CSP soportados	Características
Zscaler Cloud Security Posture Management	Zscaler	AWS, GCP, AZ	Módulo dentro de una plataforma de gestión cloud mayor Revisión de configuraciones incorrectas de la nube Visibilidad unificada Automatización de remediación de seguridad Informes de cumplimiento y remediación para NIST, PCI, SOC2, ISO, HIPAA, GDPR, entre otros Previene las vulnerabilidades de las aplicaciones
DivvyCloud	Rapid7	AWS, GCP, AZ, Alibaba	Cumplimiento normativo (PCI DSS, HIPAA, GDPR, SOC 2, ISO 27001, CIS, NIST CSF, NIST 800-53, FedRAMP, CCM CSA) Inventario / visibilidad de activos Gestión de usuarios y permisos Comprobación de configuraciones incorrectas+
McAfee Mvision CNAPP	McAfee	AWS, GCP, AZ	CWPP con funcionalidades CSPM Visibilidad en la nube Análisis de configuraciones inseguras contra las mejores prácticas y evaluación de vulnerabilidades Automatización de controles de seguridad Cumplimiento normativo
Cloudsploit / Aquawave	Aqua Security	AWS, GCP, AZ, OCI	Auditoría continua de las configuraciones de acuerdo con guías de buenas prácticas como el CIS Benchmark Remediación automática de anomalías detectadas Creación de políticas de seguridad para evitar despliegues con configuraciones inseguras Informes de cumplimiento normativo como PCI-DSS, HIPAA, GDPR, entre otros. Control de eventos en tiempo real Integraciones con SIEM y otras herramientas de terceros

			API REST para integraciones Alternativa OpenSource disponible
Prisma Cloud	PaloAlto	AWS, GCP, AZ, OCI, Alibaba Cloud	Visibilidad en la nube Gestión del cumplimiento normativo en PCI, NIST, HIPAA, RGPD, CIS, SOC2, entre otros Detección de amenazas Respuesta a incidentes Corrección automática de incidentes
Conformity	Trend Micro	AWS, AZ	Visibilidad completa en la nube y resolución automática de configuraciones inseguras. Compatible con más de 750 prácticas recomendadas sobre configuraciones de infraestructura en la nube, en más de 85 servicios de AWS y Microsoft Azure. Comprobaciones de cumplimiento de normativa y seguridad automatizadas, con cientos de controles de prácticas recomendadas del sector, incluidas SOC2, ISO 27001, NIST, CIS, GDPR, PCI DSS, HIPAA, AWS y Azure Well-Architected Frameworks, y CIS Microsoft Azure Foundations Security Benchmark Múltiples integraciones con terceros
CLOUD OPTIX	Sophos	AWS, GCP, AZ	CWPP con funcionalidades CSPM Escaneos de seguridad configurables Evaluaciones de políticas de prácticas recomendadas de seguridad (Personalizadas, pruebas comparativas de CIS, ISO 27001, prácticas recomendadas de Sophos, EBU R 143, FEDRAMP) Remediación automática Detección de anomalías en: tráfico de red; comportamiento de inicio de sesión del usuario; eventos de alto riesgo; y credenciales comprometidas Escaneados de cumplimiento configurables Evaluación de políticas de prácticas recomendadas de cumplimiento (Personalizada, FIEC, RGPD, HIPAA, PCI DSS, SOC2) Supresión de alertas (Oculte alertas con una simple casilla de verificación) Gestión de excepciones de cumplimiento (Las alertas suprimidas se aplican a futuros escaneados)

			Aumento de visibilidad en la nube Integraciones de terceros
Netskope: Seguridad en la nube pública	Netskope	AWS, GCP, AZ	Combina protección en línea basada en API y en tiempo real para proteger las implementaciones de nube públicas Evalúa la vulnerabilidad y los riesgos conforme a los estándares del sector y la conformidad normativa, como las referencias CIS, NIST, PCI-DSS, HIPAA, etc. Puede corregir y remediar automáticamente errores de configuración habituales detectados por Netskope (p. ej., eliminar el acceso a internet de los grupos de seguridad). Proporciona una consola única con controles de política unificados en AWS, Azure y GCP
CloudSOC	Broadcom (Symantec)	AWS, GCP, AZ	Es un CASB con funcionalidades tanto de CWPP como de CSPM. Las funciones de CASB solo están disponibles en AWS y AZ. Es compatible con los estándares de cumplimiento habituales (ISO, FISMA, NIST SP-800-53, SOX, PCI, e HIPAA, entre otros). Es capaz de identificar fallas de configuración y efectuar remediaciones

5. Fase práctica

En esta fase del Trabajo de Fin de Máster se pretende crear un laboratorio de prueba con los principales proveedores de nube pública, dando de alta servicios de tipo IaaS y PaaS para poner a prueba diferentes herramientas CSPM seleccionadas.

5.1. Selección de proveedores cloud y despliegue de entorno de prueba

El primer paso, sería elegir en qué CSP desplegar nuestro laboratorio. Para ello, nos hemos basado en el cuadrante mágico de Gartner de septiembre de 2020, que analiza las plataformas de servicios cloud [3], determinando a través de varios factores cuáles son los CSP líderes, visionarios, desafiantes, y “de nicho” existentes (ver Figura 14). Por ello, hemos seleccionado a Amazon Web Services, Microsoft Azure y Google Cloud Platform para desplegar nuestro laboratorio en la nube, pues son los CSP líderes en el momento de realizar dicho análisis.



Figura 14: Cuadrante mágico de Gartner de proveedores cloud públicos

En los 3 proveedores elegidos, disponemos de una capa gratuita por tiempo o importe limitado, por lo que se procurará realizar el laboratorio dentro de los límites establecidos por la capa gratuita para evitar costes adicionales.

También se dispondrá de una máquina virtual Linux en la que instalar aquellas herramientas CSPM que no son ofrecidas en modalidad SaaS y requieren su instalación en un equipo (aunque podría instalarse perfectamente sobre una de las plataformas Cloud seleccionadas)

Para probar algunas herramientas propietarias, se ha elegido la solución de Palo Alto, distribuida en modalidad SaaS, por ser una de las que mejor características ha presentado durante la búsqueda de herramientas y por disponer de un trial gratuito durante 30 días, que nos da acceso a la totalidad de la plataforma.

Para las pruebas de herramientas OpenSource, se ha elegido CloudSploit, por ser la solución de código abierto de otra herramienta propietaria de Aqua Security y por ser una de las más maduras a día de hoy.

También se probarán algunas de las soluciones nativas CSPM disponibles en los proveedores cloud, como Azure Security Center y AWS Security Hub.

En la Figura 15 se muestra el despliegue realizado en los diferentes clouds. Cada uno de los servicios usados se define brevemente en los siguientes subapartados y se forzarán configuraciones defectuosas para comprobar si son detectadas y solventadas por las herramientas CSPM. Los servicios marcados en rojo son las soluciones CSPM nativas descritas de cada proveedor, ya descritas anteriormente.

Fase práctica TFM

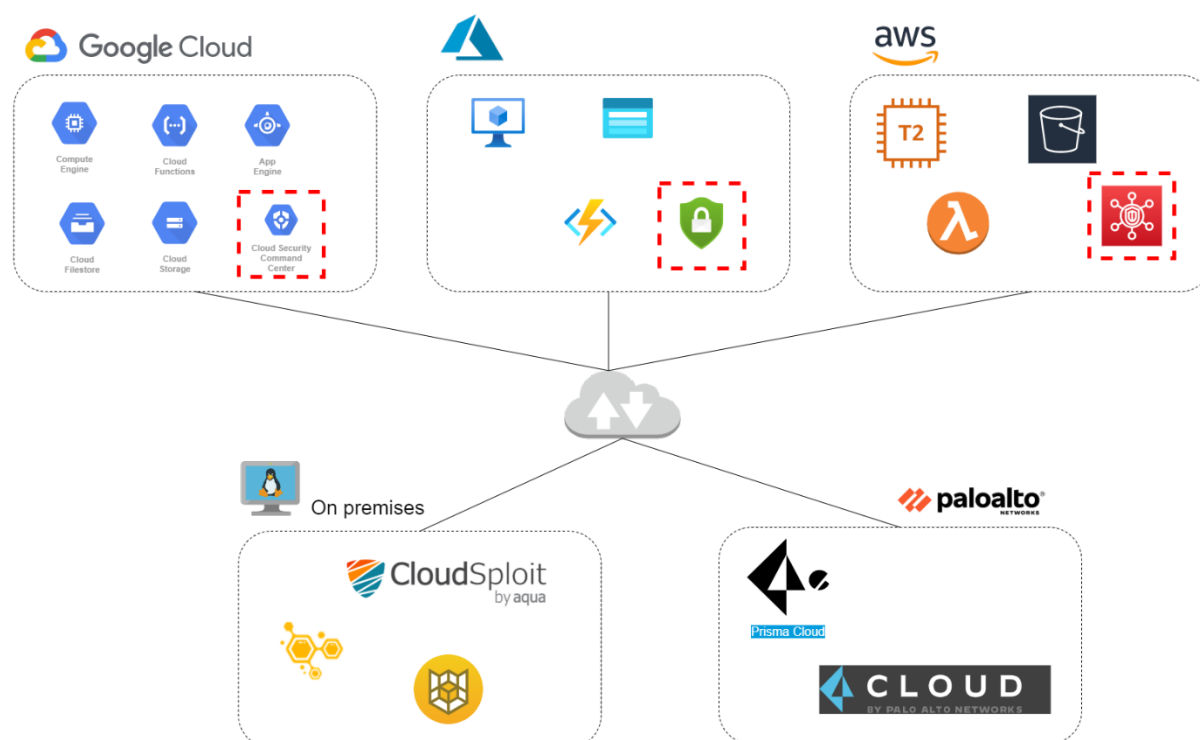


Figura 15: Laboratorio

5.1.1. Google Cloud Platform

De este proveedor cloud, se han elegido los siguientes servicios, todos ellos desplegados en la región us-central1 de Iowa, EEUU:

- App Engine (PaaS). Herramienta para alojamiento y despliegue automatizado de aplicaciones de Google. En este caso, hemos creado una simple aplicación web, con un simple mensaje de “hola mundo” al acceder a la siguiente URL: <https://uoc-tfm-project.uc.r.appspot.com/>. En este caso, se han dejado las configuraciones de seguridad por defecto.
- Compute Engine (IaaS): Se ha creado una instancia de máquina virtual Debian en la nube de Google, con acceso por SSH mediante el portal web de Google Cloud Platform. Las configuraciones de seguridad se han dejado por defecto, salvo el acceso por HTTP abierto. Debido al uso de este servicio, se deben usar otros como Persistent Disk, VPC network, entre otros.

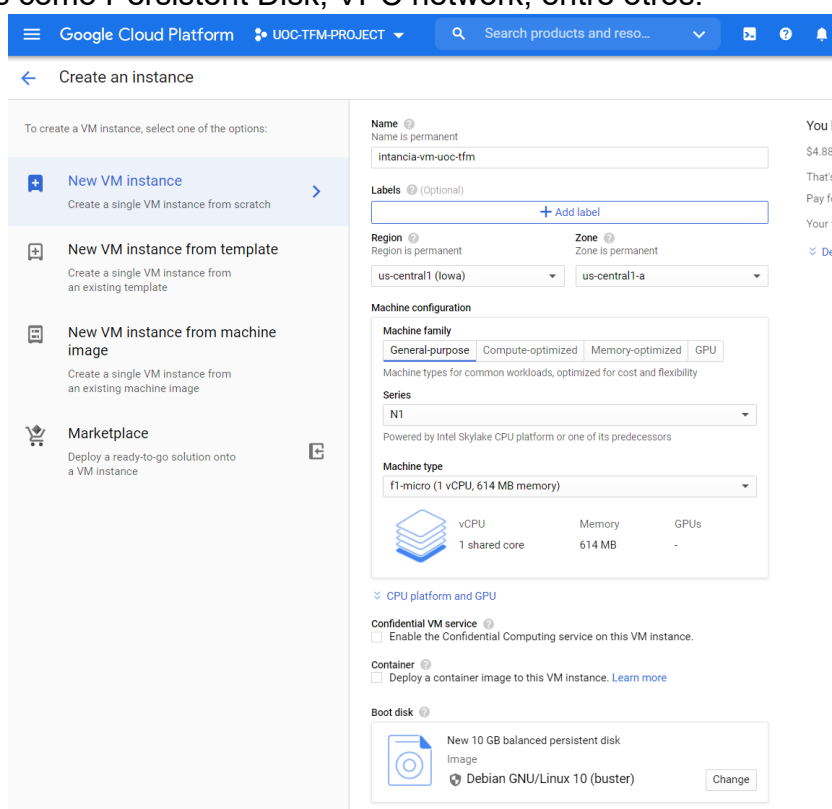


Figura 16: Creación de MV en GCP

- Firestore (PaaS, o DBaaS), una base de datos NoSQL para almacenar, sincronizar y consultar datos para aplicaciones web y móviles. Para este servicio, hemos creado una simple colección con datos, usando las configuraciones por defecto, salvo en las reglas, en las que hemos permitido lectura a todos (público), pero escritura a nadie

```

1  rules_version = '2';
2  service cloud.firestore {
3    match /databases/{database}/documents {
4      match /{document=**} {
5        allow read: if true;
6        allow write: if false;
7      }
    }
  }

```

Figura 17: Reglas Firestore

- Cloud Storage: servicio RESTful para almacenar y acceder a sus datos en la infraestructura de Google. Este servicio se ha sido necesario usarlo como bucket para otros servicios (Cloud Shell, AppEngine, entre otros)

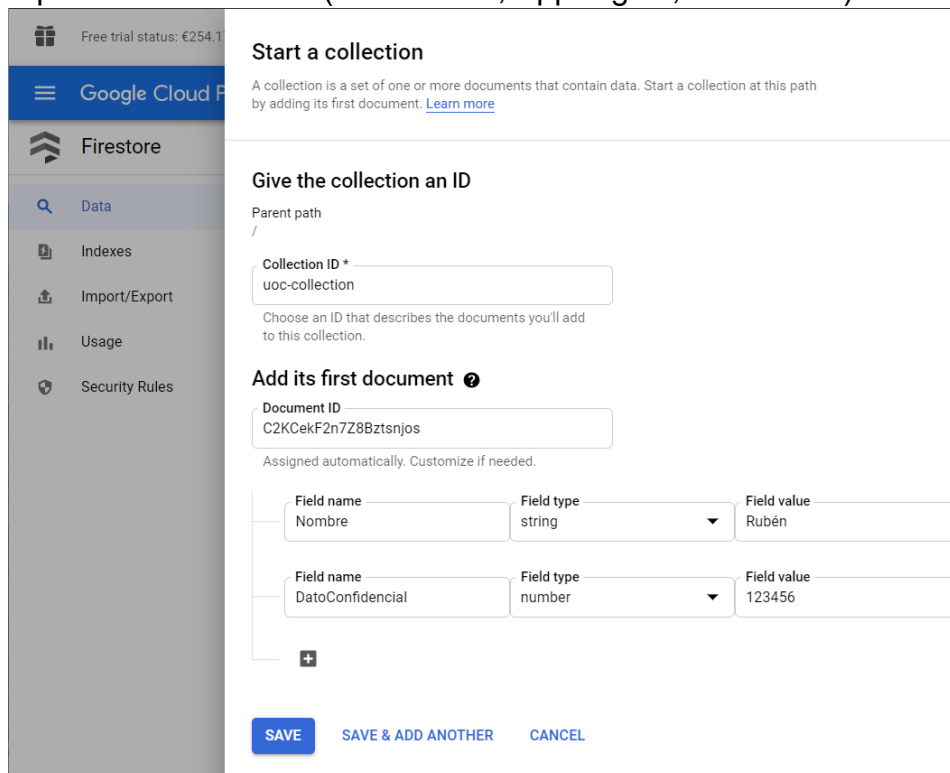


Figura 18: Configuración Cloud Storage

5.1.2. Microsoft Azure







Los servicios desplegados en Azure se han lanzado en la región del norte de Europa, entre ellos, tenemos:

- Máquina virtual (IaaS). Se ha creado una pequeña máquina virtual (instancia B1s) con Windows Server 2019. Se ha habilitado el acceso por RDP y se han desactivado algunas opciones de seguridad perimetral de Azure. La creación de este recurso ha requerido el uso de otros como las redes virtuales o almacenamiento persistente en una cuenta de almacenamiento.
- Cuenta de almacenamiento (PaaS), servicio que proporciona almacenamiento en la nube altamente disponible, seguro, duradero, escalable y redundante. Puede ser de tipo Blob (objetos), Files, Queues, Tables, DataLake Storage. En este caso, se ha creado un contenedor con documentos confidenciales y se han desmarcado algunas opciones de seguridad para hacerlo accesible públicamente. El documento creado es accesible desde:
<https://storageazuretfm.blob.core.windows.net/docconfidencial/secreto.txt>



Crear cuenta de almacenamiento ...

Datos básicos Redes **Protección de datos** Opciones avanzadas Etiquetas Revisar y crear

Recuperación

- Habilitar la restauración a un momento dado para contenedores**
 Use la restauración a un momento dado para restaurar uno o varios contenedores a un estado anterior. Si la restauración a un momento dado está habilitada, el control de versiones, la fuente de cambios y la eliminación temporal de blobs también deben estar habilitados. [Más información](#) 
- Habilitar la eliminación temporal para blobs**
 La eliminación temporal permite recuperar los blobs que se marcaron previamente para su eliminación, incluidos los blobs que se sobrescribieron. [Más información](#) 
- Habilitar la eliminación temporal para contenedores**
 La eliminación temporal permite recuperar contenedores que se marcaron anteriormente para su eliminación. [Más información](#) 
 Es necesario registrarse para cada suscripción para usar la eliminación temporal de contenedores. [Registrarse para la eliminación temporal de contenedores](#) 
- Habilitar la eliminación temporal para recursos compartidos de archivos**
 La eliminación temporal permite recuperar los recursos compartidos de archivos que se marcaron previamente para su eliminación. [Más información](#) 

Seguimiento

- Habilitar el control de versiones para blobs**
 Use el control de versiones para conservar automáticamente las versiones anteriores de los blobs con fines de recuperación y restauración. [Más información](#) 
- Habilitar la fuente de cambios del blob**
 Realice un seguimiento de la creación, la modificación y los cambios en la eliminación de los blobs de la cuenta. [Más información](#) 

Revisar y crear

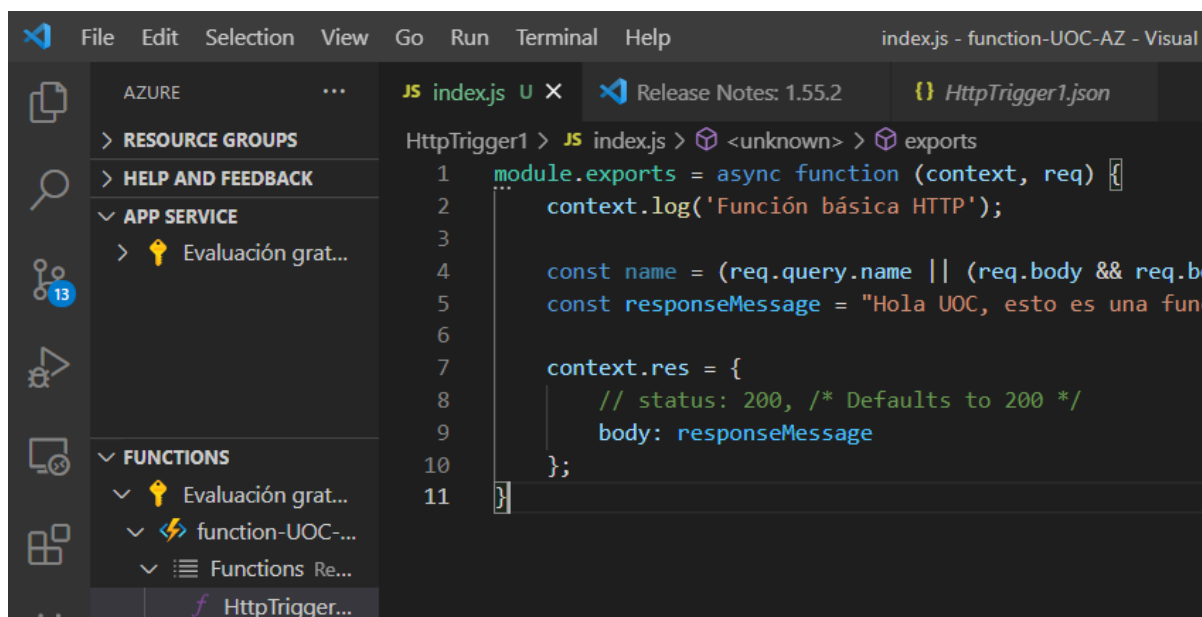
< Anterior

Siguiente: Opciones avanzadas >

Figura 19: Configuración cuenta de almacenamiento Azure

- Función (Aplicación de funciones, PaaS o fPaaS), servicio que permite ejecutar código en un entorno sin servidor y sin necesidad de crear una máquina virtual ni publicar una aplicación web. Para este caso, hemos publicado un simple mensaje de “Hola mundo”, con la configuración por defecto, tan solo cambiando la versión de TLS empleada por una antigua. El recurso es accesible mediante la siguiente URL:

<https://function-uocaz.azurewebsites.net/api/httptrigger1?code=LmVeFeQxw3qP7a7Q2w3%2F9UEN6Lwqavl966dSCu22IJZolUEK5Di6g%3D%3D>



```

HttpTrigger1 > JS index.js > <unknown> > exports
1  module.exports = async function (context, req) {
2    context.log('Función básica HTTP');
3
4    const name = (req.query.name || (req.body && req.b
5    const responseMessage = "Hola UOC, esto es una fun
6
7    context.res = {
8      // status: 200, /* Defaults to 200 */
9      body: responseMessage
10   };
11 }

```

Figura 20: Creación de función en Azure

- Azure Security Center (SaaS). Por último, se ha activado el recurso de seguridad ya comentado. No se ha vinculado a otra cuenta de otro proveedor cloud (GCP o AWS) al no disponer de una suscripción de Azure compatible. Se ha añadido la suscripción usada al alcance de la herramienta, por lo que todos los recursos citados anteriormente aparecen en su inventario. Como configuración adicional, se han añadido otros estándares de cumplimiento como el ISO 27001 para su revisión automática.

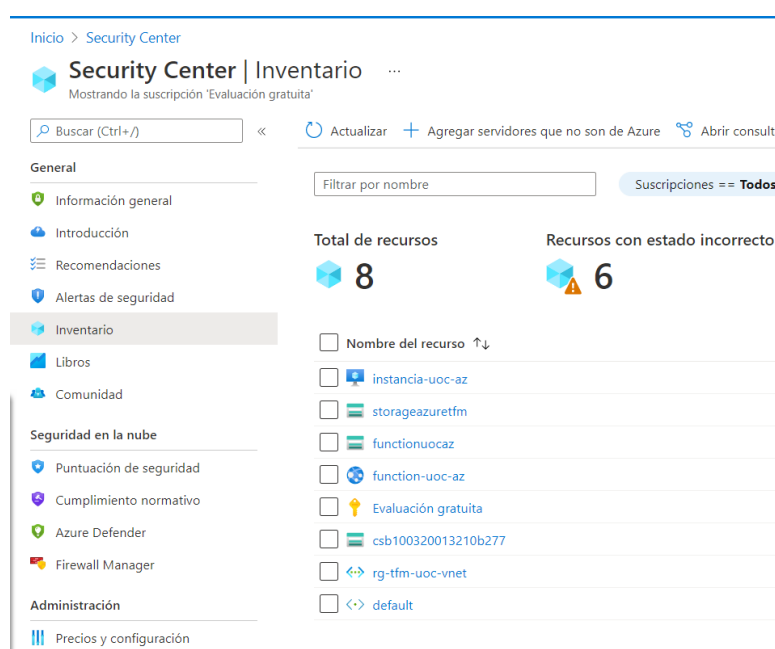


Figura 21: Azure Security Center, inventariado

5.1.3. Amazon Web Services

Para este CSP, se han desplegado recursos en la región de Londres (eu-west-2) y algunos en el norte de Virginia (us-east-1), entre los servicios desplegados, tenemos:

- EC2 (IaaS), servicio de instancias de máquinas virtuales de AWS. En este caso, se ha creado una instancia t2.micro con Ubuntu instalado. El acceso se realiza por SSH a través de clave pública. El resto de las configuraciones se han dejado por defecto. Debido al despliegue de este recurso, se han tenido que generar un volumen para almacenamiento persistente y una red VPC.

```
ubuntu@ip-172-31-33-156: ~
Rubén@LAPTOP-RF3J8R62 MINGW64 ~/Downloads
$ ssh ubuntu@ec2-18-133-27-127.eu-west-2.compute.amazonaws.com -i AWS-UBT-T2-UOC.pem
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1038-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Apr 15 19:14:36 UTC 2021

System load:  0.0          Processes:    101
Usage of /:   16.4% of 7.69GB  Users logged in:  0
Memory usage: 22%          IPv4 address for eth0: 172.31.33.156
Swap usage:  0%
```

Figura 22: Conexión a máquina virtual de AWS por SSH

- Lambda (PaaS o fPaaS), servicio informático sin servidor que permite ejecutar código sin aprovisionar ni administrar servidores. Se ha añadido un activador por HTTP y se han dejado el resto de opciones por defecto. La aplicación se ha desarrollado en node.js y es un simple “Hola Mundo”. Es accesible desde: <https://9hefi13fei.execute-api.eu-west-2.amazonaws.com/default/funcion-UOC-AWS>



The screenshot shows the AWS Lambda console for a function named 'funcion-UOC-AWS'. On the left, there's a sidebar with 'Información general de la función' and a button '+ Agregar desencadenador'. The main area shows the function's configuration, including layers. On the right, a code editor shows the following JavaScript code for 'index.js':

```
exports.handler = async (event) => {
  // TODO implement
  const response = {
    statusCode: 200,
    body: JSON.stringify('Hola UOC'),
  };
  return response;
};
```

Figura 23: Función de AWS

- Amazon Simple Storage Service o S3 (PaaS), servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento. En este caso, se ha creado un bucket expuesto públicamente a Internet, con las opciones de seguridad recomendadas deshabilitadas. Se ha añadido información confidencial, accesible mediante la siguiente URL: https://bucket-uoc-tfm.s3.eu-west-2.amazonaws.com/doc_confidencial/secreto.txt

Configuración de bloqueo de acceso público para este bucket

Se concede acceso público a los buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos, active Bloquear todo el acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración individual a continuación para adaptarla a sus casos de uso de almacenamiento específicos. [Más información](#)


Bloquear todo el acceso público
Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación. Cada uno de los siguientes ajustes son independientes entre sí.

Bloquear el acceso público a buckets y objetos concedido a través de nuevas listas de control de acceso (ACL)
S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y evitará la creación de nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos existentes que permiten acceso público a los recursos de S3 mediante ACL.

Bloquear el acceso público a buckets y objetos concedido a través de cualquier lista de control de acceso (ACL)
S3 ignorará todas las ACL que conceden acceso público a buckets y objetos.

Bloquear el acceso público a buckets y objetos concedido a través de políticas de bucket y puntos de acceso públicas nuevas
S3 bloqueará las nuevas políticas de buckets y puntos de acceso que concedan acceso público a buckets y objetos. Esta configuración no afecta a las políticas ya existentes que permiten acceso público a los recursos de S3.

Bloquear el acceso público y entre cuentas a buckets y objetos concedido a través de cualquier política de bucket y puntos de acceso pública
S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso que tengan políticas que concedan acceso público a buckets y objetos.

 **Desactivar el bloqueo de todo acceso público puede provocar que este bucket y los objetos que contiene se vuelvan públicos**
AWS recomienda que active la opción para bloquear todo el acceso público, a menos que se requiera acceso público para casos de uso específicos y verificados, como el alojamiento de sitios web estáticos.

Reconozco que la configuración actual puede provocar que este bucket y los objetos que contiene se vuelvan públicos.

Figura 24: Configuración insegura S3

- AWS Security Hub (SaaS), por último, se ha activado la herramienta CSPM comentada en el capítulo anterior. Activar este recurso ha supuesto la activación de AWS Config, que es el servicio que permite examinar, auditar y evaluar las configuraciones de sus recursos de AWS.

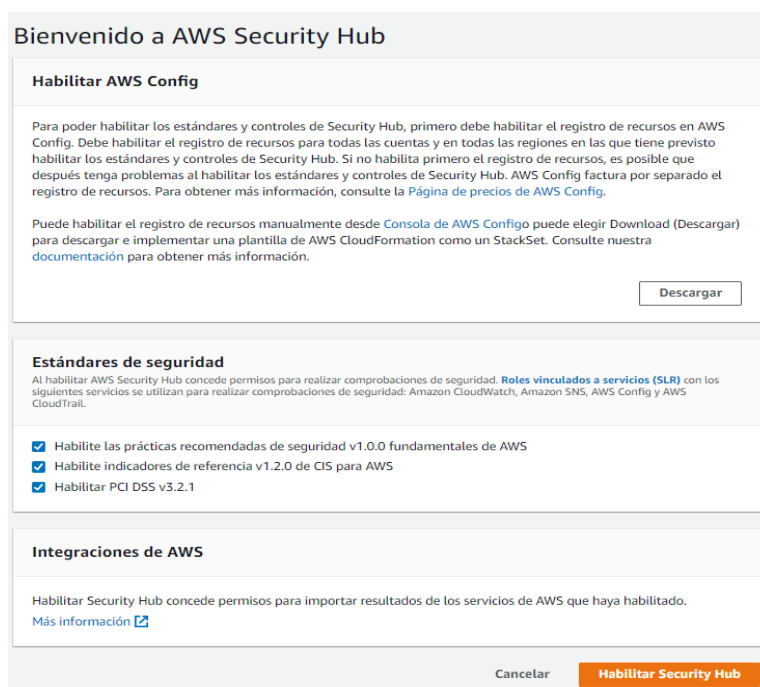
5.2. Prueba de herramientas CSPM

5.2.1. AWS Security Hub

La primera herramienta por revisar es la nativa de AWS, Security hub. De por sí sola, esta herramienta no es más que un panel de control que requiere de otros complementos de AWS para funcionar. Concretamente, dentro de sus integraciones, encontramos, entre otros:

- Amazon GuardDuty, para la protección de las cargas de trabajo (vendría a ser un CWPP)
- Amazon Inspector, que permite analizar el comportamiento de recursos de AWS y ayuda a identificar posibles problemas de seguridad.
- Amazon Config, que permite una vista detallada de los recursos de AWS, cómo se configuran, cómo se relacionan entre sí, y el histórico de configuraciones. También dispone de paquetes de conformidad con los que evaluar el despliegue de acuerdo a estándares y guías de mejores prácticas.
- Amazon Macie, para la detección de información confidencial en S3
- Amazon Detective, encargado en la recopilación de registros para verificaciones de seguridad

Para la funcionalidad CSPM, debemos habilitar las integraciones de Amazon Config (mínimo indispensable para que funciones Security Hub) y Amazon Inspector. Para cada una de las integraciones, Security Hub dispone de una guía paso a paso de cómo activar cada complemento. Durante la configuración de Security Hub, podemos seleccionar qué estándares o guías de buenas prácticas incorporar a la herramienta, en este caso, se han seleccionado las 3 disponibles:



Bienvenido a AWS Security Hub

Habilitar AWS Config

Para poder habilitar los estándares y controles de Security Hub, primero debe habilitar el registro de recursos en AWS Config. Debe habilitar el registro de recursos para todas las cuentas y en todas las regiones en las que tiene previsto habilitar los estándares y controles de Security Hub. Si no habilita primero el registro de recursos, es posible que después tenga problemas al habilitar los estándares y controles de Security Hub. AWS Config factura por separado el registro de recursos. Para obtener más información, consulte la [Página de precios de AWS Config](#).

Puede habilitar el registro de recursos manualmente desde [Consola de AWS Config](#) puede elegir Download (Descargar) para descargar e implementar una plantilla de AWS CloudFormation como un StackSet. Consulte nuestra [documentación](#) para obtener más información.

Descargar

Estándares de seguridad

Al habilitar AWS Security Hub concede permisos para realizar comprobaciones de seguridad. [Roles vinculados a servicios \(SLR\)](#) con los siguientes servicios se utilizan para realizar comprobaciones de seguridad: Amazon CloudWatch, Amazon SNS, AWS Config y AWS CloudTrail.

- Habilite las prácticas recomendadas de seguridad v1.0.0 fundamentales de AWS
- Habilite indicadores de referencia v1.2.0 de CIS para AWS
- Habilitar PCI DSS v3.2.1

Integraciones de AWS

Habilitar Security Hub concede permisos para importar resultados de los servicios de AWS que haya habilitado. [Más información](#)

Cancelar **Habilitar Security Hub**

Figura 25: Configuración AWS Security Hub

Una vez configurado, deben pasar unas 12 horas para que la herramienta comience a mostrar resultados. Security Hub es muy fácil de comenzar a usar, dispone de 6 paneles principales:

- Resumen: Un pequeño dashboard (Figura 26) con todos los hallazgos encontrados, con gráficos sobre el cumplimiento normativo, recursos afectados, observaciones e integraciones
- Estándares de seguridad, se muestra el grado de cumplimiento (Figura 27) para los estándares seleccionados durante la configuración de Security Hub, mostrando un diagrama de tipo Gauge con la puntuación del cumplimiento (en tanto %)
- Observaciones. Security hub permite la creación de observaciones, que no es más que un filtro guardado para acelerar la búsqueda de los resultados obtenidos (ver Figura 28). Usando las observaciones, la herramienta crea una gráfica indicando los recursos que cumplen ese filtrado, lo que facilita enormemente la interpretación de resultados. La propia herramienta dispone de observaciones ya creadas, en los que, por ejemplo, podemos consultar todos los recursos de tipo EC2 abiertas a Internet.

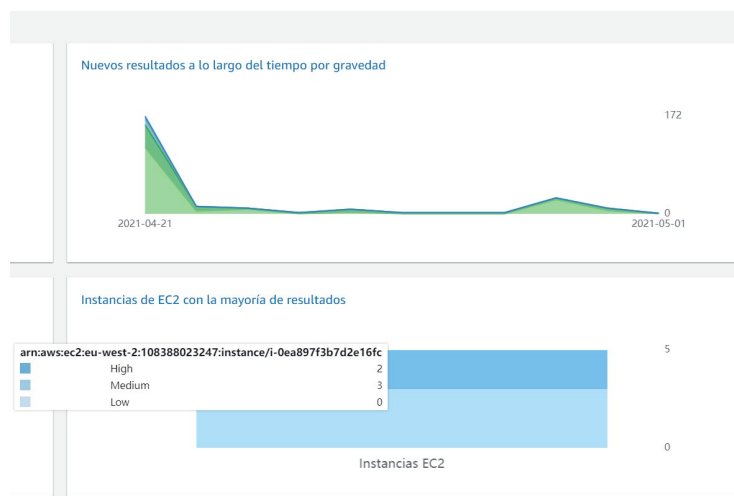


Figura 26: AWS Security Hub, resumen

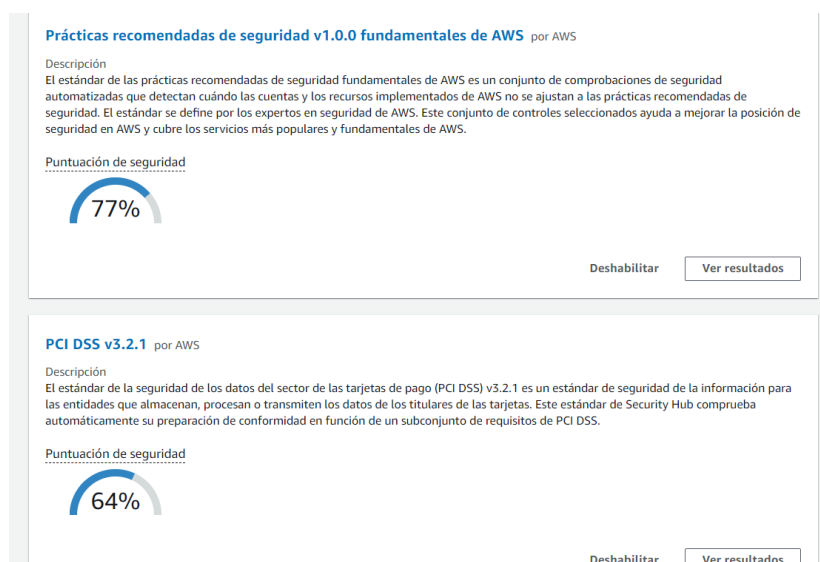
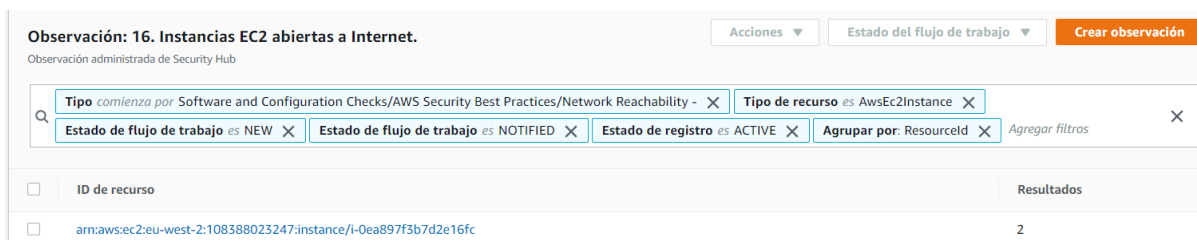


Figura 27: AWS Security Hub, estándares de seguridad



Observación: 16. Instancias EC2 abiertas a Internet. Acciones Estado del flujo de trabajo Crear observación

Observación administrada de Security Hub

Tipo comienza por Software and Configuration Checks/AWS Security Best Practices/Network Reachability - Tipo de recurso es AwsEc2Instance

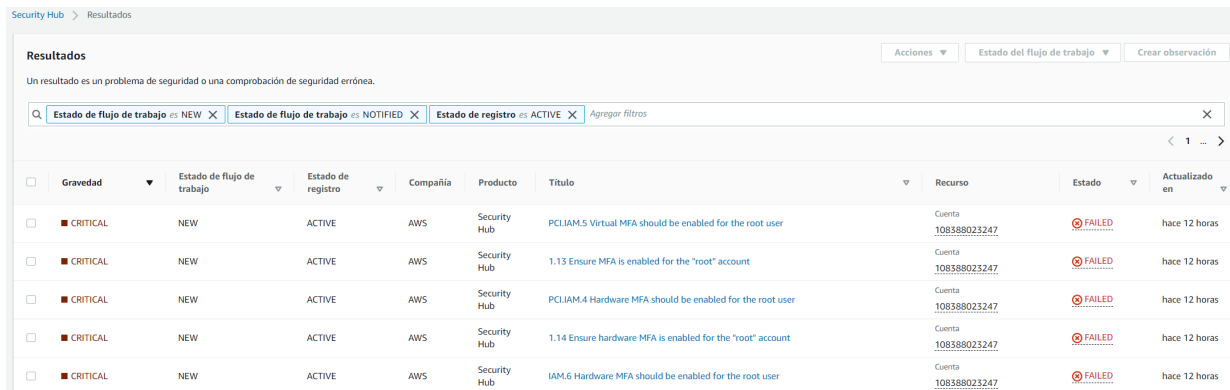
Estado de flujo de trabajo es NEW Estado de flujo de trabajo es NOTIFIED Estado de registro es ACTIVE Agrupar por: ResourceId Agregar filtros

ID de recurso	Resultados
arn:aws:ec2:eu-west-2:108388023247:instance/i-0ea897f3b7d2e16fc	2

Figura 28: AWS Security Hub, observaciones

- **Resultados:** Se muestra en formato tabla los problemas de seguridad o comprobaciones de seguridad erróneas. Entre los diferentes campos, encontramos el nivel de gravedad del hallazgo, el título del control revisado, su estado, qué recurso ha sido el afectado, y la última actualización. Si entramos en el detalle de cada resultado, vemos las reglas asociadas a ese resultado

que no se han cumplido, y que vienen a ser los controles de seguridad probados respecto a las guías de buenas prácticas y estándares de cumplimiento.



Security Hub > Resultados

Resultados

Un resultado es un problema de seguridad o una comprobación de seguridad errónea.

Acciones Estado del flujo de trabajo Crear observación

Estado de flujo de trabajo es NEW Estado de flujo de trabajo es NOTIFIED Estado de registro es ACTIVE

Gravedad	Estado de flujo de trabajo	Estado de registro	Compañía	Producto	Título	Recurso	Estado	Actualizado en
CRITICAL	NEW	ACTIVE	AWS	Security Hub	PCI.IAM.5 Virtual MFA should be enabled for the root user	Cuenta 108388023247	FAILED	hace 12 horas
CRITICAL	NEW	ACTIVE	AWS	Security Hub	1.13 Ensure MFA is enabled for the "root" account	Cuenta 108388023247	FAILED	hace 12 horas
CRITICAL	NEW	ACTIVE	AWS	Security Hub	PCI.IAM.4 Hardware MFA should be enabled for the root user	Cuenta 108388023247	FAILED	hace 12 horas
CRITICAL	NEW	ACTIVE	AWS	Security Hub	1.14 Ensure hardware MFA is enabled for the "root" account	Cuenta 108388023247	FAILED	hace 12 horas
CRITICAL	NEW	ACTIVE	AWS	Security Hub	IAM.6 Hardware MFA should be enabled for the root user	Cuenta 108388023247	FAILED	hace 12 horas

Figura 29: AWS Security Hub, resultados

- Integraciones: Permite incorporar otras funcionalidades de la propia AWS (Macie, Detective, etc.) o de terceros (McAfee: MVISION, FireEye Helix, entre otros), lo que permitiría integraciones con otros proveedores cloud.
- Configuración: Permite añadir otras cuentas de AWS para gestionarlas en la herramienta, consultar su uso, sus permisos, y crear acciones personalizadas, lo que permite enviar resultados seleccionados mediante Amazon CloudWatchEvents.

En ninguno de los puntos de menú de Security Hub es posible ver de manera sencilla el inventariado de recursos desplegados. Para poder ver esto, y administrar otras opciones, debemos ir al panel de configuración de AWS Config. En dicho panel podemos ver los recursos desplegados y el histórico (Figura 30), los paquetes de conformidad disponibles y las reglas/controles probados



AWS Config > Panel

Panel

Inventario de recursos
Vea el inventario de sus recursos de AWS y externos. [Más información](#)

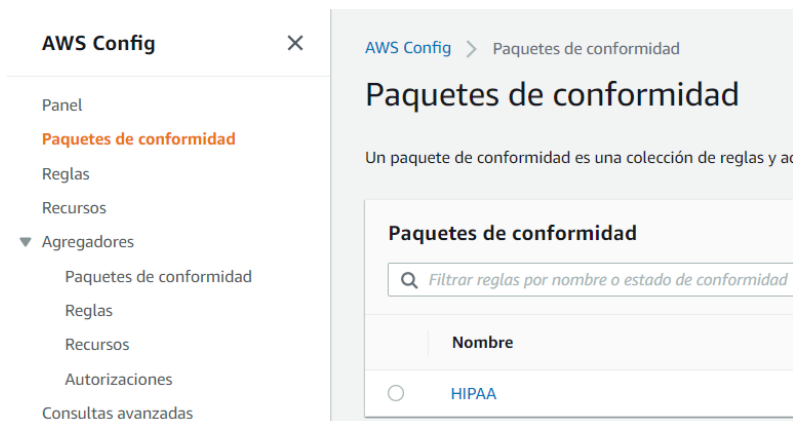
Todos los recursos

Recursos totales 57

Tipo	Recuento
Config ResourceCompliance	23
IAM Role	7
Config ConformancePackCompliance	3

Figura 30: AWS Config, inventariado

Un paquete de conformidad es una colección de reglas y acciones de corrección de AWS Config que se pueden implementar y monitorear. Por defecto, no podemos tener activos paquetes de conformidad que supongan más de 150 reglas en total.



Entre los paquetes que podemos seleccionar encontramos:

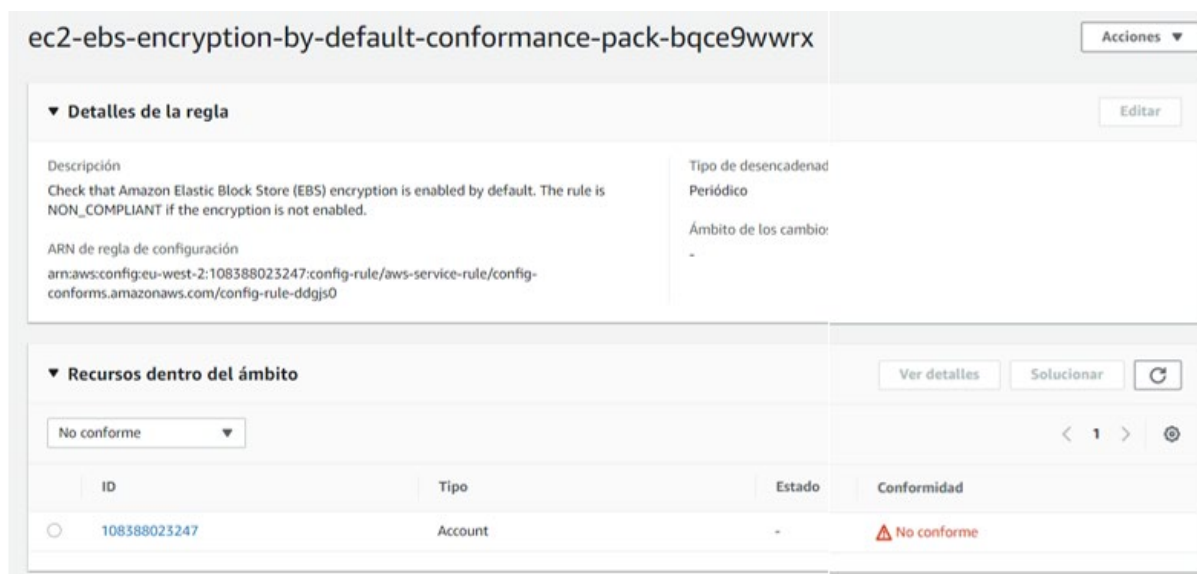
- AWS Control Tower Detective Guardrails
- Operational Best Practices for 800 53 rev 4
- Operational Best Practices for ABS CCIGv2 Standard
- Operational Best Practices for ACSC ISM
- Operational Best Practices for AI and ML
- Operational Best Practices for Amazon DynamoDB
- Operational Best Practices for Amazon S3
- Operational Best Practices for FDA 21CFR Part 11
- Operational Best Practices for FFIEC
- Operational Best Practices for FedRAMP
- Operational Best Practices for HIPAA Security
- Operational Best Practices for NIST CSF
- Operational Best Practices for NYDFS 23 NYCRR 500
- Operational Best Practices for Networking Services
- Operational Best Practices for PCI DSS

Los paquetes de conformidad aquí seleccionados no aparecen en el panel de control de Security Hub. Por ejemplo, hemos seleccionado el paquete HIPAA, y nuestro despliegue es “No conforme”, pero dicha información no aparece en Security Hub



Figura 31: AWS Config, HIPAA no conforme

Si entramos en el detalle de cada paquete de conformidad en AWS Config, podemos ver el conjunto de reglas definido en su interior. Para nuestro despliegue, vemos: una regla no conforme (Figura 32), ya que existe un EBS sin encriptación por defecto; y otra **no conforme** (Figura 33), ya que nuestra instancia EC2 se encuentra dentro de una VPC



ec2-ebs-encryption-by-default-conformance-pack-bqce9wwrx Acciones

▼ Detalles de la regla Editar

Descripción
Check that Amazon Elastic Block Store (EBS) encryption is enabled by default. The rule is NON_COMPLIANT if the encryption is not enabled.

ARN de regla de configuración
arn:aws:config:eu-west-2:108388023247:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-ddgjs0

Tipo de desencadenad
Periódico

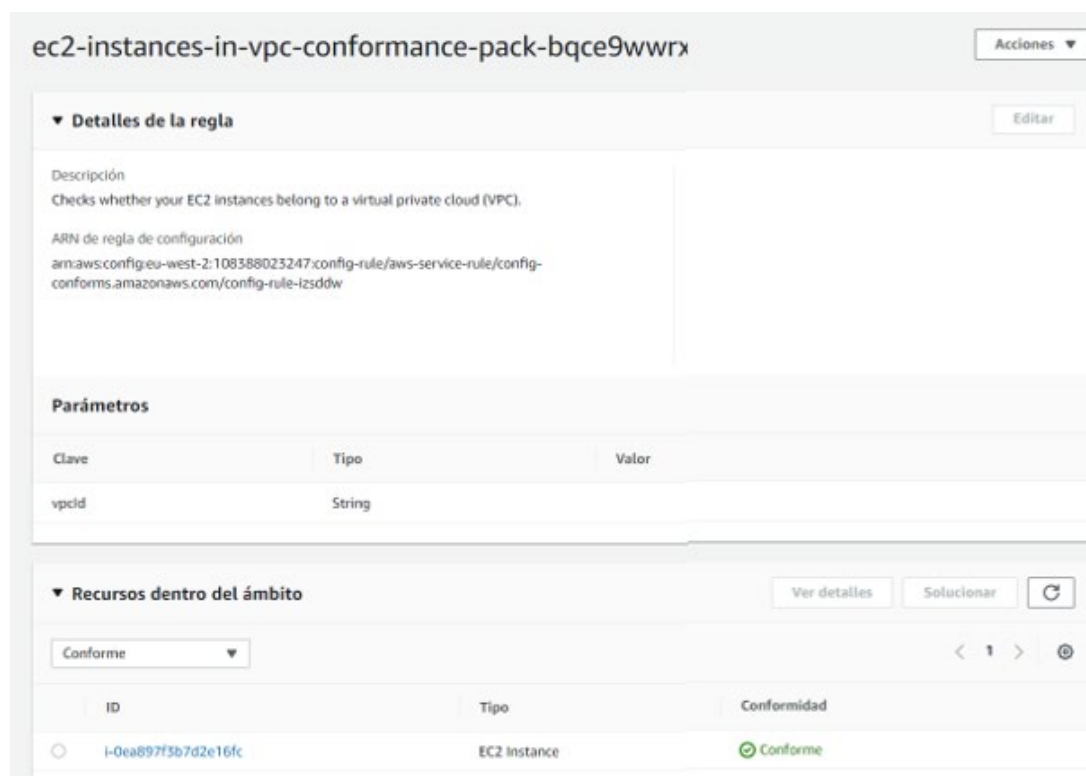
Ámbito de los cambio:
-

▼ Recursos dentro del ámbito Ver detalles Solucionar ↻

No conforme

ID	Tipo	Estado	Conformidad
108388023247	Account	-	⚠ No conforme

Figura 32: AWS Config, regla no conforme



ec2-instances-in-vpc-conformance-pack-bqce9wwrx Acciones

▼ Detalles de la regla Editar

Descripción
Checks whether your EC2 instances belong to a virtual private cloud (VPC).

ARN de regla de configuración
arn:aws:config:eu-west-2:108388023247:config-rule/aws-service-rule/config-conforms.amazonaws.com/config-rule-izsddw

Parámetros

Clave	Tipo	Valor
vpcId	String	

▼ Recursos dentro del ámbito Ver detalles Solucionar ↻

Conforme

ID	Tipo	Conformidad
i-0ea897f3b7d2e16fc	EC2 instance	✅ Conforme

Figura 33: AWS Config, regla conforme

En este apartado de reglas, se muestra tanto las reglas definidas en el paquete de conformidad seleccionado, como las reglas creadas por Security Hub, y los paquetes de conformidad de esta última. También se permite la creación de reglas personalizadas.

Ahora veamos el funcionamiento de Security Hub en combinación con AWS Config. Recordamos en este punto que, a no ser que se utilice alguna integración con terceros específica, esta herramienta de por sí es solo compatible con AWS.

En Security Hub > Resultados, vemos una regla con severidad alta (Figura 34), que indica que ningún grupo de seguridad debe permitir datos entrantes desde internet al puerto 22 (SSH)

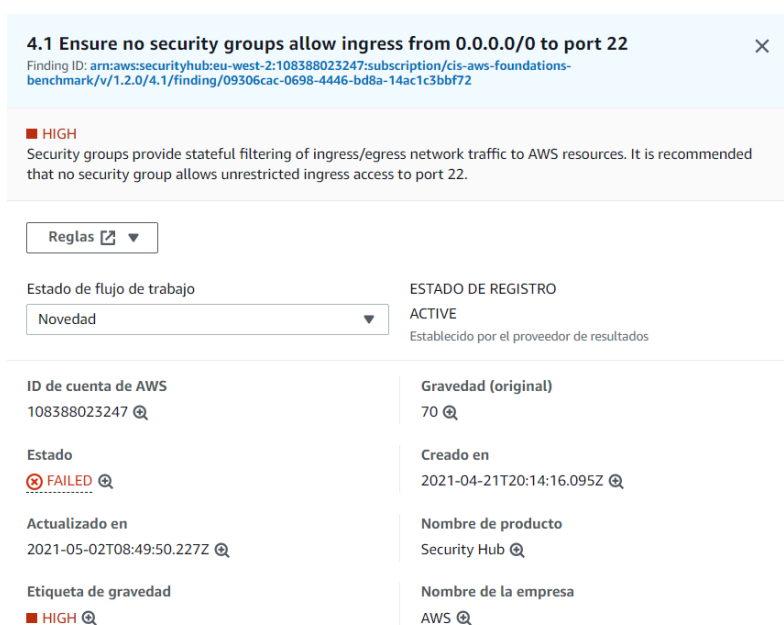


Figura 34: Regla con severidad alta

El propio resultado, nos indica la cuenta y recursos afectados, así como un enlace para corregir el hallazgo (Figura 35)



Figura 35: Detalles y corrección de la regla

Si desplegamos la regla usada para este resultado (Figura 36), se nos envía directamente a AWS Config con una descripción más detallada del hallazgo

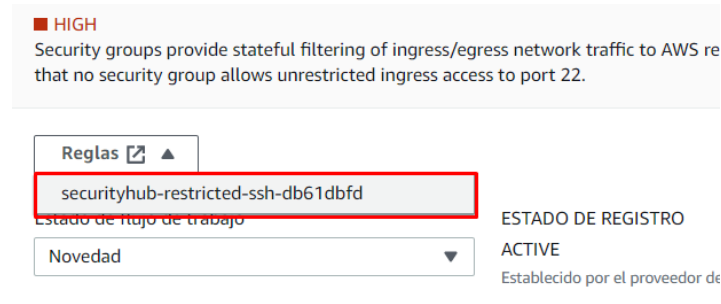


Figura 36: Regla aplicada

En AWS Config, vemos como esta regla se activa al detectar que tráfico SSH es accesible a nuestra instancia desde direcciones IP no restringidas. Por tanto, está no conforme en nuestro despliegue (

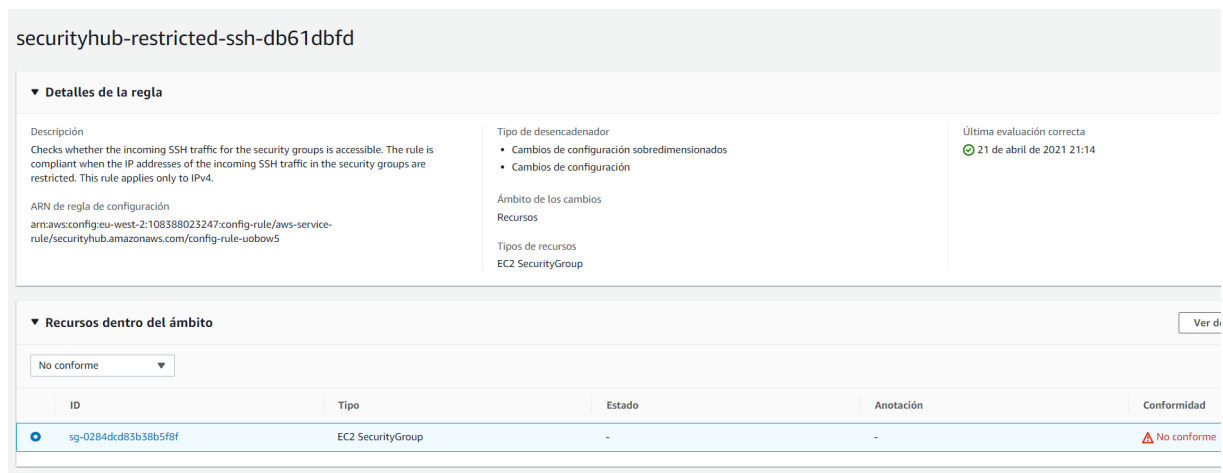


Figura 37: Detalle de la regla

Si seleccionamos el recurso afectado, AWS Config sí que nos permite solucionar el incidente de manera automática (botón Solucionar). Si pulsamos sobre solucionar, vemos como soluciona el incidente y pasa a estar conforme (Figura 38)

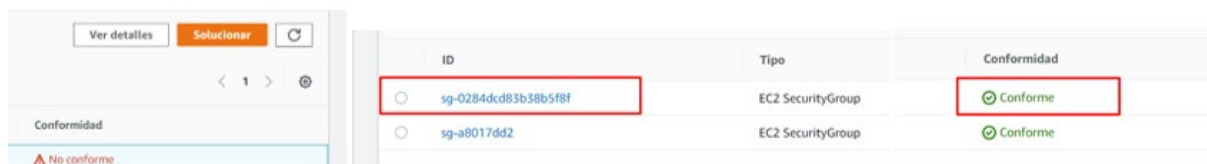


Figura 38: Botón de "Solucionar" hallazgo y solución del incidente

El siguiente punto a revisar de Security Hub, es el apartado de cumplimiento normativo. En la pestaña "Estándares de Seguridad", podemos ver el cumplimiento de nuestro despliegue frente al PCI DSS v3.2.1 por ejemplo (Figura 39)

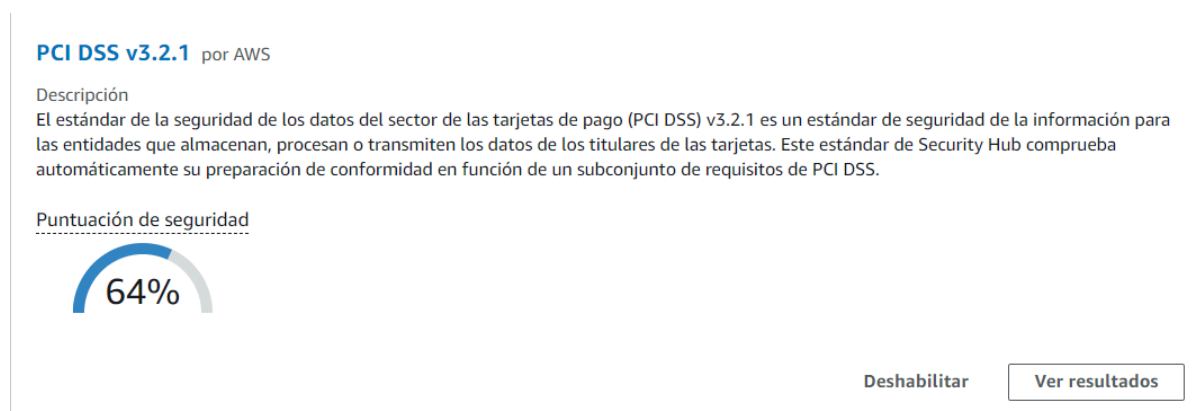


Figura 39: Cumplimiento PCI DSS v3.2.1

Podemos ver los resultados en detalle (Figura 40), donde aparecen todos los controles habilitados, cuales han fallado y cuales aprobado.

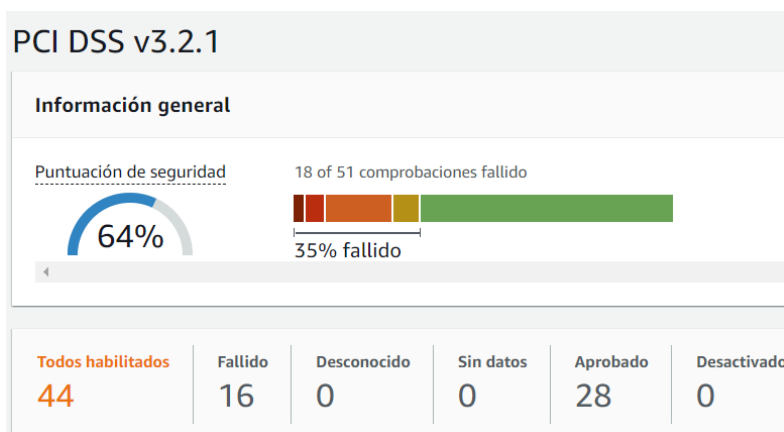


Figura 40: Detalle cumplimiento PCI DSS

Cada control probado, supone un resultado, y a su vez, una regla de AWS Config probada, por lo que el proceso de solución (manual o automático) es idéntico al descrito anteriormente para la regla del SSH.

5.2.2. Azure Security Center

La siguiente herramienta nativa a probar se trata de Security Center, de Azure. Esta solución está mucho mejor estructurada que Security Hub de AWS y no requiere de otros complementos o integraciones internas para funcionar.

Dispone de varios puntos de menú, agrupados en 3 categorías: “General”, que incluye inventariado, alertas de seguridad y recomendaciones, entre otros elementos; “Seguridad en la nube”, que dispone de la parte de cumplimiento normativo, puntuación de seguridad y Azure Defender; y “Administración de la herramienta”, con un apartado de configuración, integraciones, automatizaciones y conectores a otras nubes.

Security Center, a diferencia de su alternativa de AWS, sí que dispone de integraciones nativas para conectar con otras nubes (Figura 41). No obstante, para este TFM, dada la suscripción de la que disponemos en Azure, no será disponible usar esta funcionalidad

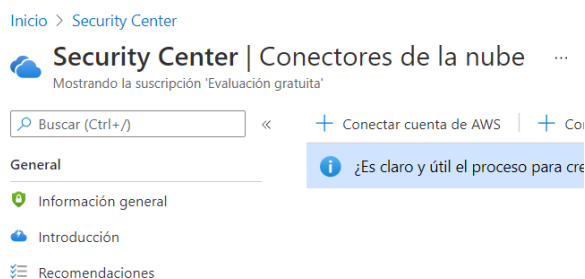


Figura 41: Security Center, conectores de nube

Como la anterior herramienta. Security Center dispone de un panel de control en el que ver un resumen de nuestro estado de seguridad mediante gráficas, e indica de forma muy clara, qué suscripciones de Azure tiene vinculadas la plataforma, cuántos recursos se evalúan, y el número de recomendaciones de seguridad activas y alertas detectado. Esto ayuda mucho a determinar si hay elementos de Azure que han quedado fuera del alcance

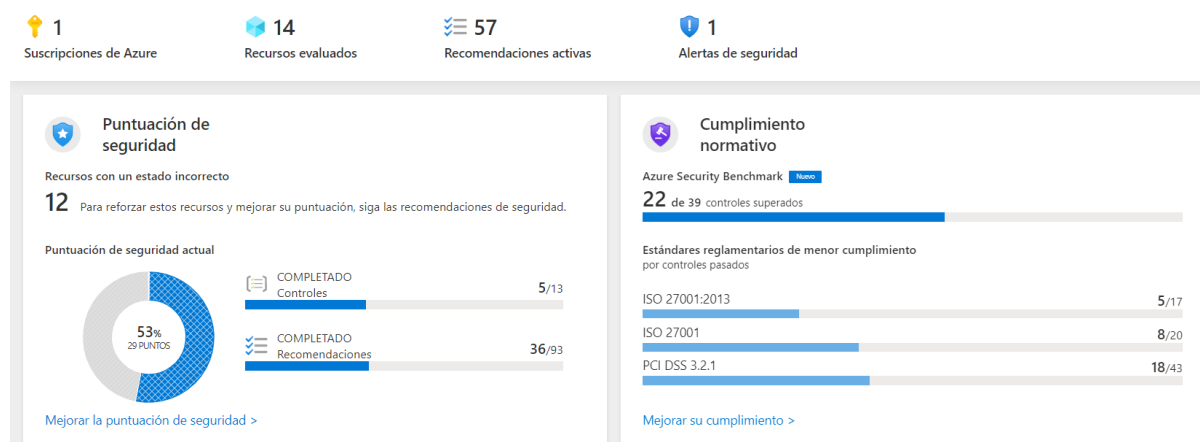


Figura 42: Security Center. resumen

Como vemos en la Figura 43, estamos controlando 1 suscripción, con un total de 14 recursos en su interior, que son todos los creados durante la fase de despliegue en Azure. Esta información se puede ampliar en el apartado de inventariado, que nos indica además los recursos y suscripciones no supervisados.

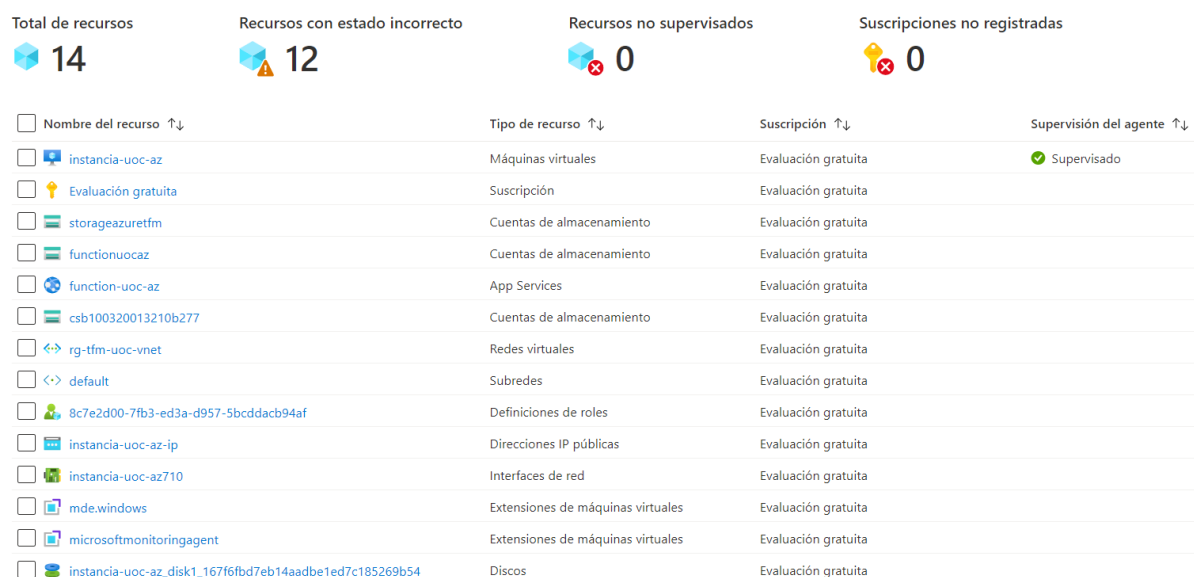


Figura 43: Detalle de inventario

Aclarar que, para supervisar ciertos elementos, como las IaaS, es necesario instalar un agente en la instancia.

En el apartado de “Recomendaciones”, tenemos un listado de todos los controles de Azure Security Benchmark probados sobre nuestro despliegue. De una forma sencilla, muestra cuantos recursos no han pasado ese control, o lo marca como OK si no hay recursos en los que aplique dicho control, tal y como se muestra en la Figura 44

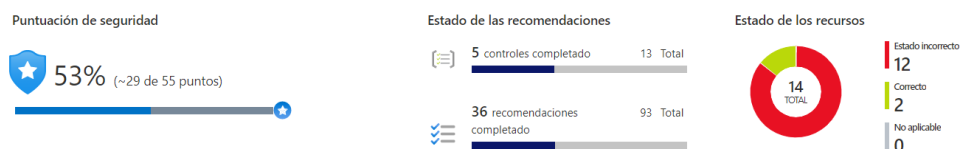





Figura 44: Security Center, recomendaciones

Vemos un ejemplo con el control “Las máquinas virtuales con conexión a Internet deben protegerse con grupos de seguridad de red.” Si entramos en el detalle (Figura 45) de ese control, podemos marcar una exención de control (el control se da por conforme/controlado), ver su severidad, una descripción, y los pasos para su corrección, además del recurso afectado (Figura 46).

Inicio > Security Center >

Las máquinas virtuales con conexión a Internet deben protegerse con grupos de seguridad de red. ...

 Exención
  Ver definición de la directiva
  Abrir consulta

Gravedad

Alta

Intervalo de actualización

 24 horas

^ Descripción

Proteja sus máquinas virtuales de posibles restringiendo el acceso a las mismas con un grupo de seguridad de red (NSG). Estos grupos contienen una lista de reglas de la lista de control de acceso (ACL) que permiten o deneguen el acceso. Tenga en cuenta que, para garantizar la seguridad de la máquina, el acceso de la VM a Internet debe estar restringido y, además, debe habilitarse un NSG en la subred. Las VM con una gravedad "Alta" son aquellas accesibles desde Internet.

^ Pasos para la corrección

Corrección manual:

Para proteger una máquina virtual con un grupo de seguridad de red:

1. Seleccione una máquina virtual de la siguiente lista o haga clic en "Realizar acción" si ha llegado hasta aquí a partir de una recomendación para una específica.
2. Asigne el NSG correspondiente al adaptador de red o subred de la máquina virtual que quiera proteger:
 - a. Para asignar el NSG a la subred de la máquina virtual (opción recomendada):
 - i. En la página Redes, seleccione "Red virtual o subred".
 - ii. Abra el menú "Subredes".
 - iii. Seleccione la subred en la que esté implementada su máquina virtual.
 - iv. Seleccione el grupo de seguridad de red que quiera asignar a la subred y haga clic en "Guardar".
 - b. Para asignar el NSG al adaptador de red:
 - i. En la página Redes, seleccione la interfaz de red que esté asociada a la máquina virtual seleccionada.
 - ii. En la página Interfaces de red, seleccione el elemento de menú "Grupo de seguridad de red".
 - iii. Haga clic en "Editar" en la parte superior de la página.
 - iv. Siga las instrucciones en pantalla y seleccione el grupo de seguridad de red que quiera asignar a este adaptador de red.

Haga clic [aquí](#) para obtener más información.

Figura 45: Detalle del control

^ Recursos afectados

Recursos con estado incorrecto (1)

Recursos con estado correcto (0)

Recursos no aplicables (0)

 Nombre

 instancia-UOC-AZ

Desencadenar aplicación lógica

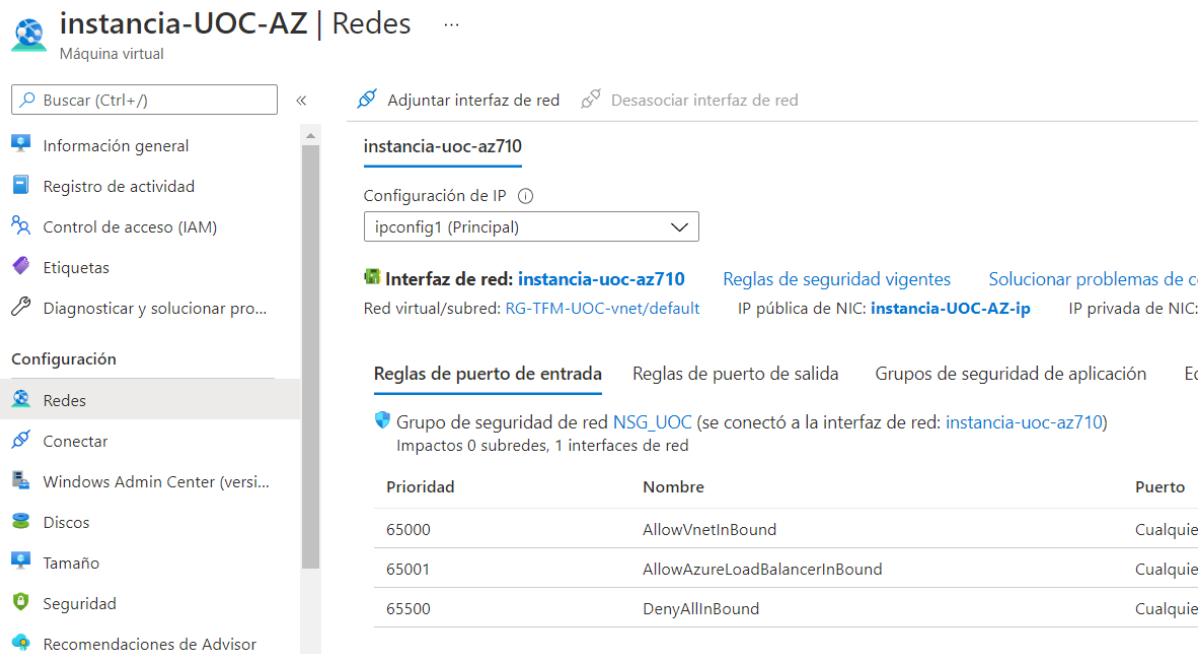
Exención

Figura 46: Recurso afectado

Además de la guía de corrección manual, si marcamos el recurso afectado, podemos desencadenar una aplicación lógica (Azure Logic Apps) para ejecutar múltiples acciones, desde solucionar la incidencia, hasta recibir un email con los detalles, agregarlo a un sistema de gestión de tareas, etc. No obstante, la programación de cada Logic App se debe hacer manualmente.

Vamos a probar a solucionar este control manualmente. Si haces click sobre el recurso, nos lleva directamente a la administración de red de la "instancia-UOC-AZ".

Siguiendo la guía descrita en la Figura 45, asignamos un grupo de seguridad de red a la interfaz de red de la instancia (Figura 47).



instancia-UOC-AZ | Redes ...
Máquina virtual

Buscar (Ctrl+/) << Adjuntar interfaz de red Desasociar interfaz de red

instancia-uoc-az710

Configuración de IP ⓘ
ipconfig1 (Principal)

Interfaz de red: instancia-uoc-az710 Reglas de seguridad vigentes Solucionar problemas de c
Red virtual/subred: RG-TFM-UOC-vnet/default IP pública de NIC: **instancia-UOC-AZ-ip** IP privada de NIC:

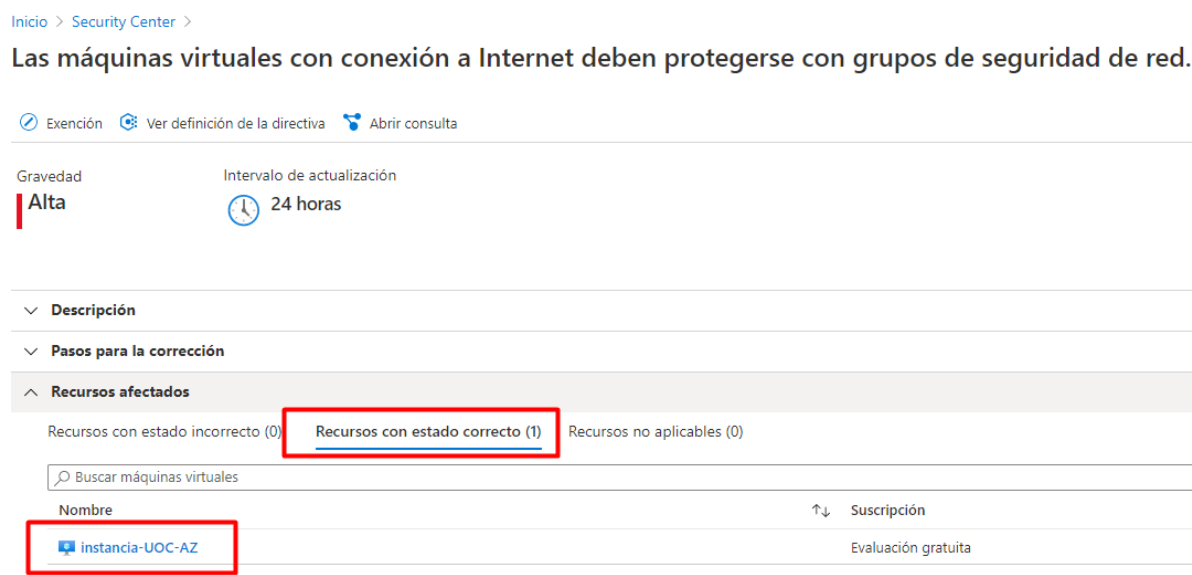
Reglas de puerto de entrada Reglas de puerto de salida Grupos de seguridad de aplicación Et

Grupo de seguridad de red **NSG_UOC** (se conectó a la interfaz de red: instancia-uoc-az710)
Impactos 0 subredes, 1 interfaces de red

Prioridad	Nombre	Puerto
65000	AllowVnetInBound	Cualquie
65001	AllowAzureLoadBalancerInBound	Cualquie
65500	DenyAllInBound	Cualquie

Figura 47: Grupo de seguridad de red

Tras pasar el plazo de actualización del control (24 horas en este caso, indicado también en la Figura 45), vemos reflejados los cambios en Security Center (Figura 48).



Inicio > Security Center >

Las máquinas virtuales con conexión a Internet deben protegerse con grupos de seguridad de red.

Exención Ver definición de la directiva Abrir consulta

Gravedad **Alta** Intervalo de actualización 24 horas

Descripción

Pasos para la corrección

Recursos afectados

Recursos con estado incorrecto (0) **Recursos con estado correcto (1)** Recursos no aplicables (0)

Buscar máquinas virtuales

Nombre	Suscripción
instancia-UOC-AZ	Evaluación gratuita

Figura 48: Recurso en estado correcto

Aunque no dispone de opciones de remediación automáticas ya integrados en Security Center, sí que dispone de una opción similar, y es una comunidad de Github

con plantillas de corrección ya creadas. Dicha comunidad dispone también de otras recomendaciones adicionales de seguridad [21]

Para la generación de informes, Security Center dispone de un menú llamado Libros (Azure Monitor Workbooks), totalmente personalizable, que nos permite generar informes visuales enriquecidos, usando múltiples fuentes de datos. No obstante, esta opción no se pudo probar por requerir de una suscripción superior a la empleada en nuestro despliegue.

Por último, Security Center integra un sistema de gestión del cumplimiento normativo (ver Figura 49). Dispone de una interfaz sencilla que nos muestra nuestro grado de cumplimiento para los estándares que seleccionemos

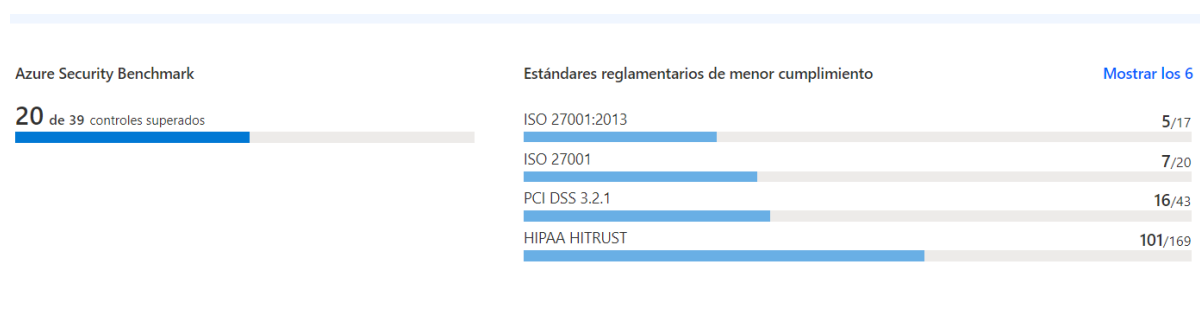


Figura 49: Security Center, cumplimiento

También dispone de una opción para generar informes en formato CSV y PDF.

Podemos administrar por suscripción los estándares revisados, concretamente, tenemos:

- Azure Security Benchmark
- PCI DSS 3.2.1
- ISO 27001
- SOC TSP
- ISO 27001:2013
- Azure CIS 1.1.0
- HIPAA HITRUST
- NIST SP 800-53 R4
- NIST SP 800 171 R2
- UKO and UK NHS
- Canada Federal PBMM
- SWIFT CSP CSCF v2020
- New Zealand ISM Restricted
- CMMC Level 3
- Azure CIS 1.3.0

Veamos ahora el grado de cumplimiento de nuestro despliegue frente a la ISO 27001:2013. Como vemos de la Figura 49, solo se han aprobado 5 **controles** de un total de 17 probados. Si nos vamos al detalle (Figura 50), vemos las 14 secciones por

las que se compone la norma ISO, compuesto por un total de 114 controles. En el detalle, se indica si cada sección aplica a nuestro despliegue, y si ha fallado al menos un control.

▼ ● A.5. Directivas de seguridad de la información
▼ ❌ A.6. Organización de la seguridad de la información
▼ ● A.7. Seguridad de recursos humanos
▼ ● A.8. Administración de activos
▼ ❌ A.9. Control de acceso
▼ ❌ A.10. Criptografía
▼ ● A.11. Seguridad física y medioambiental
▼ ❌ A.12. Seguridad de operaciones
▼ ❌ A.13. Seguridad de las comunicaciones
▼ ● A.14. Adquisición, desarrollo y mantenimiento del sistema
▼ ● A.15. Relaciones de proveedor
▼ ● A.16. Administración de incidentes de seguridad de la información
▼ ● A.17. Aspectos de seguridad de la información de la administración de continuidad empresarial
▼ ● A.18. Cumplimiento

Figura 50: Detalle cumplimiento ISO 27001:2013

Si ampliamos la sección A10 de criptografía (Figura 51), vemos los controles criptográficos probados. El A.10.1.1 aplica el otro despliegue, mientras que el otro no

❌ A.10.1.1. Directiva sobre el uso de los controles criptográficos Detalles del control C
Responsabilidad del cliente
Audit Windows machines that do not store passwords using reversible encryption
El cifrado de disco se debe aplicar en las máquinas virtuales.
Recomendación de acceso a las aplicaciones de funciones solo a través de HTTPS Quick Fix!
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identit
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs

Figura 51: Controles criptográficos

Para cada control, se nos indica los recursos en los que se ha probado dicho control, y cuáles de ellos ha fallado. Si entramos en detalle en cada uno (Figura 52), volvemos a la situación de las recomendaciones de seguridad indicadas anteriormente, se nos permite desencadenar una Logic App para solucionarlo, o una guía para implantarlo manualmente.

Inicio > Security Center >

El cifrado de disco se debe aplicar en las máquinas virtuales. ...

ISO 27001:2013

[Exención](#) [Ver definición de la directiva](#) [Abrir consulta](#)

Gravedad

Alta

Intervalo de actualización

 **24 horas**
Descripción

Cifre los discos de máquinas virtuales con Azure Disk Encryption tanto para máquinas virtuales Windows como Linux. Azure Disk Encryption (ADE) aprovecha la característica BitLocker de Windows estándar del sector y la característica DM-Crypt de Linux para proporcionar cifrado de datos y del SO para ayudar a proteger y salvaguardar los datos y ayudarle a cumplir con los compromisos de seguridad y cumplimiento en el almacén de claves de Azure de cliente. Si el requisito de seguridad y cumplimiento exige que cifre los datos de un extremo a otro con claves de cifrado, incluido el cifrado del disco efímero (temporalmente conectado de forma local), use el cifrado de discos de Azure. También, de manera predeterminada, los discos administrados están cifrados en reposo con Azure Storage Service Encryption, donde las claves de cifrado son claves administradas de Microsoft en Azure. Si esto cumple con sus requisitos de seguridad y cumplir puede aprovechar el cifrado de discos administrados predeterminado para cumplir con los requisitos.

Pasos para la correcciónCorrección manual:Para habilitar el cifrado de disco en las máquinas virtuales, siga las [instrucciones de cifrado](#).**Recursos afectados**
Recursos con estado incorrecto (1) Recursos con estado correcto (0) Recursos no aplicables (0)

 Nombre

  instancia-UOC-AZ

Figura 52: Detalle control no conforme de cumplimiento

Para algunos recursos y controles, la aplicación los marca como “Quick fix”, por lo que es posible corregir el error automáticamente tocando un botón. Veamos el caso de la “Recomendación de acceso a las aplicaciones de funciones solo a través de HTTPS”

^ ✖ A.10.1.1. Directiva sobre el uso de los controles criptográficos [Detalles del control](#) C

Responsabilidad del cliente

[Audit Windows machines that do not store passwords using reversible encryption](#)

[El cifrado de disco se debe aplicar en las máquinas virtuales.](#)

[Recomendación de acceso a las aplicaciones de funciones solo a través de HTTPS](#) Quick Fix!

[Add system-assigned managed identity to enable Guest Configuration assignments on virtual m](#)

Figura 53: Prueba de Quick Fix

Al hacer click en corregir y esperar los 30 minutos de intervalo de actualización (Figura 54), vemos que ya se ha solucionado el problema (Figura 55)

Recomendación de acceso a las aplicaciones de funciones solo a través de HTTPS

ISO 27001:2013

[Exención](#) [Ver definición de la directiva](#) [Abrir consulta](#)

Gravedad

Medio

Intervalo de actualización

 30 min

^ Descripción

El uso de HTTPS garantiza la autenticación del servicio y el servidor, y protege los datos en tránsito frente a ataques de interceptación de nivel de red.

^ Pasos para la corrección

^ Recursos afectados

Recursos con estado incorrecto (1) Recursos con estado correcto (0) Recursos no aplicables (0)

 Nombre

  function-uoc-az
Corregir

Desencadenar aplicación lógica

Exención

Figura 54: Corregir hallazgo

Recomendación de acceso a las aplicaciones de funciones solo a través de HTTPS ...

ISO 27001:2013

[Exención](#) [Ver definición de la directiva](#) [Abrir consulta](#)

Gravedad

Medio

Intervalo de actualización

 30 min

^ Descripción

^ Pasos para la corrección

^ Recursos afectados

Recursos con estado incorrecto (0) **Recursos con estado correcto (1)** Recursos no aplicables (0)

Nombre

↑↓

Suscripción

 function-uoc-az

Evaluación gratuita

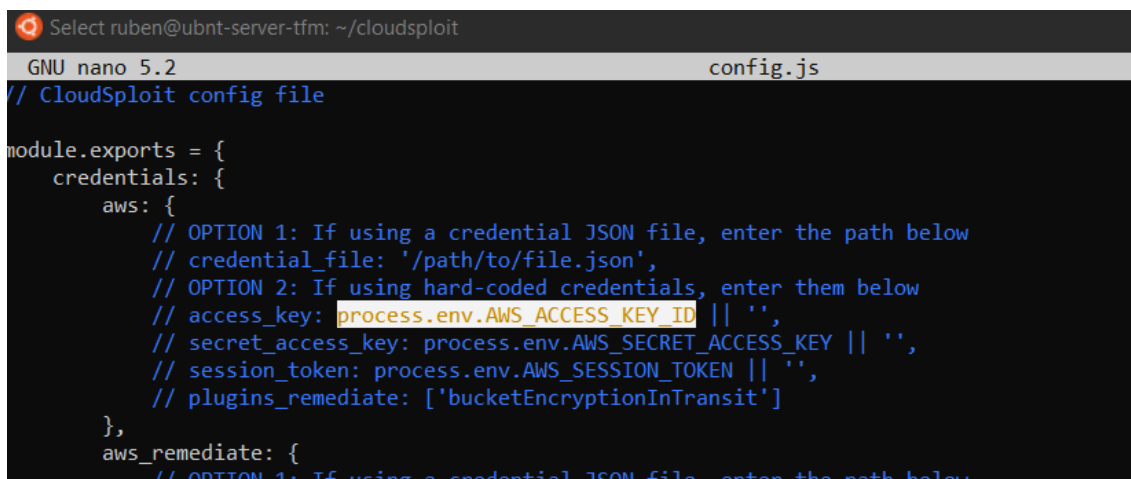
Figura 55: Solución del hallazgo

5.2.3. CloudSploit

CloudSploit es la alternativa OpenSource CSPM de Aqua Security. Esta herramienta se ha instalado sobre una máquina virtual Linux on-premises, aunque se hubiese

podido instalar en una IaaS en cualquiera de los proveedores o incluso, en un servicio PaaS de contenedores.

Para su instalación y configuración, se han seguido las instrucciones de su página de GitHub [22]. Para poder conectar con cada una de las nubes, es necesario configurar las credenciales de la API de cada uno de los proveedores, de manera que CloudSploit pueda conectarse y leer/editar (según el permiso otorgado) las configuraciones realizadas. La creación de estas credenciales se realiza a través del portal web de cada uno de los proveedores. Para AWS, por ejemplo, primero debía crearse un usuario con acceso a programación, darle permiso de auditoría (además de otros específicos de control de logs) y posteriormente se generaban un par de claves (clave de acceso y clave de acceso secreta) que debían introducirse en el fichero config.js de CloudSploit (Figura 56). Es necesario aclarar que estas instrucciones indican cómo crear los usuarios con permisos de lectura, por lo que no podrán editar las configuraciones en caso de usar la función de remediación.



```

Select ruben@ubnt-server-tfm: ~/cloudsploit
GNU nano 5.2 config.js
// CloudSploit config file

module.exports = {
  credentials: {
    aws: {
      // OPTION 1: If using a credential JSON file, enter the path below
      // credential_file: '/path/to/file.json',
      // OPTION 2: If using hard-coded credentials, enter them below
      // access_key: process.env.AWS_ACCESS_KEY_ID || '',
      // secret_access_key: process.env.AWS_SECRET_ACCESS_KEY || '',
      // session_token: process.env.AWS_SESSION_TOKEN || '',
      // plugins_remediate: ['bucketEncryptionInTransit']
    },
    aws_remediate: {
      // OPTION 1: If using a credential JSON file, enter the path below

```

Figura 56: Fichero config.js

Para facilitar el uso de la herramienta, y dividir la ejecución por proveedor de nube, se han creado tres archivos de configuración diferentes (config_aws.js, config_az.js y config_gcp.js).

Dentro del directorio “plugin” de la herramienta, tenemos una carpeta por cada proveedor de nube soportado (AWS, GCP, AZ y OCI). Dentro de cada proveedor, tenemos todos los servicios de nube soportados para dicho CSP, y dentro a su vez, tantos ficheros (o plugins/extensiones) como controles a probar por cada servicio. La Tabla 4 muestra la relación de plugins por CSP soportado

Tabla 4: CloudSploit, controles por CSP

CSP	Nº de servicios soportados
AWS	45
GCP	10
AZ	25
OCI	8

Dentro de los ficheros que contienen los controles a probar, se especifica si ese control específico aplica para alguno de los estándares de cumplimiento soportados por la aplicación. Es decir, a diferencia de las herramientas anteriores donde los estándares de cumplimiento son una recopilación de controles, aquí tenemos que es cada control el que tiene definido si aplica o no para un estándar de cumplimiento determinado, lo que supone una mayor complejidad a la hora de mantener la herramienta.

CloudSploit, a diferencia de las anteriores, no dispone de interfaz gráfica, y para interactuar con ella se debe hacer a través de línea de comandos. Las diferentes opciones que permite la herramienta se observan en la Tabla 5.

Tabla 5: CloudSploit, órdenes y descripción

Orden	Descripción
--config	Especifica el archivo de configuración a emplear, con las credenciales de acceso necesarias
--compliance {hipaa,cis,cis1,cis2,pci}	Indica qué estándar de cumplimiento probar entre los 3 disponibles (CIS aplica para CIS nivel 1 y CIS nivel 2 a la vez)
--plugin PLUGIN	Especifica qué conjuntos de controles específicos se probarán
--csv CSV, --json JSON, --junit JUNIT, --console {none,text,table}	Función de informe, con diferentes formatos de salida, por fichero o consola
--ignore-ok	Ignora los controles probados que están correctos
--suppress REGEX	Elimina los resultados de salida según la expresión regular añadida (regiones, plugin o recursos)
--remediate	Ejecutar la remediación (automática o muestra una guía paso a paso) de los plugin seleccionados. Esta opción está en desarrollo actualmente y solo soporta AWS por el momento.

Haremos un ejemplo con Azure. Mediante la siguiente orden (Tabla 6), validamos el control del nivel mínimo de versión de TLS empleado en AppServices (Azure Functions), usando el archivo de configuración de Azure, mostrando solo recursos que no hayan pasado el control, dando de formato de salida la tabla por consola.

Tabla 6: CloudSploit, TLSVersionCheck

```
./index.js --config ./config_az.js --plugin tlsVersionCheck --ignore-ok --console table
```

Tras unos segundos, obtenemos el resultado visto en la Figura 57. Se observa que hay un recurso, de categoría AppService, llamado function-UOC-AZ, que ha fallado en ese control en la región del norte de Europa.

Category	Plugin	Description	Resource	Region	Status	Message
App Service	TLS Version Check	Ensures that all web apps are using the latest version of TLS	/subscriptions/fc5cd4b8-239f-48f1-9d90-2d3ba394de9b/resourceGroups/RG-TFM-UOC/providers/Microsoft.Web/sites/function-UOC-AZ	north europe	FAIL	Minimum TLS version is not 1.2

Figura 57: CloudSploit, resultado TLSVersionCheck

Para probar la característica de remediación de CloudSploit, debemos emplear AWS, pues es el único soportado en el momento de redactar esta memoria. Probaremos la opción de encriptación del bucket, que ahora mismo está desactivada, y produce fallo de control. Si ejecutamos la orden de la Tabla 7, vemos que nos devuelve dos recursos afectados (bucket-uoc-tfm y config-bucket-108388023247) en la región global (ver Figura 58)

Tabla 7: CloudSploit, AWS, comprobar encriptación de bucket

```
./index.js --config ./config_aws.js --ignore-ok --plugin bucketEncryption
```

Category	Plugin	Description	Resource	Region	Status	Message
S3	S3 Bucket Encryption	Ensures object encryption is enabled on S3 buckets	arn:aws:s3:::bucket-uoc-tfm	global	FAIL	Bucket: bucket-uoc-tfm has encryption disabled
S3	S3 Bucket Encryption	Ensures object encryption is enabled on S3 buckets	arn:aws:s3:::config-bucket-108388023247	global	FAIL	Bucket: config-bucket-108388023247 has encryption disabled

INFO: Scan complete
AccessDenied: Access Denied

Figura 58: CloudSploit, AWS, resultado encriptación de bucket

Para poder ejecutar la remediación, es necesario otorgar privilegios de escritura en configuraciones para el usuario de CloudSploit creado en AWS, para ello, le añadimos el role AWSConfigRole a través de la consola.

Si ahora ejecutamos la orden de la Tabla 8, y volvemos a re-ejecutar la comprobación inicial, vemos como los buckets pasan a estar todos OK, y que se ha aplicado AES256 como cifrado (ver Figura 59).

Tabla 8: CloudSploit, AWS, remediación

```
./index.js --config ./config_aws.js --remediate bucketEncryption
```

Category	Plugin	Description	Resource	Region	Status	Message
S3	S3 Bucket Encryption	Ensures object encryption is enabled on S3 buckets	arn:aws:s3:::bucket-uoc-tfm	global	OK	Bucket: bucket-uoc-tfm has AES256 encryption enabled
S3	S3 Bucket Encryption	Ensures object encryption is enabled on S3 buckets	arn:aws:s3:::config-bucket-108388023247	global	OK	Bucket: config-bucket-108388023247 has AES256 encryption enabled

Figura 59: CloudSploit, AWS, re-comprobación

Si accedemos a través del portal de AWS, aparecen reflejados los cambios. A la izquierda de la Figura 60 se observa el cifrado previo a la remediación, y a la derecha tras realizar la acción en CloudSploit.



Figura 60: Cifrado de bucket antes y después, vía panel de AWS

Las últimas opciones a probar de la herramienta son la de cumplimiento y exportación. Recordemos que CloudSploit es compatible con los estándares de cumplimiento y guías de buenas prácticas HIPAA, PCI DSS, CIS Benchmark nivel 1 y nivel 2. Por otro lado, soporta exportaciones básicas en formato CSV y JSON para su fácil integración con otras herramientas. Para hacer la prueba, comprobaremos el cumplimiento de nuestro despliegue en GCP, frente al estándar PCI DSS, dando la salida en formato CSV. Ejecutando la orden de la Tabla 9, se obtiene un CSV con el resultado.

Tabla 9: CloudSploit, GCP, compliance en PCI DSS

```
./index.js --config ./config_gcp.js --compliance pci --csv gcp_pci_compliance.csv
```

Vemos que nuestro despliegue en GCP tan solo tiene dos categorías de recursos que disponen de controles en CloudSploit sujetos al estándar PCI DSS, que son, las redes privadas virtuales (VPC) y la gestión de identidades (IAM). Para cada categoría, solo se ha probado un control (registros de red activos y rotación de claves cada 90 días). Como vemos en la Tabla 10, el control de los registros de red ha fallado en 20 recursos desplegados. Si recordamos, todo nuestro despliegue se realizó en la región us-central1, por lo que no tendría sentido el resto de las regiones en las que ha fallado dicho control. Si acudimos al dashboard de GCP (Figura 61), y vamos a la VPC usada por la máquina virtual, observamos que dicha VPC creada por defecto crea una subred por cada región disponible de Google Cloud, lo que explica que ese control haya fallado en 20 ocasiones. El resultado en CSV exportado se puede ver en la Tabla 10.

Name ↑	Region	Subnets	MTU ⓘ	Mode	IP address ranges
▼ default		25	1460	Auto ▼	
	us-central1	default			10.128.0.0/20
	europa-west1	default			10.132.0.0/20
	us-west1	default			10.138.0.0/20
	asia-east1	default			10.140.0.0/20
	us-east1	default			10.142.0.0/20
	asia-northeast1	default			10.146.0.0/20

```
{
  "gatewayAddress": "10.132.0.1",
  "id": "1420440847273106648",
  "ipCidrRange": "10.132.0.0/20",
  "name": "default",
  "networkUrl": "projects/uoc-tfm-project/global/networks/default",
  "regionUrl": "projects/uoc-tfm-project/regions/europe-west1",
  "selfLink": "projects/uoc-tfm-project/regions/europe-west1/subnetworks/default"
}
```

Figura 61: GCP, una VPC por región

Tabla 10: Resultado VPC GCP

category	title	resource	region	statusWord
VPC Network	Flow Logs Enabled	53031111150476504	us-east1	FAIL
VPC Network	Flow Logs Enabled	201867960491305288	us-east4	FAIL
VPC Network	Flow Logs Enabled	368613082571178722	us-west1	FAIL
VPC Network	Flow Logs Enabled	858775711843556568	us-west2	FAIL
VPC Network	Flow Logs Enabled	852862284182343599	us-central1	FAIL
VPC Network	Flow Logs Enabled	335409795500887983	northamerica-northeast1	FAIL
VPC Network	Flow Logs Enabled	342808083550641368	southamerica-east1	FAIL
VPC Network	Flow Logs Enabled	142044084727310664	europa-west1	FAIL
VPC Network	Flow Logs Enabled	770462201019230536	europa-west2	FAIL
VPC Network	Flow Logs Enabled	188257231034614498	europa-west3	FAIL
VPC Network	Flow Logs Enabled	145744120025416418	europa-north1	FAIL
VPC Network	Flow Logs Enabled	728451102967458120	asia-south1	FAIL
VPC Network	Flow Logs Enabled	568956127919388181	asia-southeast1	FAIL
VPC Network	Flow Logs Enabled	363471364620255970	asia-east1	FAIL
VPC Network	Flow Logs Enabled	187116508336639919	asia-east2	FAIL
VPC Network	Flow Logs Enabled	446652364750081967	asia-northeast1	FAIL
VPC Network	Flow Logs Enabled	397067363178716376	asia-northeast2	FAIL
VPC Network	Flow Logs Enabled	626241329260102370	australia-southeast1	FAIL
IAM	Service Account Rotation Key	6a579d0dcd8390800a4a763f6e01916466ff49e4	global	OK
IAM	Service Account Rotation Key	875d58338eb3e50286ebfd47b74c07f3f4e76a20	global	OK

Aclarar que, aunque en estos ejemplos hemos realizado pruebas de los diferentes CSP por separado, es posible crear un único archivo de configuración con todas las credenciales de acceso para cada proveedor, y obtener una única salida.

Por último, aunque los catálogos de controles revisados para cada servicio y nube, y las plantillas de cumplimiento disponibles pueden no parecer muy amplias en comparación a otras herramientas, CloudSploit tiene un potencial enorme al ser una aplicación Open Source. Su código fuente en Node.js está disponible en GitHub [22], con multitud de comentarios en su interior que facilitan su comprensión. Además, disponen de una guía en la que explican cómo desarrollar extensiones (plugins) propios, por lo que ampliar la funcionalidad de la herramienta podría ser relativamente sencillo para una empresa que cuente con un equipo de desarrollo.

5.2.4. Palo Alto Prisma Cloud

La última herramienta se trata de la propietaria de Palo Alto, Prisma Cloud. Esta herramienta se distribuye en modalidad SaaS, accesible vía web mediante la URL <https://login.paloaltonetworks.com/>, y pertenece a un hub de aplicaciones mucho mayor, que integran otras funcionalidades como DLP, seguridad de IoT, entre otros.

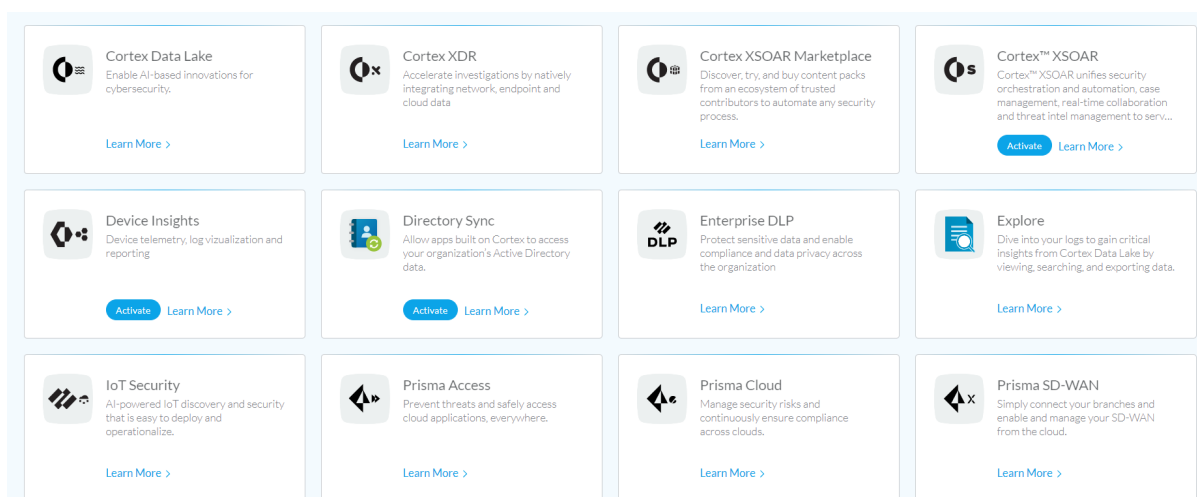
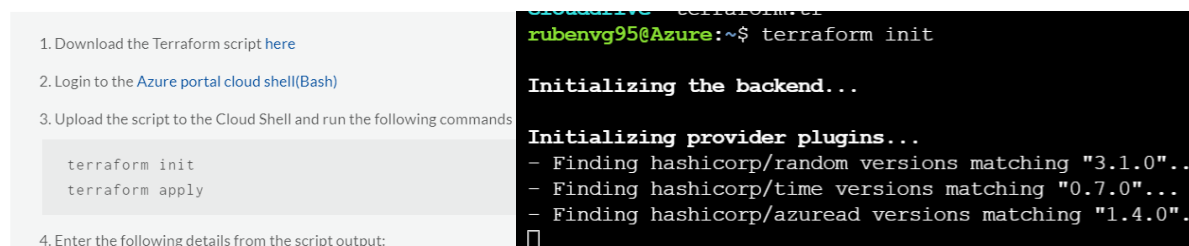


Figura 62: Hub de aplicaciones de Palo Alto para nube

El módulo de Prisma Cloud, dispone de una demo de 30 días, sin limitaciones. Con esta herramienta, hemos conectado las cuentas de los 3 proveedores que hemos creado para el laboratorio. Para conectar cada uno de los proveedores, Prisma Cloud dispone de una guía paso a paso con la que asistir a los usuarios, con scripts en Terraform para la automatización de la creación de usuarios en las diferentes nubes. Lo que es un punto diferenciador con respecto a la herramienta CloduSploit. En la Figura 63, se observa este proceso para Azure:

Account Details



```

1. Download the Terraform script here
2. Login to the Azure portal cloud shell\(Bash\)
3. Upload the script to the Cloud Shell and run the following commands
  terraform init
  terraform apply
4. Enter the following details from the script output:
  
```

```

cloudshell@cloudshell:~$ terraform init
Initializing the backend...
Initializing provider plugins...
- Finding hashicorp/random versions matching "3.1.0"...
- Finding hashicorp/time versions matching "0.7.0"...
- Finding hashicorp/azuread versions matching "1.4.0"...
  
```

Figura 63: Script Terraform para la creación del usuario

Tras vincular cada una de las cuentas, debemos esperar varias horas para que Prisma Cloud encuentre todos los recursos creados en las diferentes nubes y genere las alertas pertinentes ante las violaciones en las políticas predefinidas en la aplicación. Tras realizar la configuración de cuentas, nos encontramos un panel lateral para ir navegando por las diferentes opciones de la herramienta. Dicho panel contiene opciones que requieren otros módulos que no están habilitados, por lo que no se podrán usar.

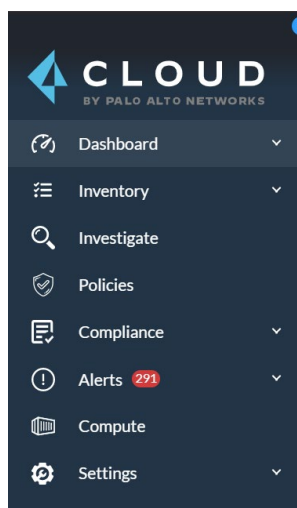


Figura 64: Panel lateral de Prisma Cloud

El primer punto, el “Dashboard”, nos muestra un panel con gráficas, indicando los aspectos más relevantes como: alertas por nivel de severidad, tipos de violaciones de políticas, recursos y cuentas monitorizadas, e incluso analíticas del tráfico de red generado (ver Figura 65)

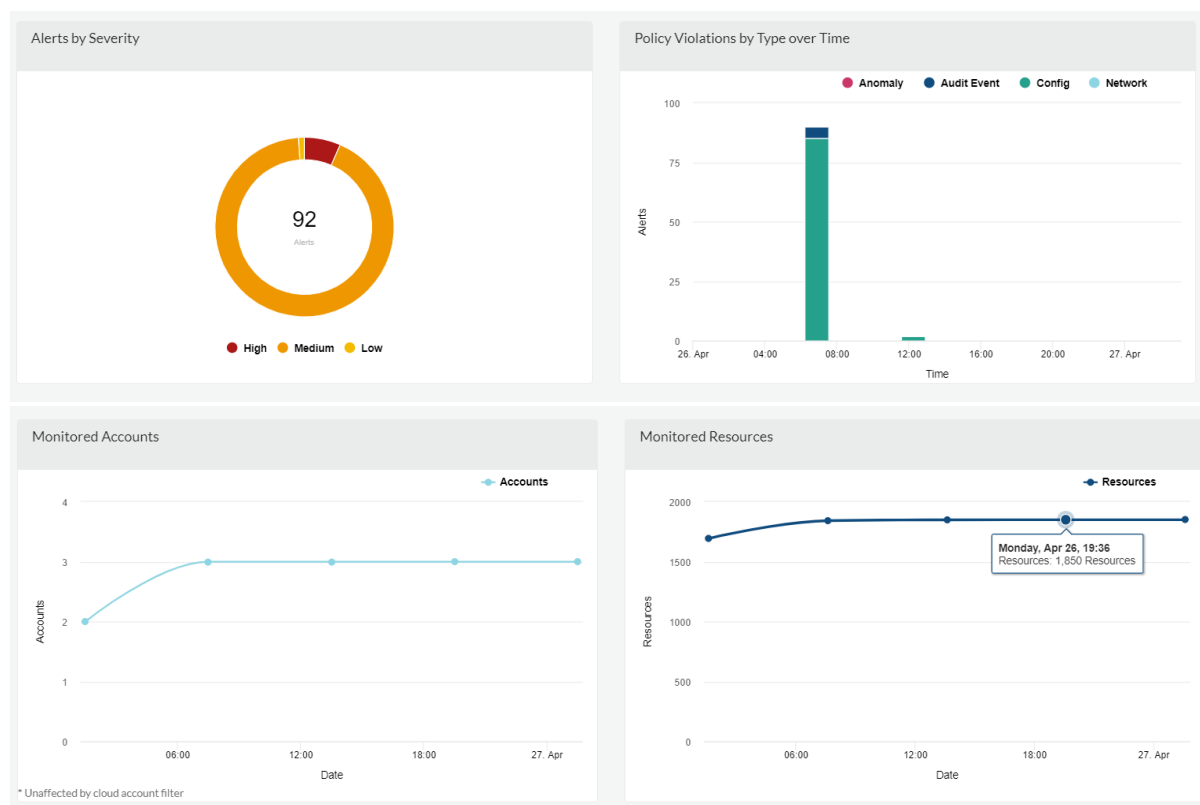


Figura 65: Dashboard de Prisma Cloud

Los siguientes menús, desglosan cada uno de los puntos vistos en este Dashboard. El de inventario (Figura 66), muestra los todos los recursos a los que la plataforma tiene acceso, indicando el número de recursos que han pasado/aprobado las políticas establecidas por la plataforma, y cuales han fallado. La herramienta dispone en la gran mayoría de menús opciones de exportación en CSV y creación de informes ejecutivos en PDF.

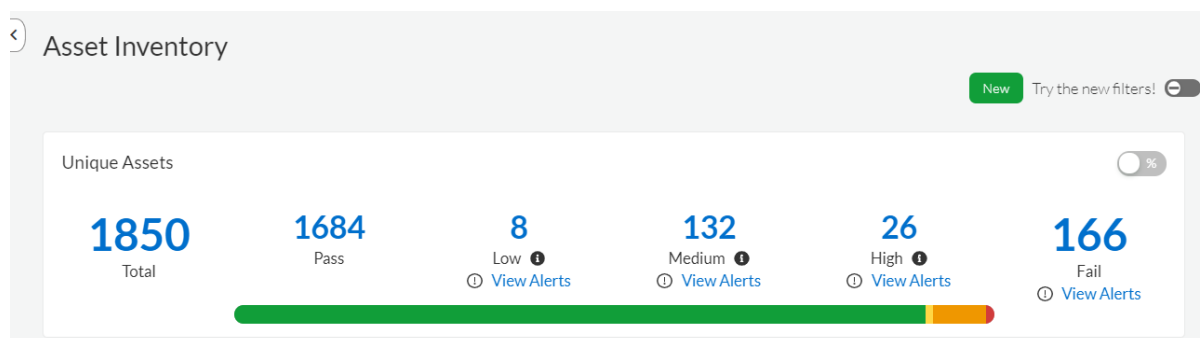


Figura 66: Inventario de activos en la nube

En este mismo bloque, viene una tabla detallando el número de recursos encontrados de cada tipo, y el número de esos recursos que han pasado las políticas definidas y los que han fallado. También clasifica esos recursos por severidad si no han pasado las políticas. En este menú, tomaremos de ejemplo la configuración del servicio AWS S3. Vemos en la Figura 67 que, de un total de 3 recursos definidos, en los que 2 de

ellos han violado la política definida por Prisma Cloud, con severidad alta. Si entramos en los detalles, vemos primero los dos buckets que han creado el conflicto

SERVICE NAME ↓↑	CLOUD ↓↑	TOTAL ↓↑	PASS ↓↑	FAIL ↓	HIGH ↓↑
Amazon S3		3	1	ⓘ 2	ⓘ 2

RESOURCE NAME ↓↑	CLOUD ↓↑	ACCOUNT ID ↓↑	ACCOUNT NAME ↓↑	RESOURCE ID ↓↑
config-bucket-108388023247		108388023247	AWS Account UOC	config-bucket-108388023247
bucket-uoc-tfm		108388023247	AWS Account UOC	bucket-uoc-tfm

Figura 67: Prisma Cloud, recurso S3 de AWS afectado

Si entramos a ver qué política han infringido, vemos la siguiente (Figura 68), que es debido a el no bloqueo de acceso público del bucket. También nos marca la política como “Remediable” (tic verde), lo que significa que dispone de medidas de auto remediación.

Alerts Overview

Group By 1 alerts on 1 policies

<input type="checkbox"/>	Policy Name ↓↑	Alerts ↓	Policy Type ↓↑	Severity ↓↑
<input type="checkbox"/>	AWS S3 Buckets Block public access setting disabled	1	Config	●●● High

Figura 68: Prisma Cloud, S3 con acceso publico

Por otro lado, para esa política, la herramienta también indica qué estándar de cumplimiento normativo está violando, y nos permite aplazar o descartar esa alerta.

Si ahora vamos al menú de “Policies” (o políticas), podemos navegar entre todas las que dispone la herramienta, un total de 752 políticas para los 5 proveedores de nube cubiertos por la aplicación. Si buscamos la política anterior “AWS S3 Buckets Block public access setting disabled”, vemos una guía de 8 pasos para remediar manualmente el hallazgo (ver Figura 69).

AWS S3 Buckets Block public access setting disabled

This policy identifies AWS S3 buckets which have 'Block public access' setting disabled. Amazon S3 provides 'Block public access' setting to manage public access of AWS S3 buckets. Enabling recommended to enable 'Block public access' setting for all AWS s3 buckets appropriately.

Recommendation

1. Login to the AWS Console
2. Navigate to the 'S3' service
3. Click on the 'S3' resource reported in the alert
4. Click on the 'Permissions'
5. Under 'Block public access' click on 'Edit'
6. Select 'Block all public access' checkbox
7. Click on Save
8. 'Confirm' the changes

Note: Make sure updating 'Block public access' setting does not affect S3 bucket data access.

Figura 69: Prisma Cloud, guía de remediación manual.

Si vamos al editor de políticas, y buscamos la anterior, podemos incluso editarla para cambiar datos, severidad, la query que realiza a nivel de API para comprobar la política, para qué control de cada estándar de cumplimiento aplica y, por último, la guía de remediación del control tanto de forma manual, como mediante el CLI (Figura 70).

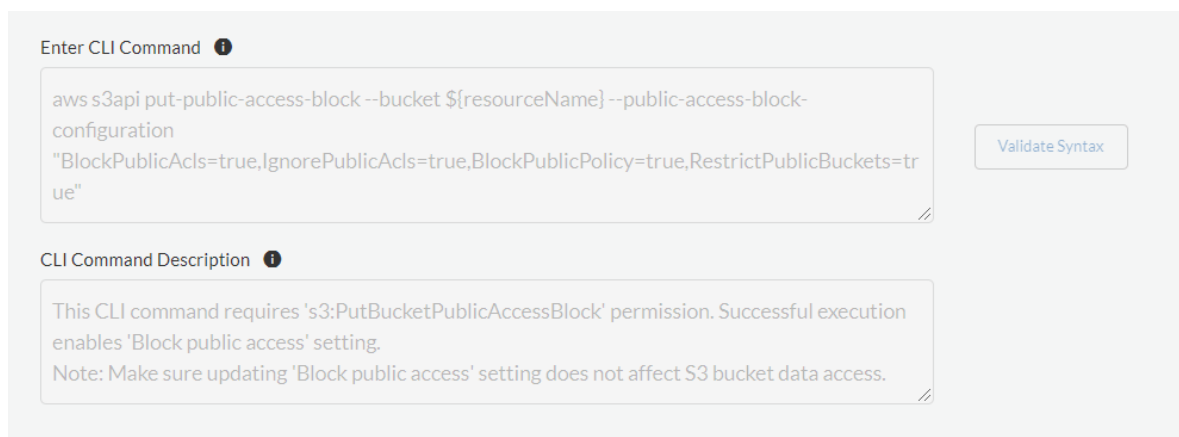


Figura 70: Comando CLI para remediación automática

Si ahora vamos al menú de “Alerts”, y buscamos la alerta creada por la violación de la política anterior, volvemos a ver los recursos afectados. Esta vez, además de darnos la guía manual de cómo remediar el control, tenemos un botón para iniciar nosotros la remediación, que empujará el comando de CLI anterior (ver Figura 71)

ALERT ID ↓↑	RESOURCE NAME ↓↑	OPTIONS
P-27	bucket-uoc-tfm 🔗	<input type="button" value="📄"/> <input type="button" value="🕒"/> <input type="button" value="Remediate"/>

Figura 71: Recurso afectado y remediación de la política

Si le damos a “Remediate”, nos pide confirmar el comando del CLI. Tras su ejecución, la alerta desaparece, y el fichero de AWS S3 expuesto públicamente deja de ser accesible (Figura 72), desapareciendo todas las alertas en la aplicación sobre S3 para ese recurso.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>6E1RQJMRW7CMA00Q</RequestId>
  <HostId>TnT8mgRnZl6XtPdJoaajsnd2zxDb4Vvk959zJmABh0H1sWNd59xrHoRz0fvijt1F+b+dIkAaig8s=</HostId>
</Error>

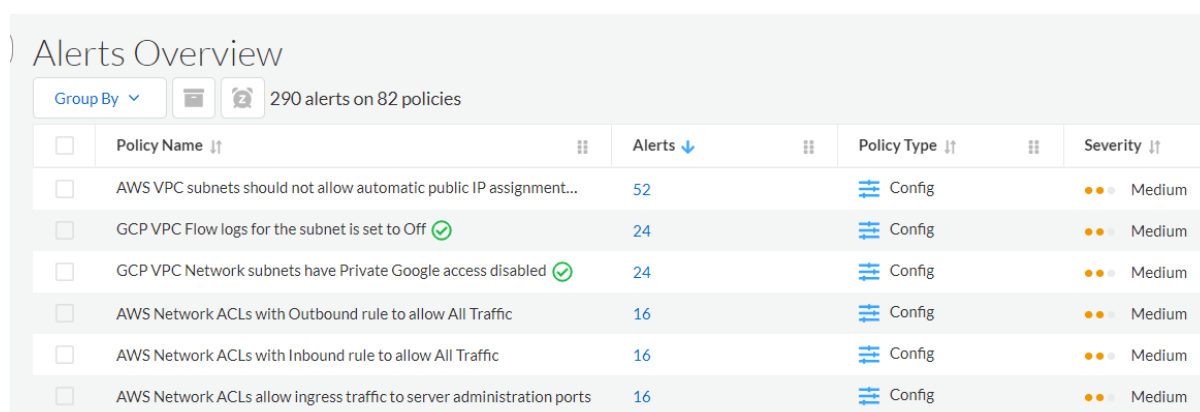
```

Figura 72: Acceso denegado al fichero del bucket de S3

Aclarar que Prima Cloud no dispone de remediaciones para todas las políticas creadas. De un total de 752, tan solo 92 de ellas (menos del 15%) están marcadas

como “Remediable”. No obstante, como hemos visto, cada política es fácilmente editable, además de poder crear nosotros nuestra política personalizada. Indicar también que, entre esas 752 políticas, no todas son sobre configuraciones anómalas, sino que también existen políticas de comportamiento de usuarios, protección de red, monitoreo de la actividad de usuarios privilegiados, y vulnerabilidades.

En el menú de “Alerts” (Figura 73) se representan todas las alertas (o violaciones de políticas) que han surgido en el análisis llevado a cabo por Prisma Cloud. Nos permite crear también informes con todas las alertas surgidas (informe ejecutivo o informe para evaluación de seguridad en la nube).



<input type="checkbox"/>	Policy Name ↑↓	Alerts ↓	Policy Type ↑↓	Severity ↑↓
<input type="checkbox"/>	AWS VPC subnets should not allow automatic public IP assignment...	52	Config	Medium
<input type="checkbox"/>	GCP VPC Flow logs for the subnet is set to Off ✓	24	Config	Medium
<input type="checkbox"/>	GCP VPC Network subnets have Private Google access disabled ✓	24	Config	Medium
<input type="checkbox"/>	AWS Network ACLs with Outbound rule to allow All Traffic	16	Config	Medium
<input type="checkbox"/>	AWS Network ACLs with Inbound rule to allow All Traffic	16	Config	Medium
<input type="checkbox"/>	AWS Network ACLs allow ingress traffic to server administration ports	16	Config	Medium

Figura 73: Listado de alertas de Prisma Cloud

También dispone de un motor reglas (Figura 74) que nos van a permitir notificar por diferentes vías las alertas surgidas, en el que incluso podemos añadir una plantilla para la alerta. Entre los diferentes sistemas de notificación, encontramos integraciones con ServiceNow, Jira, Slack, hasta el envío de un simple correo electrónico.

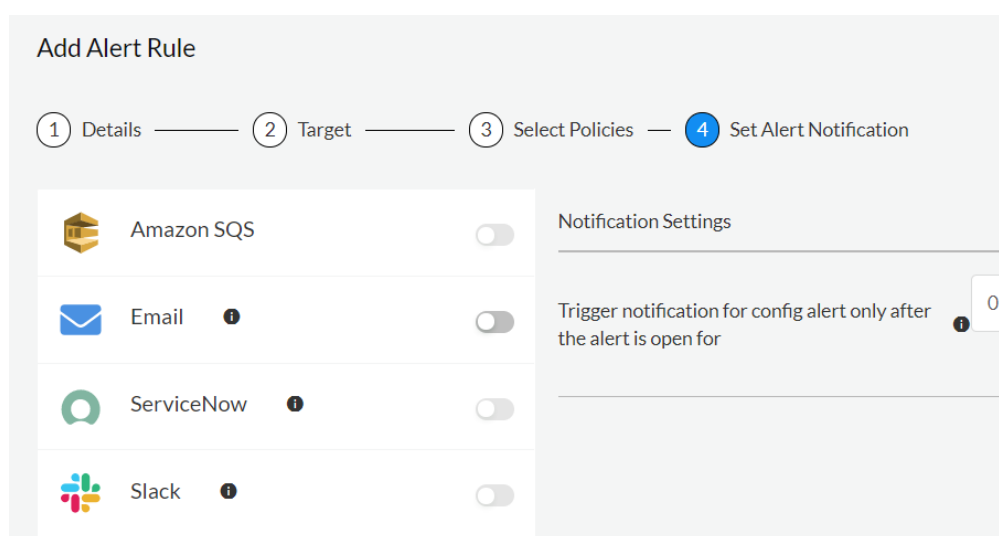


Figura 74: Motor de reglas de Prisma Cloud

El siguiente menú de interés para este TFM (el resto están desactivados por depender de servicios externos), es el de “Compliance”. Este menú se subdivide en:

- Un dashboard donde visualizar los gráficamente el grado de cumplimiento normativo de nuestros despliegues mediante gráficas dinámicas. En la Figura 75 se observa el cumplimiento en los diferentes marcos regulatorios, y específicamente para la ISO 27001:2013

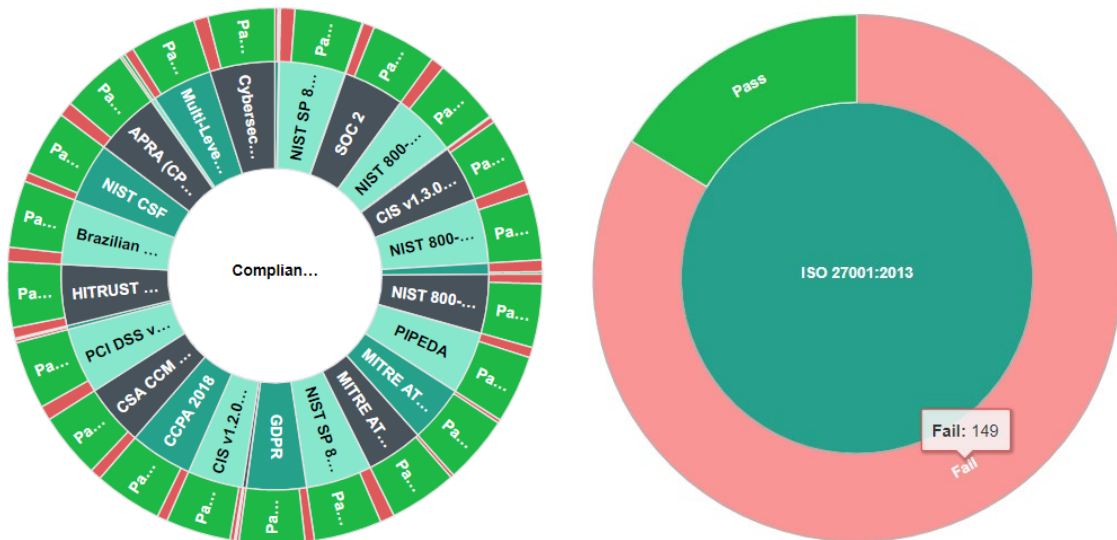


Figura 75: Cobertura de cumplimiento general (izquierda) y específico del ISO 27001:2013 (derecha)

Este apartado también nos incluye un listado detallado de todos los estándares disponibles (Figura 76), las políticas testeadas en cada caso, y cuantos recursos están afectadas, indicando cuales de ellos han cumplido con la política. Dentro de cada estándar en detalle podemos ver qué requerimientos del estándar no se están cumpliendo, y qué política de la aplicación tiene vinculada, además de mostrar el porcentaje de cumplimiento

REQUIREMENT ↓↑	POLICIES ↓↑	COMPLIANCE POSTURE ↓↑
Protection of Records	43	34%
Management of Information Security Incidents and Improvements	34	35%
Security Requirements of Information Systems	44	3%
Asset Management	20	4%
Operations Security	8	0%
Access Control	15	81%
Network Security Management	19	17%
Cryptographic Controls	6	0%
Organization of Information Security	0	0%

Figura 76: Estándares de cumplimiento disponibles

En este submenú, una vez y hemos entrado en el detalle de un estándar, podemos solicitar la generación de un informe y su envío por correo, e incluso automatizar su generación.

- Otro de los menús de la herramienta nos permite descargar los informes generados (una vez y se han solicitado anteriormente)
- El último menú, lista todos los estándares disponibles. La herramienta es compatible con un total de 33 estándares de cumplimiento y códigos de buenas prácticas. Cada estándar, tiene vinculado uno o varios proveedores de nube según su aplicación, y varias políticas que debe cumplir. El listado completo de estándares, indicando el proveedor al que aplica y el número de políticas de Prisma Cloud aplicadas puede verse en la Tabla 11.

Tabla 11: Listado de estándares de cumplimiento por CSP y políticas aplicadas

Estándares de cumplimiento y guías de buenas prácticas soportadas	CSP	Políticas aplicadas
APRA (CPS 234) Information Security	AWS, AZ, GCP	491
Brazilian Data Protection Law (LGPD)	Alibaba, AWS, AZ, GCP	499
CCPA 2018	AWS, AZ, GCP	285
CIS v1.0.0 (Alibaba Cloud)	Alibaba	19
CIS v1.0.0 (GCP)	GCP	51
CIS v1.0.0 (OCI)	OCI	23
CIS v1.1 (Azure)	AZ	80
CIS v1.1.0 (GCP)	GCP	52
CIS v1.1.0 (GKE)	GCP	26
CIS v1.1.0 (OCI)	OCI	22
CIS v1.2.0 (AWS)	AWS	43
CIS v1.2.0 (Azure)	AZ	83
CIS v1.3.0 (AWS)	AWS	45
CIS v1.3.0 (Azure)	AZ	83
CSA CCM v3.0.1	AWS, AZ, GCP	133
Cybersecurity Maturity Model Certification (CMMC) v.1.02	Alibaba, AWS, AZ, GCP	499
GDPR	AWS, AZ, GCP	108
HIPAA	AWS, AZ, GCP	82
HITRUST CSF v9.3	AWS, AZ, GCP	127
ISO 27001:2013	AWS, AZ, GCP	138
MITRE ATT&CK v6.3	AWS, AZ, GCP	194
MITRE ATT&CK v8.2	Alibaba, AWS, AZ, GCP, OCI	267
MPAA Content Protection Best Practices	Alibaba, AWS, AZ, GCP, OCI	147
Multi-Level Protection Scheme (MLPS) v2.0	Alibaba, AWS, AZ	334

NIST 800-171 Rev1	AWS	68
NIST 800-53 Rev 5	Alibaba, AWS, AZ, GCP	375
NIST 800-53 Rev4	Alibaba, AWS, AZ, GCP	453
NIST CSF	AWS, AZ, GCP	109
NIST SP 800-171 Revision 2	Alibaba, AWS, AZ, GCP, OCI	620
NIST SP 800-172	Alibaba, AWS, AZ, GCP, OCI	620
PCI DSS v3.2.1	Alibaba, AWS, AZ, GCP, OCI	625
PIPEDA	AWS, AZ, GCP	287
SOC 2	AWS, AZ, GCP	138

6. Conclusiones

El cloud computing es un sector en alza, en el que se prevé para 2024 (según la consultora Gartner) que el gasto de las organizaciones en este aspecto suponga el 14,2% del gasto total de TI. Las ventajas que supone la adopción del cloud computing para las organizaciones son innegables, dotan de elasticidad, escalabilidad y alta disponibilidad a las cargas de trabajo desplegadas. No obstante, su opacidad, causada mayoritariamente por el desconocimiento en su funcionamiento, unido a los continuos cambios en los servicios ofrecidos y los diferentes modelos de despliegue disponibles, provoca que las organizaciones no sepan identificar correctamente las amenazas a las que se encuentran expuestas. Una de estas principales amenazas son las malas configuraciones, que pueden provocar que datos estén expuestos a Internet abiertamente, o que las medidas de seguridad implementadas para evitar el acceso a un recurso sean débiles.

Debido a esta problemática ha surgido este TFM, en el que se han repasado las diferentes herramientas disponibles para conseguir seguridad en la nube, centrándose en las herramientas CSPM, que buscan precisamente evitar esas malas configuraciones en los entornos cloud/multi-cloud de las organizaciones.

Este TFM ha ayudado a comprender las amenazas más habituales a las que se enfrenta el cloud computing y cuáles son los controles más frecuentemente usados para evitarlas. También se ha conseguido definir cuál es la hoja de ruta necesaria en las organizaciones para conseguir seguridad en la nube pública, haciendo un repaso de los diferentes tipos de herramientas disponibles para evitarlo (CASB, CWPP y CSPM). Por otro lado, en este TFM no nos hemos quedado solo en el terreno teórico, sino que se han analizado algunas de las soluciones CSPM disponibles en el mercado y se han implantado algunas de ellas en un entorno de laboratorio, que nos han ayudado a entender mejor el funcionamiento de este tipo de herramientas y sus características en mayor profundidad, conociendo cuales son los puntos clave a la hora de elegir entre una u otra solución.

Podemos concluir entonces que, para este TFM, se han cumplido todos los principales objetivos propuestos, en el que se ha seguido la metodología de tres fases indicada. No obstante, sí que hubo desviaciones en la planificación inicial, ya que la fase teórica se retrasó alrededor de dos semanas debido al gran número de herramientas CSPM localizadas, lo que requirió más tiempo para su análisis. Debido a esto, hubo que acortar la fase práctica y limitar las pruebas realizadas a solo ciertos recursos desplegados en la nube.

Este TFM deja abiertas varias líneas de trabajo futuras. Al igual que se han analizado las herramientas CSPM, se podría hacer un análisis teórico y un despliegue práctico de los otros dos tipos de herramientas citados, las CASB y las CWPP, lo que supondría cubrir la totalidad de los diferentes modelos de despliegue en la nube. Otra alternativa sería orientar el trabajo a un enfoque más práctico, desplegando en la nube

un entorno más complejo, en el que se ejecuten soluciones de negocio (ERP, CRM, etc.) en diferentes nubes y emplear herramientas CSPM para fortificar dicho despliegue, y cumplir algún estándar de cumplimiento propuesto

7. Glosario

Definición de los términos y acrónimos más relevantes utilizados dentro de la Memoria.

Término/Abreviatura	Definición
TI	Tecnologías de la información
CASB	Cloud Access Security Brokers
CWPP	Cloud Workload Protection Platforms
CSPM	Cloud Security Posture Management
IaaS	Infraestructure as a Service o Infraestructura como servicio
PaaS	Platform as a Service o Plataforma como Servicio
SaaS	Software as a Service o Software como Servicio
CSP	Cloud Service Provider
AWS	Amazon Web Services
AZ	Azure
GCP	Google Cloud Platform
OpEx	Operation Expenditures, o costes de operación
SLA	Service Level Agreement
RAM	Random Access Memory
CPU	Centro Processing Unit
VM o MV	Virtual Machine o Máquina Virtual
OS o SO	Operating System o Sistema Operativo
DBaaS	DataBase as a Service o base de datos como servicio
DaaS	Desktop as a Service o escritorio como servicio
BaaS	Backup as a Service o copia de respaldo como servicio
CSA	Cloud Security Alliance
INCIBE	Instituto Nacional de Ciberseguridad de España
INTECO	Instituto de Tecnologías de la Comunicación
NIST	National Institute of Standards and Technology
CCM	Cloud Controls Matrix
ISO	International Organization for Standardization o Organización Internacional de Normalización
API	Application Programming Interfaces
CSC	Cloud Service Client
SABSA	Sherwood Applied Business Security Architecture
WAF	Web Application Firewalls
SWG	Secure Web Gateways
EDR	Endpoint Detection and Response
DNS	Domain Name System
SSO	Single Sign-On
EFW	Enterprise Firewalls
DLP	Data Loss Prevention
UEBA	User and Entity Behavior Analytics
AAC	Adaptive access control
PAC	Proxy Auto Configuration

PEC	Prueba de Evaluación Continua
SOC	System and Organization Controls
CIS	Center for Internet Security
DevOps	Development and operations
SASE	Secure Access Service Edge
CRM	Customer Relationship Management
OCI	Oracle Cloud Infraestructure
ASFF	AWS Security Finding Format
SQL	Structured Query Language
SDK	Software development kit
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guides
SSH	Secure SHell
EBS	Amazon Elastic Block Store
EC2	Amazon Elastic Compute Cloud
S3	Amazon Simple Storage Service
IP	Internet Protocol
IoT	Internet of Things, o Internet de las Cosas
CSV	Comma-separated values
JSON	JavaScript Object Notation

8. Bibliografía

- [1] Gartner, “Public Cloud Services, Worldwide, 2018-2024, 3Q20 Update,” 2020. [Online]. Available: <https://www.gartner.com/en/documents/3987438/forecast-public-cloud-services-worldwide-2018-2024-2q20->.
- [2] “Gartner Invest Analyst Insight: Catalyst 2019 — Cloud Security 201: CASB, CSPM, CWPP — What Does It All Mean?” <https://www.gartner.com/en/documents/3956463> (accessed Feb. 25, 2021).
- [3] “Gartner Magic Quadrant for Cloud Infrastructure and Platform Services.” <https://www.gartner.com/en/documents/3989743/magic-quadrant-for-cloud-infrastructure-and-platform-ser> (accessed Feb. 25, 2021).
- [4] INTECO-CERT/INCIBE, “RIESGOS Y AMENAZAS EN CLOUD COMPUTING,” 2011. Accessed: Apr. 07, 2021. [Online]. Available: www.inteco.es.
- [5] “Active Working Groups | Cloud Security Alliance.” <https://cloudsecurityalliance.org/research/working-groups/> (accessed Apr. 07, 2021).
- [6] “Top Threats to Cloud Computing: Egregious | Cloud Security Alliance.” <https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/> (accessed Apr. 07, 2021).
- [7] “Is the Cloud Secure? - Smarter With Gartner.” <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/> (accessed Apr. 07, 2021).
- [8] “Cumplimiento normativo en la empresa (Compliance),” Accessed: Apr. 07, 2021. [Online]. Available: <https://www.iberley.es/temas/cumplimiento-normativo-empresa-compliance-62705>.
- [9] “What is Cloud Compliance? | AWS & Azure Firewall Compliance | AlgoSec.” <https://www.algosec.com/cloud-compliance/> (accessed May 08, 2021).
- [10] B. A. R. Bartley, “Solution Path for Security in the Public Cloud.”
- [11] D. X. Patrick Hevesi, Richard Bartley, “Guide to Cloud Security Concepts.”
- [12] “New eBook: Which CASB Deployment Architecture is Right for Me? | McAfee Blogs.” <https://www.mcafee.com/blogs/enterprise/cloud-security/new-ebook-which-casb-deployment-architecture-is-right-for-me/> (accessed Apr. 14, 2021).
- [13] “CIS Benchmarks.” <https://www.cisecurity.org/cis-benchmarks/> (accessed Apr. 15, 2021).
- [14] N. MacDonald, “Innovation Insight for Cloud Security Posture Management.”
- [15] RevistaSIC, “Las compras de empresas de protección en la nube y para el trabajo en remoto, protagonistas del mercado en tiempos de Covid,” 2020.

- [16] “AWS Security Hub | Amazon Web Services (AWS).”
<https://aws.amazon.com/es/security-hub/> (accessed Apr. 21, 2021).
- [17] “Partners | AWS Security Hub | Amazon Web Services (AWS).”
<https://aws.amazon.com/es/security-hub/partners/> (accessed May 09, 2021).
- [18] “Centro de seguridad de Azure | Microsoft Azure.” <https://azure.microsoft.com/es-es/services/security-center/> (accessed Apr. 21, 2021).
- [19] “Security Command Center | Security Command Center | Google Cloud.”
<https://cloud.google.com/security-command-center> (accessed Apr. 21, 2021).
- [20] “Aqua Cloud Native Security, Container Security & Serverless Security.”
<https://www.aquasec.com/> (accessed May 09, 2021).
- [21] “Azure/Azure-Security-Center: Welcome to the Azure Security Center community repository.” <https://github.com/Azure/Azure-Security-Center> (accessed May 10, 2021).
- [22] “GitHub - aquasecurity/cloudsploit: Cloud Security Posture Management (CSPM).”
<https://github.com/aquasecurity/cloudsploit> (accessed May 11, 2021).