Auditoría de seguridad y cumplimiento en entornos Cloud

Mapeo de Soluciones de Seguridad CASB, CSPM, y CWPP en la CCM - Multicloud.

Brenda Alejandra López Ávila

Master en ciberseguridad y privacidad

Tutor de TF:
Pau del Canto Rodrigo
Profesor responsable de la asignatura:
Víctor García Font

Fecha Entrega:
18 de junio 2024

Universitat Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Auditoria de Seguridad y Cumplimiento en entornos Cloud* *Mapeo de Soluciones de Seguridad CASB, CSPM, y CWPP en la CCM -Multicloud.*
Nombre del autor:	*Brenda Alejandra López Ávila*
Nombre del consultor/a:	*Pau del Canto Rodrigo*
Nombre del PRA:	*Victor Garcia Font*
Fecha de entrega (mm/aaaa):	2024
Titulación o programa:	*Máster universitario de Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Seguridad Empresarial*
Idioma del trabajo:	*Español*
Palabras clave	*CASB, CSPM, CWPP, IaaS, Multi-cloud, Nube , PaaS, SaaS, Seguridad.*

Resumen del Trabajo

Este trabajo aborda la seguridad en entornos de nube múltiple, enfrentando los desafíos emergentes en la adopción de nubes públicas en un entorno tecnológico en constante evolución. El objetivo principal es desarrollar un conjunto de directrices de auditoría de seguridad y cumplimiento, basado en la Cloud Control Matrix, que asigna herramientas de los grupos CASB, CSPM y CWPP a cada uno de sus controles para mejorar la seguridad, el cumplimiento normativo y la confianza en la adopción de soluciones en la nube.

La metodología empleada incluye una revisión exhaustiva de la literatura sobre seguridad en la nube, la formulación de un marco teórico robusto y la identificación de riesgos comunes. Se realiza un análisis detallado de herramientas especializadas como CASB, CSPM y CWPP para profundizar la evaluación técnica, asegurando que las herramientas se alineen con los modelos de servicios en la nube (IaaS, PaaS, SaaS) y demostrando la flexibilidad necesaria para adaptarse a diversas arquitecturas cloud.

Los resultados esperados son la elaboración de un checklist teórico que incorpore estas herramientas especializadas, facilitando la identificación y mitigación de riesgos. Además, el proyecto aspira a mejorar la eficacia operativa de las organizaciones que adoptan servicios en la nube. En conclusión, este estudio no solo profundiza en la evaluación de la seguridad en la nube, sino que también extiende su visión hacia los beneficios económicos y de sostenibilidad, ofreciendo una guía práctica para asegurar eficazmente los entornos de nube múltiple en el dinámico contexto tecnológico actual.

Abstract

This work addresses security in multi-cloud environments, tackling the emerging challenges in the adoption of public clouds in a constantly evolving technological environment. The main objective is to develop a set of security audit and compliance guidelines, based on the Cloud Control Matrix, that assigns tools from the CASB, CSPM, and CWPP groups to each of its controls to enhance security, regulatory compliance, and trust in cloud solution adoption.

The methodology employed includes a comprehensive review of literature on cloud security,

the formulation of a robust theoretical framework, and the identification of common risks. A detailed analysis of specialized tools such as CASB, CSPM, and CWPP is conducted to deepen the technical evaluation, ensuring that the tools align with cloud service models (IaaS, PaaS, SaaS) and demonstrating the flexibility needed to adapt to various cloud architectures.

The expected results are the creation of a theoretical checklist that incorporates these specialized tools, facilitating the identification and mitigation of risks. Additionally, the project aims to improve the operational effectiveness of organizations adopting cloud services. In conclusion, this study not only delves into the evaluation of cloud security but also extends its vision towards economic and sustainability benefits, offering a practical guide to effectively securing multi-cloud environments in today's dynamic technological context.

Tabla de contenido

Lista de figuras

1. Introducción: Plan de trabajo

1.1. Contexto y justificación del Trabajo

La computación en la nube, con sus propiedades como la alta disponibilidad, elasticidad y agilidad, ha llevado a un aumento significativo en la adopción por parte de las organizaciones para mejorar la eficiencia operativa y reducir costos. Este cambio hacia la nube no solo ha transformado la forma en que las empresas gestionan sus cargas computacionales, sino que también ha impulsado la sostenibilidad al reducir la necesidad de infraestructuras físicas y minimizar el desperdicio de recursos.

En el dinámico escenario tecnológico actual, marcado por el constante avance en la adopción de nubes públicas, observamos un notorio incremento en los riesgos inherentes. A pesar de la existencia de diversos marcos y regulaciones de seguridad que abordan aspectos específicos de cumplimiento en entornos de nube, la rápida evolución de las amenazas exige una estrategia más precisa y actualizada. En este contexto, surge la necesidad de desarrollar un enfoque integral que permita evaluar la seguridad en la nube de manera multinube, considerando los riesgos comunes.

La adopción de nubes públicas, además de mitigar riesgos, conlleva ventajas notables, como la optimización de recursos, la eficiencia operativa y la capacidad de adaptación a las demandas cambiantes del mercado. Estos aspectos, a menudo pasados por alto, constituyen pilares fundamentales en el desarrollo sostenible y económico de las organizaciones.

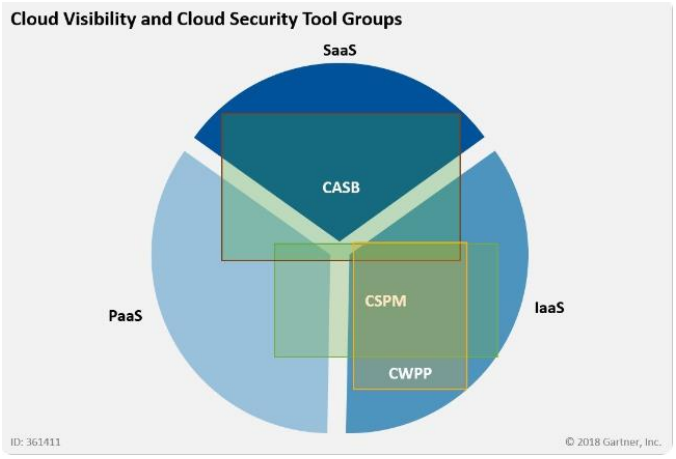

Figura 1. Herramientas de seguridad en la nube.

En el ámbito técnico, el proyecto se adentrará en el análisis de herramientas especializadas, como se muestra en la Figura 1. Como lo son CASB (Cloud Access Security Brokers), CSPM (Cloud Security Posture Management) y CWPP (Cloud Workload Protection Platforms), buscando enriquecer la evaluación de seguridad desde una perspectiva técnica avanzada. Esta inclusión estratégica no solo contribuirá a la identificación y mitigación de riesgos, sino que también potenciará la eficacia operativa de las empresas. Al profundizar en estas herramientas, se establecerá un puente crucial entre la

seguridad multinube y la sostenibilidad, consolidando así un marco integral que respalde el desarrollo continuo y positivo de las organizaciones.

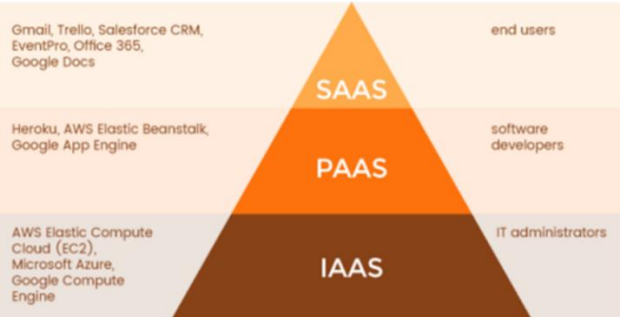

Figura 2. Modelos de servicios cloud.

Al considerar el impacto de estas herramientas, se revela una conexión directa con el modelo de nube utilizado (IaaS/PaaS/SaaS) como se muestra en la Figura 2. Este detalle técnico no solo refleja la diversidad de enfoques en la nube, sino que también subraya la importancia de adaptar las soluciones de seguridad a las particularidades de cada proveedor. Esta adaptabilidad se traduce en una mayor efectividad y, por ende, en un desarrollo empresarial más sólido y sostenible.

Es por esto que al abordar la seguridad desde un enfoque integral y técnico, se contribuye no solo a la comprensión profunda de los desafíos, sino también a proporcionar una guía práctica y avanzada para asegurar entornos multinube de manera efectiva y eficiente. Este enfoque integrado propone no solo proteger, sino también potenciar el desarrollo continuo y sostenible de las empresas en el vertiginoso y desafiante mundo tecnológico actual.

1.2. Objetivos del Trabajo

Objetivo General: Desarrollar un conjunto de directrices de auditoría de seguridad y cumplimiento para entornos cloud, basada en la Cloud Control Matrix, que permita asignar herramientas de los grupos CASB, CSPM, y CWPP a cada uno de sus controles. Esta metodología debe aplicarse de manera efectiva en las plataformas de servicios en la nube más populares como AWS, Azure, y GCP, con el fin de mejorar la seguridad, el cumplimiento normativo, y la confianza en la adopción de soluciones cloud.

Objetivos específicos:

- Realizar un análisis detallado de los riesgos de seguridad asociados con entornos cloud públicos, proporcionando una visión general que sirva como base para el desarrollo del checklist.
- Investigar y comprender los grupos de herramientas CASB (Cloud Access Security Broker), CSPM (Cloud Security Posture Management) y CWPP (Cloud Workload Protection Platform), analizando sus funciones y capacidades específicas en términos de seguridad y cumplimiento en entornos cloud.
- Desarrollar una metodología de asignación que permita vincular cada

control de la Cloud Control Matrix con una o dos herramientas del grupo CASB, CSPM y CWPP, asegurando su adecuación para las plataformas de servicios en la nube mencionadas.

- Informar el desarrollo de las directrices de auditoría de seguridad y cumplimiento, asegurando que aborden los requisitos de seguridad y cumplimiento en los modelos de servicios en la nube, y proporcionen recomendaciones específicas para cada plataforma principal (AWS, Azure, GCP).

1.3. Impacto en sostenibilidad, ético-social y de diversidad

La ejecución del proyecto de fin de máster tendrá un impacto significativo en las dimensiones de "Compromiso ético y global" de la UOC, con especial énfasis en la ciberseguridad, privacidad y la seguridad de la información. Al adoptar enfoques avanzados, se fortalecerán los controles de seguridad, contribuyendo a un cumplimiento normativo más efectivo. La implementación de medidas especializadas también asegurará la confidencialidad, integridad y disponibilidad de la información almacenada en nubes públicas, reforzando así la postura defensiva frente a amenazas cibernéticas.

Desde la perspectiva ética y social, el proyecto se compromete a salvaguardar la privacidad de los datos, fomentando la confianza de los usuarios finales en el entorno digital. Además, al abordar las particularidades de cada proveedor de nube, se promoverá la inclusión y diversidad en la adopción tecnológica, alineándose con principios éticos fundamentales. En conjunto, estos esfuerzos contribuirán a la construcción de entornos cibernéticos más seguros, éticos y alineados con los estándares normativos vigentes.

1.4. Enfoque y método seguido

A continuación, se presenta la metodología para la creación del checklist teórico respaldado por herramientas especializadas en ciberseguridad. La estrategia elegida se enfoca en evaluar la seguridad en nubes públicas desde una perspectiva multinube, priorizando la protección de la información y el cumplimiento normativo.

- Fase 1: En la primera fase, se llevará a cabo un análisis exhaustivo para identificar los riesgos de seguridad de la información en entornos cloud, centrándose en la Cloud Control Matrix (CCM). Se explorarán y evaluarán frameworks destacados como ISO/IEC 27001, Cloud Security Alliance (CSA), Google Cloud Security, Cloud Adoption Framework (CAF) de Microsoft Azure y IBM Security Framework para determinar su relevancia y capacidad para abordar los desafíos identificados. Además, se investigarán los mecanismos de mitigación existentes para respaldar la formulación teórica de soluciones, sin la necesidad de generar un checklist inicial.

- Fase 2: Una vez completada la fase de investigación, se procederá a adoptar un enfoque centrado en las herramientas de seguridad cloud,

como CASB (Cloud Access Security Broker), CSPM (Cloud Security Posture Management) y CWPP (Cloud Workload Protection Platform), en función de los controles de la CCM. Se buscarán activamente herramientas técnicas que respalden la mitigación de los riesgos identificados, priorizando la compatibilidad multinube y la eficacia en diversos entornos de nube. Se asignarán específicamente una o dos herramientas del grupo CASB, CSPM y CWPP a cada control de la CCM, asegurando que las soluciones seleccionadas sean efectivas y eficientes para mejorar la seguridad y el cumplimiento en los entornos cloud.

- Conclusiones y Futuras Líneas de Trabajo: En la fase final del proyecto, se presentarán las conclusiones extraídas de las pruebas y estudios realizados, destacando los hallazgos clave y los éxitos obtenidos en la asignación de herramientas a los controles de la CCM. Se identificarán los desafíos enfrentados durante el proceso y se propondrán posibles mejoras continuas y adaptaciones en función de la evolución del panorama de seguridad en la nube. Asimismo, se plantearán recomendaciones para futuras líneas de trabajo, considerando la necesidad de mantener la seguridad y el cumplimiento normativo en entornos cloud en constante cambio.

1.5. Planificación del Trabajo

A continuación, se describen los recursos necesarios para realizar el proyecto y las tareas a realizar.

1.5.1. Recursos necesarios

Los recursos necesarios para llevar a cabo las fases descritas en el punto anterior son los siguientes:

- Un computador personal con conexión a Internet equipado con un software de procesador de textos para elaborar el documento final del proyecto.
- Un navegador web para acceder a la información y bibliografía necesaria durante todas las etapas del proyecto.

1.5.2. Cronograma

TFM : Enfoque Integral para la Seguridad y Eficiencia en Nubes Públicas

Cronograma de Actividades
Brenda Alejandra López Ávila

Actividad	Inicio	Duración	Fin
Planificación	28/02/2024	13	12/03/2024
Definir el contexto y los objetivos.	28/02/2024	4	3/03/2024
Evaluar el impacto ético-social.	3/03/2024	2	5/03/2024
Elaborar la planificación del proyecto.	5/03/2024	2	7/03/2024
Establecer plazos y fechas clave.	7/03/2024	2	9/03/2024
Iniciar la redacción de la PEC1.	9/03/2024	3	12/03/2024
Entrega de seguimiento 1	12/03/2024	30	9/04/2024
Revisar la literatura sobre seguridad en la nube.	12/03/2024	9	21/03/2024
Desarrollar el marco teórico a tener en cuenta.	21/03/2024	2	23/03/2024
Identificar y documentar riesgos comunes.	14/03/2024	16	30/03/2024
Investigar normativas de seguridad.	30/03/2024	7	6/04/2024
Entender todos los puntos de la CMM y entrega PEC 2	6/04/2024	5	8/04/2024
Entrega de seguimiento 2	9/04/2024	28	7/05/2024
Analizar CASB, CSPM y CWPP.	9/04/2024	5	14/04/2024
Evaluar su aplicabilidad al check list.	14/04/2024	10	24/04/2024
Integrar herramientas seleccionadas.	20/04/2024	15	5/05/2024
Realizar ajustes pertinentes PEC 3	5/05/2024	2	7/05/2024
Presentación	7/05/2024	52	28/06/2024
Sintetizar hallazgos y resultados.	7/05/2024	9	16/05/2024
Evaluar eficacia de herramientas y check list.	16/05/2024	6	22/05/2024
Identificar áreas de mejora.	22/05/2024	4	26/05/2024
Redactar conclusiones finales y PEC 4.	26/05/2024	16	11/06/2024
Elaboración y ejecución de la presentación	11/06/2024	7	18/06/2024
Defensa	18/06/2024	10	28/06/2024

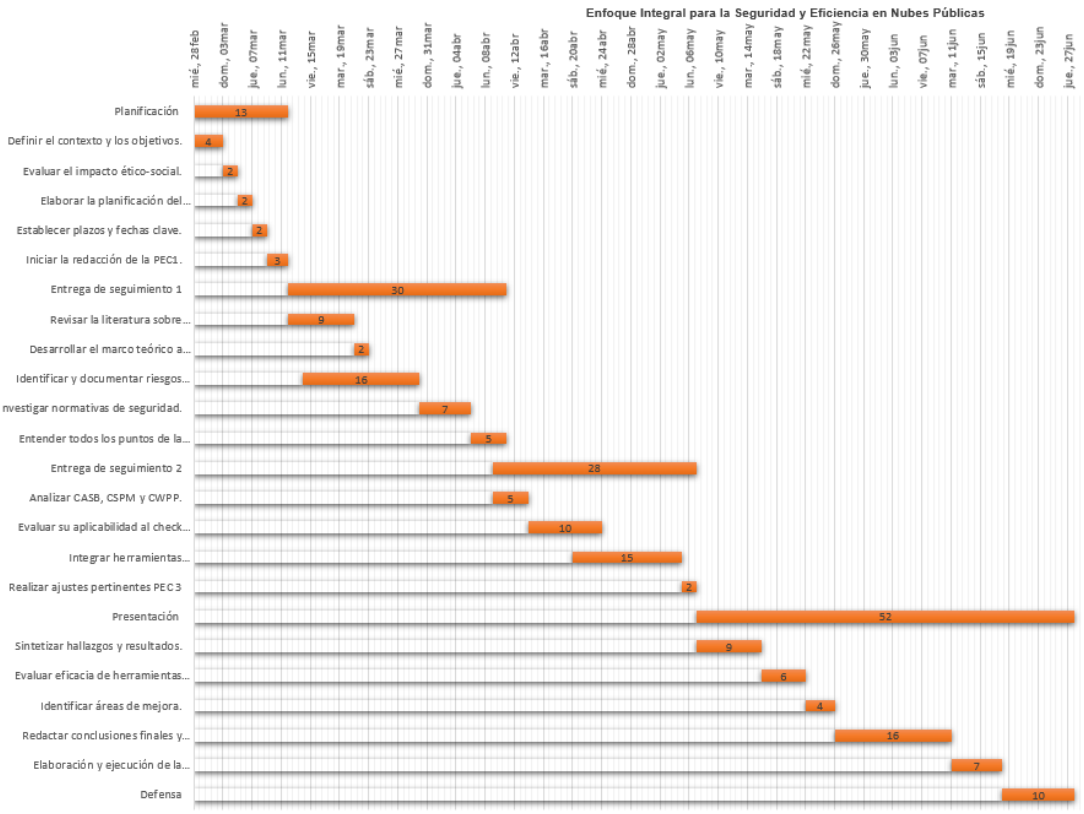

Figura 3. Cronograma de actividades.

1.6. Breve descripción de los otros capítulos de la memoria

Esta memoria se dividirá en cuatro entregables correspondientes a las PECs y un espacio final de presentación y defensa como se describe a continuación:

PEC1. Plan de trabajo: En este documento se presenta la explicación del problema abordado en el trabajo, el análisis del estado actual de la tecnología cloud, el establecimiento de los objetivos del proyecto, la descripción detallada de la metodología empleada, la especificación de los recursos necesarios y la definición de una planificación con tareas a llevar a cabo.

PEC2. Entrega de seguimiento 1: Aquí se presenta un informe que detalla las tareas realizadas hasta el momento, ajustando la planificación según sea necesario. Además, se presenta un resumen conciso del estudio teórico, destacando los diversos riesgos

PEC3. Entrega de seguimiento 2: Similar al entregable anterior, este documento reflejará los avances realizados y ajustará la planificación según sea necesario. En esta fase, se presenta el entregable de auditoría detallando la selección de proveedores de cloud públicos y herramientas que han sido investigadas, proporcionando información detallada sobre sus características, ventajas y desventajas.

PEC4. Memoria final: En este documento se presenta la síntesis del trabajo realizado durante el proyecto, mostrando las conclusiones obtenidas. También

se incluirá información adicional, como anexos y bibliografía.

Presentación: La síntesis del trabajo se presenta en un video, utilizando diapositivas como soporte visual.

Defensa: Como fase final del TFM, se presenta la defensa del trabajo ante una comisión de evaluación. Esta defensa se realiza de manera síncrona mediante una herramienta de videoconferencia e incluye una presentación resumida del trabajo y la respuesta a preguntas formuladas por la comisión.

2. Seguridad en la nube

2.1 Computación en la nube

Este modelo de computación se basa en la virtualización de recursos, lo que permite una mayor flexibilidad, escalabilidad y eficiencia en el uso de los recursos informáticos. En lugar de invertir en infraestructura costosa y mantenerla localmente, las organizaciones pueden aprovechar los servicios en la nube ofrecidos por proveedores como Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), entre otros. [1]

La computación en la nube ha revolucionado la forma en que las organizaciones gestionan sus recursos informáticos, permitiendo una mayor agilidad, innovación y reducción de costos.

2.1.2 Modelos de despliegue

Los escenarios de servicios en la nube se han clasificado en infraestructuras públicas, privadas, comunitarias o híbridas; así:

Nube pública: La infraestructura de esta nube está disponible para el público en general o para un gran grupo de industria y dicha infraestructura la controla un proveedor de servicios en la nube.
Nube privada: La infraestructura de esta nube es operada únicamente por y para una organización.
Nube comunitaria: La infraestructura de esta nube es compartida por varias organizaciones relacionadas entre ellas y que comparten requisitos de servicio. Uno de sus miembros controla los recursos.
Nube híbrida: Es la composición de dos o más modelos, por ejemplo, privada y pública, que permanecen como entidades únicas pero que coexisten por tener tecnología que permite compartir datos o aplicaciones entre las mismas.

2.1.3 Modelos de servicio

Infraestructura como Servicio (IaaS): En este modelo, los proveedores de la nube ofrecen recursos informáticos fundamentales, como servidores virtuales, almacenamiento y redes, a través de Internet. Los clientes pueden escalar y gestionar estos recursos según sus necesidades. [2]

Plataforma como Servicio (PaaS): PaaS proporciona a los desarrolladores una plataforma completa para desarrollar, ejecutar y gestionar aplicaciones sin la complejidad de construir y mantener la infraestructura subyacente. Los servicios incluyen bases de datos, herramientas de desarrollo y entornos de ejecución. [3]

Software como Servicio (SaaS): En este modelo, los usuarios acceden a aplicaciones alojadas en la nube a través de Internet. Los proveedores gestionan y mantienen la infraestructura, así como las actualizaciones del software. Los ejemplos comunes incluyen correos electrónicos basados en la web, aplicaciones de productividad y sistemas de gestión empresarial. [4]

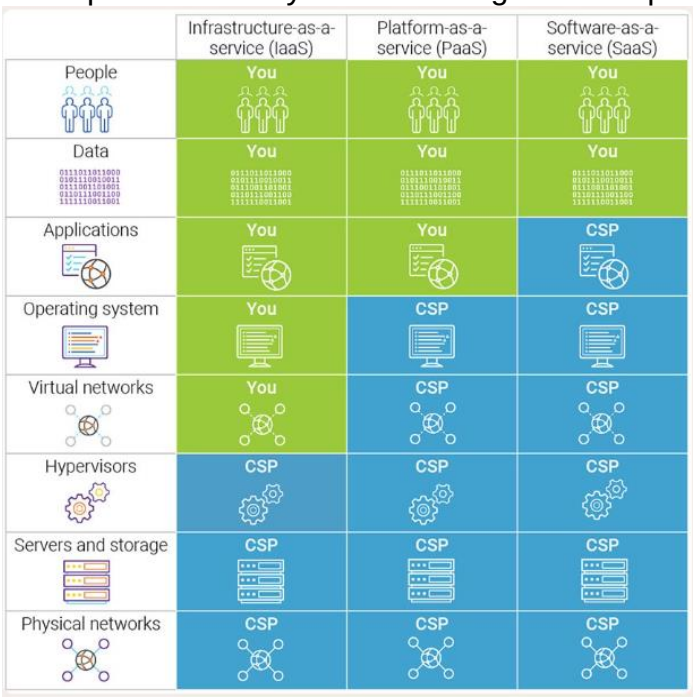

Figura 4. Modelo de seguridad compartida

La evolución de la computación en la nube, representada en la Figura 4 para los modelos IaaS, PaaS y SaaS, implica una creciente transferencia de responsabilidades hacia los proveedores, reduciendo la carga de seguridad para los clientes. No obstante, el progreso tecnológico y la adopción de la nube han introducido nuevos desafíos en materia de seguridad de la información. Como resultado, se ha vuelto imperativo implementar controles específicos para mitigar las amenazas emergentes y los riesgos inherentes a este entorno dinámico y en constante evolución.

En Colombia, tanto Colciencias como el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) juegan un papel clave al proporcionar orientación y recursos para promover prácticas seguras en el uso de tecnologías digitales, especialmente en el ámbito de la seguridad en la nube. Paralelamente, existen otras instituciones relevantes como el Cloud Security Alliance (CSA), la consultora Gartner, y el National Institute of Standards and Technology (NIST). [5]

De estas, la CSA se destaca por su enfoque en promover las mejores prácticas

para garantizar la seguridad en la nube, mediante la creación de la Cloud Controls Matrix (CCM), un marco de referencia para evaluar y mitigar los riesgos de seguridad asociados con la adopción de servicios en la nube [6]. Por su parte, el NIST es reconocido por su Marco de Ciberseguridad y sus publicaciones sobre seguridad de la información, mientras que la ISO ha desarrollado estándares importantes como ISO/IEC 27001 y 27002. [7]

Además, la IEC se enfoca en la ciberseguridad de los sistemas de control industrial, y la ISACA ha creado el marco COBIT para la gobernanza de TI. Estas organizaciones y marcos desempeñan un papel crucial al proporcionar orientación y estándares para el desarrollo de prácticas de seguridad efectivas en la nube, garantizando así la protección de la información y los recursos críticos.

Figura 5. Aspectos de seguridad en la nube **[8]**

A continuación, se analizarán los principales aspectos de seguridad en entornos cloud mostrados en la Figura 5, así como las estrategias para gestionar y mitigar estos riesgos

- Autenticación: Garantiza que solo usuarios autorizados accedan a los recursos en la nube.
- Controles de Acceso: Restringen el acceso a datos y recursos sensibles.
- Aprobación Secundaria: Asegura que las acciones críticas requieran una verificación adicional.
- Analítica del Comportamiento del Usuario: Detecta patrones anómalos de usuario.
- Registro y Reporte: Permiten la detección temprana de actividades sospechosas y facilitan la respuesta a incidentes, mejorando la capacidad de supervisión y la resiliencia del sistema.
- Descubrimiento de Datos: Ayuda a identificar datos sensibles y su ubicación.
- Clasificación de Activos y Datos: Permite priorizar la protección según su importancia y riesgo, garantizando una protección efectiva de los recursos críticos.
- Encriptación: Protege la confidencialidad de los datos, asegurando que

solo los destinatarios autorizados puedan acceder a la información.
- Gestión de Claves: Asegura la seguridad de los datos encriptados.
- Endurecimiento de Configuración: Reduce la superficie de ataque al minimizar vulnerabilidades y asegurar una configuración segura de los recursos en la nube. [9]
- Segmentación Lógica: Limita el acceso a recursos y datos específicos. [9]
- Cumplimiento de Límites: Establece fronteras claras entre los sistemas, protegiendo contra accesos no autorizados y garantizando la separación adecuada de recursos. [9]

El informe Pandemic 11 [10] de la Cloud Security Alliance (CSA) presenta las principales amenazas a la computación en la nube, destacando que los problemas tradicionales de seguridad en la nube están disminuyendo en preocupación. Este informe clasifica las preocupaciones en orden de importancia, proporcionando recomendaciones de control y ejemplos de referencia del mundo real para ayudar al personal de cumplimiento, riesgos y tecnología. Este reporte proporciona una visión actualizada de las amenazas emergentes y cambiantes en el entorno de la computación en la nube, enfatizando la necesidad de adoptar nuevas estrategias y controles de seguridad. [11]

1. Gestión insuficiente de identidades, credenciales, accesos y claves (n.º 4)
2. Interfaces y API inseguras (n.º 7)
3. Mala configuración y control de cambios inadecuado (n.º 2)
4. Falta de arquitectura y estrategia de seguridad en la nube (n.º 3)
5. Desarrollo de software inseguro
6. Recursos de terceros no seguros
7. Vulnerabilidades del sistema
8. Divulgación/divulgación accidental de datos en la nube
9. Configuración incorrecta y explotación de cargas de trabajo sin servidor y de contenedores
10. Crimen organizado/hackers/APT
11. Exfiltración de datos de almacenamiento en la nube

Así como otras referencias mencionan otras posibles preocupaciones en la nube como lo son [12]:

- Cuestiones de cumplimiento: Es posible que los servicios en la nube no siempre cumplan con los requisitos normativos y de cumplimiento para el almacenamiento y la seguridad de datos.
- Riesgos de multiinquilino: los servicios de nube pública suelen ser multiinquilino, lo que significa que varios usuarios comparten la misma infraestructura física. Esto puede aumentar el riesgo de fuga de datos o acceso no autorizado si no se gestionan adecuadamente.
- Vulnerabilidades en herramientas de terceros: los servicios de nube pública a menudo dependen de herramientas y proveedores de terceros, lo que puede crear vulnerabilidades si estos proveedores no son examinados adecuadamente o cuentan con medidas de seguridad

débiles.

- Falta de control: Los servicios de nube pública son gestionados por el proveedor de la nube, lo que significa que los usuarios tienen un control limitado sobre las medidas de seguridad que se implementan.
- Ataques DDoS : Nube públicalos servicios pueden servulnerable a ataques distribuidos de denegación de servicio (DDoS), que pueden alterar la disponibilidad del servicio.
- Filtraciones de datos a través de API: los servicios de nube pública a menudo utilizan API para permitir la integración con otros sistemas, lo que puede crear vulnerabilidades si estas API no están protegidas adecuadamente.
- Exposición de datos a través de servicios mal configurados: los servicios de nube pública pueden ser vulnerables a la exposición de datos si los servicios están mal configurados o los controles de acceso no se han configurado correctamente.

En este contexto, es fundamental reconocer que los frameworks de seguridad en la nube, como la Cloud Controls Matrix (CCM) desarrollada por el Cloud Security Alliance (CSA), desempeñan un papel crucial en la evaluación y mitigación de riesgos. La CCM proporciona un marco detallado para evaluar los controles de seguridad ofrecidos por los proveedores de servicios en la nube, abordando aspectos como la gestión de accesos, la criptografía, la gestión de incidentes y la continuidad del negocio. Además, el National Institute of Standards and Technology (NIST) ofrece su Marco de Ciberseguridad, que brinda pautas exhaustivas para la seguridad de la información en la nube, incluyendo la identificación de riesgos, la protección de datos y la respuesta a incidentes.

En el ámbito de la nube, se encuentran diversas formas de auditoría. Los proveedores de servicios en la nube pueden certificar sus controles operativos mediante estándares como SOC 2, ISO o NIST. Además, las empresas pueden optar por cumplir con estándares específicos de la industria, como PCI. En este contexto, nos enfocaremos en la auditoría de entornos de clientes en la nube desde una perspectiva informática de TI.

Tanto para auditores internos como externos, comprender cómo aplicar controles de TI en entornos de nube es crucial. Por ejemplo, los controles de PCI DSS que requieren un inventario detallado de activos empresariales pueden necesitar ajustes para adaptarse a la naturaleza dinámica de la nube. Además, se deben considerar procesos relacionados con la facturación, gestión financiera, asignación de recursos y administración de usuarios. La capacidad de evaluar los riesgos asociados con el uso de servicios en la nube se vuelve esencial para los auditores en la actualidad.

La clasificación por niveles en proveedores de servicios en la nube, conocida como Tier, ofrece una guía para entender las diferencias entre ellos y sus capacidades. En el nivel Tier 1, encontramos proveedores globales altamente escalables que ofrecen una amplia gama de servicios de nube, incluyendo Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS). Estos proveedores tienen un amplio catálogo

de servicios para todas las verticales de negocio y su público objetivo es global, con una vasta experiencia en el sector tecnológico. En el nivel Tier 2, se encuentran proveedores que también ofrecen múltiples modelos de nube, pero tienden a enfocarse en uno de ellos. Aunque pueden estar limitados geográficamente o en ciertas verticales de negocio, ofrecen características de valor añadido como un amplio soporte. Por último, en el nivel Tier 3, se ubican proveedores más pequeños que suelen ofrecer principalmente SaaS, a menudo desplegados sobre proveedores Tier 1. Esta categoría puede presentar una mayor tasa de fallos debido a que cualquier persona con conocimientos básicos de programación puede ofrecer soluciones SaaS básicas [13]

2.2 Herramientas de seguridad

En el contexto de la auditoría de seguridad y cumplimiento en entornos cloud, es crucial comprender las diferencias entre las herramientas nativas y de terceros en nubes públicas. Las herramientas nativas son aquellas integradas directamente en la plataforma de la nube, proporcionadas por el proveedor de servicios. Estas herramientas suelen ofrecer funcionalidades básicas de seguridad y cumplimiento, como la gestión de identidad y acceso, la encriptación de datos y la supervisión de la infraestructura. Por ejemplo, servicios como Amazon GuardDuty y Azure Advanced Threat Protection son herramientas nativas que monitorean eventos y protegen los datos en entornos cloud públicos. [14]

Por otro lado, las herramientas de terceros son desarrolladas por proveedores externos y pueden ofrecer funcionalidades más avanzadas y especializadas. Estas herramientas complementan las capacidades nativas de la nube y pueden abordar necesidades específicas de seguridad y cumplimiento. Por ejemplo, soluciones como Prisma Cloud ofrecen una gestión integral de la seguridad en la nube, que incluye la detección de amenazas, la protección de datos y el cumplimiento de normativas, proporcionando una capa adicional de seguridad en entornos cloud públicos [5]. Es fundamental evaluar las necesidades y requisitos de seguridad de cada organización para determinar si es necesario complementar las herramientas nativas con soluciones de terceros en entornos cloud públicos.

En el contexto de la creciente adopción de servicios en la nube por parte de las organizaciones, la seguridad de los datos y los activos digitales se ha convertido en una prioridad fundamental. Por esta razón, en este proyecto de grado se abordarán tres categorías de herramientas clave de seguridad en la nube: Cloud Access Security Broker (CASB), Cloud Security Posture Management (CSPM) y Cloud Management and Monitoring (CMM). Estas herramientas desempeñan roles críticos en la protección y gestión de entornos cloud, abordando aspectos esenciales como la autenticación, el control de acceso, la evaluación de riesgos y el monitoreo del rendimiento. A lo largo de este estudio, se explorarán en profundidad las funciones, características y ejemplos de implementación de cada una de estas herramientas. Además, se examinará cómo pueden integrarse de manera efectiva para fortalecer la postura de seguridad en la nube de las organizaciones.

2.2.1 CASB (Cloud Access Security Broker)

CASB, o Cloud Access Security Broker, es un punto de cumplimiento de directiva de seguridad que se posiciona entre los usuarios de la empresa y los proveedores de servicio en la nube. Los CASB pueden combinar varias directivas de seguridad diferentes, desde la autenticación y asignación de credenciales al cifrado, detección de malware y mucho más, lo que ofrece soluciones empresariales flexibles que ayudan a garantizar la seguridad de aplicaciones en la nube, tanto en aplicaciones autorizadas como no autorizadas y en dispositivos administrados y no administrados. [15]

Ventajas:
Mejora la seguridad y el cumplimiento en la nube.
Facilita la adopción segura de servicios cloud.

Desventajas:
Puede introducir latencia y complejidad.
Requiere una configuración y gestión adecuadas.

Aplicabilidad: SaaS, PaaS, IaaS.

Ejemplos de CASB: Netskope, McAfee MVISION Cloud, Microsoft Cloud App Security.

2.2.2 CSPM (Cloud Security Posture Management)

CSPM, o Cloud Security Posture Management, se enfoca en garantizar que las configuraciones y políticas de seguridad en la nube cumplan con las mejores prácticas y estándares de seguridad. Garantiza la configuración segura y conforme a las políticas de seguridad en la nube, mejorando la postura de seguridad

Ventajas:
Identifica y remedia configuraciones erróneas.
Mantiene el cumplimiento continuo con estándares de seguridad.

Desventajas:
Puede generar falsos positivos y requerir esfuerzo de implementación.
Complejidad en la configuración y gestión.

Aplicabilidad: IaaS.

Ejemplos de CSPM: Palo Alto Networks Prisma Cloud, AWS Security Hub, Check Point CloudGuard.

2.2.3 CWPP (Cloud Workload Protection Platform)

Es una solución de seguridad que protege las cargas de trabajo y aplicaciones en entornos cloud, ofreciendo protección en tiempo real contra amenazas.

Brinda visibilidad y protección avanzada para cargas de trabajo, incluyendo detección y respuesta a amenazas, control de acceso y segmentación de red.

Ventajas:
Protección específica para cargas de trabajo en entornos cloud.
Reducción del riesgo de ataques y violaciones de seguridad.

Desventajas:
Puede requerir integración y ser complejo de implementar.
Costo adicional y gestión compleja.

Aplicabilidad: IaaS, PaaS.

Ejemplos de CWPP: CrowdStrike Falcon, Trend Micro Cloud One - Workload Security, Palo Alto Networks Prisma Cloud Compute.

Tabla 1. Cuadro comparativo entre las principales características del conjunto de herramientas CSPM. CWPP y CASB

Aspecto	CSPM (Gestión de la Postura de Seguridad en la Nube)	CWPP (Plataforma de Protección de Cargas de Trabajo en la Nube)	CASB (Gestión de Seguridad en la Nube y Brokers de Acceso en la Nube)
Enfoque Principal	Identificar y corregir configuraciones incorrectas y vulnerabilidades en la nube.	Proteger las cargas de trabajo y aplicaciones en la nube.	Gestionar el acceso, uso y seguridad de aplicaciones y datos en la nube.
Alcance	- Identificación de configuraciones inseguras y cumplimiento de políticas.	- Detección y respuesta a amenazas en cargas de trabajo.	- Control de acceso y políticas para aplicaciones en la nube.
Alcance	- Evaluación de la postura de seguridad de la infraestructura en la nube.	- Protección contra malware, intrusiones y actividades maliciosas.	- Monitoreo y gestión de actividades y datos en la nube.
Funcionalidades	- Evaluación continua de la configuración y cumplimiento de políticas de seguridad en la nube.	- Protección contra amenazas de seguridad, incluyendo malware y vulnerabilidades.	- Implementación y aplicación de políticas de seguridad para aplicaciones y datos.
Funcionalidades	- Identificación y corrección de configuraciones incorrectas y vulnerabilidades.	- Detección de comportamiento anómalo y respuesta automatizada a incidentes.	- Análisis de riesgos, auditorías de seguridad y cumplimiento de políticas.
Funcionalidades	- Monitoreo y alertas sobre eventos de seguridad y cambios en la infraestructura.	- Gestión de acceso y control de seguridad para cargas de trabajo en la nube.	- Encriptación de datos, prevención de fuga de información y control de acceso.

Xz v

3. Resultados

En la presente sección del proyecto, se abordará un análisis detallado de los controles de auditoría especificados en la Cloud Control Matrix de la Cloud Security Alliance. Este marco es fundamental para garantizar la seguridad y el cumplimiento de los entornos cloud en empresas que utilizan servicios de

AWS, Azure y GCP.

A partir de la pasada revisión y análisis que incluía información general sobre las herramientas, sus funciones y características principales, ventajas, desventajas y aplicabilidad en distintos contextos de nube. Además, del cuadro comparativo que facilita la visualización de las diferencias y similitudes entre las herramientas evaluadas y la revisión meticulosa de los sitios oficiales y otros recursos autorizados, este estudio se centrará en la identificación y evaluación de herramientas específicas dentro de las categorías de Cloud Access Security Broker (CASB), Cloud Security Posture Management (CSPM), y Cloud Workload Protection Platform (CWPP).

Estas herramientas son esenciales para la implementación y gestión de los controles de seguridad en la nube y ofrecen diversas funcionalidades que permiten a las organizaciones mantener un alto nivel de seguridad y cumplir con las normativas vigentes.

Cada uno de los controles de la matriz será examinado con el objetivo de asignar al menos una o dos herramientas pertinentes que correspondan a las descripciones de los controles y que sean aplicables en AWS, Azure y GCP. Este enfoque no solo facilita una comprensión clara de cómo cada herramienta contribuye a la validación del cumplimiento de los controles durante las auditorías, sino que también proporciona una guía práctica sobre cómo los auditores pueden utilizar estas herramientas para evaluar el cumplimiento de una empresa.

Las referencias y fuentes de información primarias para este análisis serán los sitios web oficiales de los proveedores de servicios en la nube y las plataformas de las herramientas mencionadas, asegurando la veracidad y actualidad de la información presentada.

Este enfoque integral permitirá a los usuarios y auditores identificar de manera efectiva y eficiente las herramientas adecuadas para cada control de la matriz, optimizando así las estrategias de seguridad y cumplimiento en sus respectivos entornos cloud.

Tabla 2. Trabajo de asignación de herramientas de cada grupo (CASB, CSMP y CWPP) a cada control de la Control Cloud Matrix

CLOUD CONTROLS MATRIX v4.0.10						
				Herramientas		
Control Domain	**Control Title**	**Control ID**	**Control Specification**	**CASB**	**CSMP**	**CWPP**
Audit & Assurance - A&A						
Auditoría y Aseguramiento	Política y Procedimientos de Auditoría y Aseguramiento	**A&A-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas, procedimientos y normas de auditoría y aseguramiento. Revisión y actualización las políticas y procedimientos al menos una vez al año.	**Netskope Security Cloud:** Ofrece visibilidad en tiempo real y control de políticas para actividades en la nube, incluyendo auditorías y evaluaciones de conformidad. **McAfee MVISION Cloud:** Permite a las empresas auditar y monitorear todas las actividades en aplicaciones en la nube, gestionar el cumplimiento y proteger los datos.	**P alo Alto Networks Prisma Cloud:** Proporciona evaluación continua de la configuración y cumplimiento de las políticas de seguridad en la nube. **Check Point CloudGuard Posture Management:** Ayuda a automatizar la gobernanza y asegura el cumplimiento en ambientes de nube, incluyendo auditorías y evaluaciones de riesgo.	Las herramientas CWPP están enfocadas en proteger cargas de trabajo en la nube, mientras que las auditorías y aseguramientos requieren capacidades de revisión y gestión de conformidad que son características de las herramientas CASB y CSPM, no de los CWPP.
Auditoría y Aseguramiento	Evaluaciones independientes	**A&A-02**	Llevar a cabo auditorías independientes y evaluaciones de aseguramiento de acuerdo con normas pertinentes al menos una vez al año.			
Auditoría y Aseguramiento	Evaluación de la planificación basada en riesgos	**A&A-03**	Realizar auditorías independientes y evaluaciones de aseguramiento de acuerdo con planes y políticas basados en el riesgo.			
Auditoría y Aseguramiento	Cumplimiento de requisitos	**A&A-04**	Verificar el cumplimiento de todas las normas, reglamentos, legales/contractuales, y los requisitos legales aplicables a la auditoría.			
Auditoría y Aseguramiento	Proceso de Gestión de Auditorías	**A&A-05**	Definir e implementar un proceso de gestión de auditorías para respaldar la auditoría planificación, análisis de riesgos, evaluación del control de seguridad, conclusión, corrección cronogramas, generación de informes y revisión de informes anteriores y evidencia de respaldo.			
Auditoría y Aseguramiento	Remediación	**A&A-06**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener un plan de acción correctiva basado en el riesgo para remediar los hallazgos de la auditoría, revisar y Informar sobre el estado de la corrección a las partes interesadas pertinentes.			
Application & Interface Security - AIS						

Seguridad de aplicaciones e interfaces	Política y procedimientos de seguridad de aplicaciones e interfaces	**AIS-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la seguridad de las aplicaciones con el fin de proporcionar orientación a la Planificación, entrega y soporte adecuados de la aplicación de la organización capacidades de seguridad. Revisar y actualizar las políticas y procedimientos al menos anualmente.			
Seguridad de aplicaciones e interfaces	Requisitos de línea base de seguridad de aplicaciones	**AIS-02**	Establecer, documentar y mantener los requisitos básicos para la protección diferentes aplicaciones.	**Symantec CloudSOC CASB:** Ofrece protección para aplicaciones en la nube mediante políticas de seguridad, evaluación de riesgos y detección de anomalías. **Microsoft Cloud App Security:** Integra políticas de seguridad y realiza evaluaciones de conformidad en aplicaciones en la nube, ayudando en el diseño y la implementación segura.	**Veracode:** Proporciona pruebas automatizadas de seguridad en aplicaciones, incluyendo análisis estático, dinámico y de software compuesto para identificar vulnerabilidades antes de la implementación. **Checkmarx:** Es una plataforma que facilita el diseño y desarrollo de aplicaciones seguras, ofreciendo análisis estático y dinámico de código, así como pruebas de seguridad integradas en el proceso de desarrollo (DevSecOps).	Los CWPP están diseñados para la protección en tiempo de ejecución de cargas de trabajo en la nube, y no abordan aspectos del ciclo de desarrollo de aplicaciones como el diseño, las pruebas de seguridad automatizadas, y la gestión de vulnerabilidades, que son clave para la seguridad de aplicaciones e interfaces.
Seguridad de aplicaciones e interfaces	Métricas de seguridad de aplicaciones	**AIS-03**	Definir e implementar métricas técnicas y operativas alineadas con objetivos comerciales, requisitos de seguridad y obligaciones de cumplimiento.			
Seguridad de aplicaciones e interfaces	Diseño y desarrollo de aplicaciones seguras	**AIS-04**	Definir e implementar un proceso SDLC para el diseño de aplicaciones, desarrollo, despliegue y funcionamiento de conformidad con los requisitos de seguridad definidos por el la organización.			
Seguridad de aplicaciones e interfaces	Pruebas automatizadas de seguridad de aplicaciones	**AIS-05**	Implementar una estrategia de pruebas, que incluya criterios para la aceptación de nuevos sistemas de información, actualizaciones y nuevas versiones, lo que proporciona garantía de seguridad y mantiene el cumplimiento al tiempo que permite la velocidad de la organización de los objetivos de entrega. Automatice cuando corresponda y sea posible.			
Seguridad de aplicaciones e interfaces	Implementación automatizada de aplicaciones seguras	**AIS-06**	Establecer e implementar estrategias y capacidades para y la implementación de aplicaciones compatibles. Automatiza siempre que sea posible.			
Seguridad de aplicaciones e interfaces	Corrección de vulnerabilidades de aplicaciones	**AIS-07**	Definir e implementar un proceso para corregir la seguridad de las aplicaciones vulnerabilidades, automatizando la corrección cuando sea posible.			
Business Continuity Management and Operational Resilience - BCR						

Gestión de la Continuidad del Negocio y Resiliencia Operativa	Política y procedimientos de gestión de la continuidad del negocio	**BCR-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos de gestión de la continuidad del negocio y resiliencia operativa. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	Fusion Risk Management: Proporciona una plataforma completa para manejar políticas de continuidad del negocio. Avalution Catalyst: Ayuda en la documentación y actualización de políticas y procedimientos.	IBM Resilient: Soporta la gestión de políticas de continuidad en integración con la seguridad. Splunk Enterprise Security: Facilita la auditoría y actualización de políticas de continuidad.	No Aplica
Gestión de la Continuidad del Negocio y Resiliencia Operativa	Evaluación de Riesgos y Análisis de Impacto	**BCR-02**	Determinar el impacto de las interrupciones y los riesgos del negocio para establecer Criterios para el desarrollo de estrategias de continuidad del negocio y resiliencia operativa y capacidades.	Tenable.io: Identificación de vulnerabilidades y riesgos en la nube. Qualys Cloud Platform: Evaluación de riesgos y visibilidad en la nube.	RSA Archer Suite: Gestión de riesgos y análisis de impacto. MetricStream: Evaluación integral de riesgos y continuidad del negocio.	No Aplica
Gestión de la Continuidad del Negocio y Resiliencia Operativa	Estrategia de continuidad del negocio	**BCR-03**	Estrategias para reducir el impacto, resistir y recuperarse de las interrupciones del negocio dentro del apetito de riesgo.	Netskope Security Cloud: Gestiona la seguridad en aplicaciones de nube para mantener la continuidad. Microsoft Cloud App Security: Supervisa y controla el acceso a aplicaciones en la nube para asegurar la operatividad.	Palo Alto Networks Prisma Cloud: Evalúa y mejora la postura de seguridad para proteger contra interrupciones. Check Point CloudGuard Posture Management: Monitoriza configuraciones de seguridad y asegura la resiliencia en la nube.	No Aplica
Gestión de la Continuidad del Negocio y Resiliencia Operativa	Planificación de la continuidad del negocio	**BCR-04**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener un plan de continuidad de negocio basado en los resultados de la resiliencia operativa estrategias y capacidades	McAfee MVISION Cloud: Gestión de políticas de seguridad en la nube. Symantec CloudSOC: Control y seguridad de aplicaciones en la nube. CSPM:	AWS Config: Auditoría y configuración de recursos en AWS. Azure Security Center: Seguridad y gestión de riesgos en Azure.	No Aplica

Gestión de la Continuidad del Negocio y Resiliencia Operativa	Documentación	**BCR-05**	Desarrollar, identificar y adquirir documentación que sea relevante para Apoyar los programas de continuidad del negocio y resiliencia operativa. Haga que el documentación a disposición de las partes interesadas autorizadas y revisarla periódicamente.	Microsoft Cloud App Security: Facilita la documentación y control sobre las aplicaciones en la nube. Netskope Security Cloud: Proporciona visibilidad y control para gestionar documentación relevante en la nube.	Google Workspace: Herramientas colaborativas para crear y gestionar documentación. OneDrive for Business (parte de Microsoft 365): Almacenamiento y acceso seguro a documentos para partes interesadas.	No Aplica
Gestión de la Continuidad del Negocio y Resiliencia Operativa	Ejercicios de Continuidad de Negocio	**BCR-06**	Ejercitar y probar la continuidad del negocio y la resiliencia operativa al menos una vez al año o en caso de cambios significativos.	Microsoft Cloud App Security: Pruebas de políticas y control de acceso en aplicaciones en la nube. Netskope Security Cloud: Simulaciones para evaluar la efectividad de las políticas de seguridad en entornos de nube.	AWS Config: Herramientas para probar y verificar configuraciones de seguridad y cumplimiento. Azure Security Center: Proporciona funcionalidades para simular y probar escenarios de seguridad y continuidad.	No Aplica
Gestión de la Continuidad del Negocio y Resiliencia Operativa	Comunicación	**BCR-07**	Establecer comunicación con las partes interesadas y los participantes en la Procedimientos de continuidad y resiliencia del negocio	Microsoft Cloud App Security: Gestión de comunicaciones seguras. Netskope Security Cloud: Control del tráfico de datos en la nube.	AWS Config: Auditoría y aseguramiento de configuraciones de comunicación. Azure Security Center: Supervisión y seguridad en comunicaciones.	CWPP no se menciona aquí ya que se enfoca en la protección de cargas de trabajo, no en la gestión de comunicaciones.
Gestión de la Continuidad del Negocio y Resiliencia Operativa	Copia de seguridad	**BCR-08**	Realice copias de seguridad periódicas de los datos almacenados en la nube. Garantizar la confidencialidad, integridad y disponibilidad de la copia de seguridad, y verificar la restauración de datos a partir de la copia de seguridad para la resiliencia.	Microsoft Cloud App Security: Monitorea y asegura copias de seguridad en aplicaciones en la nube. Netskope Security Cloud: Protección de datos y gestión de copias de seguridad en entornos de nube.	AWS Backup: Gestión automatizada de copias de seguridad en AWS. Azure Backup: Servicio de copias de seguridad y restauración en Microsoft Azure.	Rubrik: Protección y gestión de datos, incluyendo copias de seguridad y recuperación. Veeam: Soluciones de backup y recuperación para asegurar la integridad y disponibilidad de datos.

Gestión de la Continuidad del Negocio y Resiliencia Operativa	Plan de Respuesta a Desastres	**BCR-09**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Un plan de respuesta a desastres para recuperarse de los desastres naturales y provocados por el hombre. Actualizar el plan al menos una vez al año o en caso de cambios significativos.	Microsoft Cloud App Security: Gestión y documentación de políticas para respuesta a desastres. Netskope Security Cloud: Control y evaluación de protocolos de seguridad para emergencias.	AWS Config: Herramientas para auditar y evaluar la resiliencia ante desastres. Azure Security Center: Gestión y actualización de planes de respuesta a desastres.	VMware Site Recovery Manager: Automatización de la recuperación ante desastres. Zerto: Plataformas para la continuidad del negocio y la recuperación de desastres.
Gestión de la Continuidad del Negocio y Resiliencia Operativa	Ejercicio del Plan de Respuesta	**BCR-10**	Ejercitar el plan de respuesta ante desastres anualmente o cuando cambios, incluidas, si es posible, las autoridades locales de emergencia.			
Gestión de la Continuidad del Negocio y Resiliencia Operativa	Redundancia de equipos	**BCR-11**	Complemente los equipos críticos para el negocio con equipos redundantes de forma independiente ubicado a una distancia mínima razonable de acuerdo con la industria aplicable normas.			
Change Control and Configuration Management - CCC						
Control de cambios y gestión de la configuración	Política y procedimientos de gestión de cambios	**CCC-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para gestionar los riesgos asociados a la aplicación de cambios a los activos de la organización, incluidas las aplicaciones, los sistemas, la infraestructura, la configuración, etc., independientemente de si los activos se gestionan interna o externamente (es decir, subcontratados). Revisar y actualizar las políticas y procedimientos al menos una vez al año	Microsoft Cloud App Security: Facilita la supervisión y control de cambios en aplicaciones en la nube. Netskope Security Cloud: Permite gestionar y controlar los cambios en el uso de aplicaciones en la nube.	AWS Config: Herramienta que registra y evalúa cambios en la configuración de recursos en AWS. Azure Policy: Automatiza y controla políticas para asegurar la gestión de cambios en Azure.	Palo Alto Networks Prisma Cloud: Supervisa y protege contra cambios no autorizados en cargas de trabajo en la nube. Symantec Cloud Workload Protection: Detecta y responde a cambios en la configuración de seguridad en entornos de nube.

Control de cambios y gestión de la configuración	Pruebas de calidad	**CCC-02**	Seguir un proceso definido de control de cambios de calidad, aprobación y pruebas con líneas de base, pruebas y estándares de lanzamiento establecidos.
Control de cambios y gestión de la configuración	Tecnología de gestión del cambio	**CCC-03**	Gestionar los riesgos asociados a la aplicación de cambios en la organización activos, incluidas las aplicaciones, los sistemas, la infraestructura, la configuración, etc., independientemente de si los activos se gestionan interna o externamente (es decir, externalizado).
Control de cambios y gestión de la configuración	Protección contra cambios no autorizados	**CCC-04**	Restrinja la adición, eliminación, actualización y administración no autorizadas de los activos de la organización.
Control de cambios y gestión de la configuración	Acuerdos de cambio	**CCC-05**	Incluir disposiciones que limiten los cambios que afecten directamente a los CSC de propiedad entornos/inquilinos a solicitudes autorizadas explícitamente dentro del nivel de servicio acuerdos entre los CSP y los CSC.
Control de cambios y gestión de la configuración	Línea base de gestión de cambios	**CCC-06**	Establecer líneas de base de gestión de cambios para todas las Cambios en los activos de la organización
Control de cambios y gestión de la configuración	Detección de la desviación de la línea de base	**CCC-07**	Implemente medidas de detección con notificación proactiva en caso de que de cambios que se desvían de la línea de base establecida.
Control de cambios y gestión de la configuración	Gestión de excepciones	**CCC-08**	«Aplicar un procedimiento para la gestión de las excepciones, que incluya emergencias, en el proceso de cambio y configuración. Alinee el procedimiento con los requisitos de la GRC-04: Proceso de excepción de políticas»
Control de cambios y gestión de la configuración	Restauración de cambios	**CCC-09**	Defina e implemente un proceso para revertir los cambios de forma proactiva en Un buen estado conocido anterior en caso de errores o problemas de seguridad

Cryptography, Encryption & Key Management - CEK						
Criptografía, Encriptación y Gestión de Claves	Política y procedimientos de cifrado y administración de claves	**CEK-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la criptografía, el cifrado y la gestión de claves. Revisión y actualizar las políticas y procedimientos al menos una vez al año.			
Criptografía, Encriptación y Gestión de Claves	Funciones y responsabilidades de CEK	**CEK-02**	Defina e implemente la gestión criptográfica, de cifrado y de claves funciones y responsabilidades.	Microsoft Cloud App Security: Administra políticas de cifrado y claves para aplicaciones en la nube. Netskope Security Cloud: Controla el cifrado y la gestión de claves en entornos de nube.	AWS Key Management Service (KMS): Gestiona claves de cifrado de forma segura. Azure Key Vault: Centraliza la administración de claves en un entorno protegido.	Palo Alto Networks Prisma Cloud: Implementa políticas de cifrado y administra claves en cargas de trabajo. Symantec Cloud Workload Protection: Supervisa el cifrado y las claves en la nube.
Criptografía, Encriptación y Gestión de Claves	Cifrado de datos	**CEK-03**	Proporcionar protección criptográfica a los datos en reposo y en tránsito, Uso de bibliotecas criptográficas certificadas según estándares aprobados.			
Criptografía, Encriptación y Gestión de Claves	Algoritmo de encriptación	**CEK-04**	Utilizar algoritmos de cifrado que sean apropiados para la protección de datos, teniendo en cuenta la clasificación de los datos, los riesgos asociados y la usabilidad de los tecnología de encriptación			
Criptografía, Encriptación y Gestión de Claves	Gestión de cambios de cifrado	**CEK-05**	Establecer un procedimiento estándar de gestión de cambios, para cambios de fuentes internas y externas, para su revisión, aprobación, implementación y la comunicación de la tecnología criptográfica, de cifrado y de gestión de claves Cambios			
Criptografía, Encriptación y Gestión de Claves	Análisis de costo-beneficio del cambio de cifrado	**CEK-06**	Gestione y adopte cambios en la criptografía, el cifrado y la gestión de claves sistemas (incluidas las políticas y los procedimientos) que tengan plenamente en cuenta las Efectos de los cambios propuestos, incluido el análisis de riesgos residuales, costos y beneficios			
Criptografía, Encriptación y Gestión de Claves	Gestión de riesgos de cifrado	**CEK-07**	Establecer y mantener un programa de riesgo de cifrado y administración de claves que incluya disposiciones para la evaluación de riesgos, el tratamiento de riesgos, el contexto de riesgo, monitoreo y retroalimentación.			

Criptografía, Encriptación y Gestión de Claves	Capacidad de gestión de claves CSC	**CEK-08**	Los CSP deben proporcionar la capacidad para que los CSC administren sus propios datos claves de cifrado.	McAfee MVISION Cloud: Permite a los clientes controlar y gestionar sus claves de cifrado, asegurando la privacidad y seguridad de sus datos. Bitglass CASB: Ofrece soluciones de cifrado con la opción de que los clientes administren sus propias claves.	AWS Key Management Service (KMS): Permite a los usuarios crear y gestionar sus propias claves de cifrado en AWS. Azure Key Vault: Facilita a los clientes la capacidad de importar, generar y administrar sus propias claves de cifrado en Azure.	VMware Cloud Trust Authority: Ofrece control de claves como servicio, permitiendo a los clientes gestionar sus claves de cifrado de forma segura. Thales CipherTrust Cloud Key Manager: Permite a los clientes gestionar y controlar el acceso a sus claves de cifrado en múltiples nubes.
Criptografía, Encriptación y Gestión de Claves	Auditoría de cifrado y gestión de claves	**CEK-09**	Audite los sistemas, las políticas y los procesos de cifrado y gestión de claves con una frecuencia proporcional a la exposición al riesgo del sistema con auditoría que se efectúe preferiblemente de forma continua, pero al menos una vez al año y después de cualquier evento(s) de seguridad.	Microsoft Cloud App Security: Ofrece capacidades de auditoría para políticas de cifrado y gestión de claves, permitiendo revisiones continuas. Netskope Security Cloud: Proporciona herramientas de auditoría y monitoreo en tiempo real para las políticas y prácticas de cifrado y claves.	AWS Key Management Service (KMS): Incluye funciones de auditoría para rastrear el uso y administración de claves de cifrado. Azure Key Vault: Proporciona registros de auditoría detallados que facilitan el seguimiento de las operaciones de cifrado y clave.	Palo Alto Networks Prisma Cloud: Realiza auditorías de configuraciones de cifrado y control de claves en las cargas de trabajo de la nube. Symantec Cloud Workload Protection: Ofrece capacidades de auditoría para verificar la implementación y gestión de políticas de cifrado y claves.
Criptografía, Encriptación y Gestión de Claves	Generación de claves	**CEK-10**	Genere claves criptográficas utilizando claves criptográficas aceptadas por la industria Bibliotecas que especifican la fuerza del algoritmo y el generador de números aleatorios usado.	Microsoft Cloud App Security: Facilita la generación de claves seguras utilizando bibliotecas criptográficas estándar de la industria. Netskope Security Cloud: Soporta la creación de claves con bibliotecas validadas para asegurar la robustez criptográfica	AWS Key Management Service (KMS): Utiliza bibliotecas criptográficas aprobadas para la generación de claves, cumpliendo con estándares de la industria. Azure Key Vault: Permite la generación de claves seguras usando generadores de números aleatorios fuertes y bibliotecas validadas.	Palo Alto Networks Prisma Cloud: Asegura la generación de claves usando métodos y bibliotecas criptográficas recomendadas. Thales CipherTrust Cloud Key Manager: Permite la generación de claves utilizando bibliotecas criptográficas estándar y asegura la gestión de claves en entornos multi-nube.
Criptografía, Encriptación y Gestión de Claves	Propósito clave	**CEK-11**	Administrar el secreto criptográfico y las claves privadas que se aprovisionan para un propósito único.			

Criptografía, Encriptación y Gestión de Claves	Rotación de teclas	**CEK-12**	Rotar las claves criptográficas de acuerdo con el período criptográfico calculado, que incluye disposiciones para considerar el riesgo de divulgación de información y los requisitos legales y reglamentarios.			
Criptografía, Encriptación y Gestión de Claves	Revocación de claves	**CEK-13**	Definir, implementar y evaluar procesos, procedimientos y medidas para revocar y eliminar las claves criptográficas antes de que finalice su cryptoperiod, cuando una clave se ve comprometida o una entidad ya no forma parte de la borganización, que incluyen disposiciones para los requisitos legales y reglamentarios.			
Criptografía, Encriptación y Gestión de Claves	Destrucción de llaves	**CEK-14**	Definir, implementar y evaluar procesos, procedimientos y Medidas para destruir las claves almacenadas fuera de un entorno seguro y revocar las claves almacenados en módulos de seguridad de hardware (HSM) cuando ya no son necesarios, lo que incluir disposiciones sobre los requisitos legales y reglamentarios.			
Criptografía, Encriptación y Gestión de Claves	Activación de claves	**CEK-15**	Definir, implementar y evaluar procesos, procedimientos y Medidas para crear claves en un estado preactivado cuando se han generado pero no autorizadas para su uso, que incluyen disposiciones legales y reglamentarias Requisitos.			
Criptografía, Encriptación y Gestión de Claves	Suspensión de llaves	**CEK-16**	Definir, implementar y evaluar procesos, procedimientos y medidas para monitorear, revisar y aprobar transiciones clave de cualquier estado hacia/desde suspensión, que incluyen disposiciones sobre los requisitos legales y reglamentarios.			
Criptografía, Encriptación y Gestión de Claves	Desactivación de claves	**CEK-17**	Definir, implementar y evaluar procesos, procedimientos y medidas para desactivar las claves en el momento de su fecha de caducidad, que incluyen disposiciones para los requisitos legales y reglamentarios.			
Criptografía, Encriptación y Gestión de Claves	Archivo clave	**CEK-18**	Definir, implementar y evaluar procesos, procedimientos y Medidas para gestionar las claves archivadas en un repositorio seguro que requiere privilegios mínimos acceso, que incluyen disposiciones sobre los requisitos legales y reglamentarios.	CipherCloud: Gestiona claves archivadas con control de acceso. Forcepoint CASB: Seguridad y cumplimiento en la gestión de claves.	Google Cloud KMS: Almacenamiento seguro de claves con acceso restringido. IBM Cloud Key Protect: Políticas de acceso estrictas para la gestión de claves	Symantec Cloud Workload Protection: Seguridad avanzada para claves archivadas. Trend Micro Deep Security: Controles detallados para proteger claves almacenadas.

Criptografía, Encriptación y Gestión de Claves	Compromiso clave	**CEK-19**	Definir, implementar y evaluar procesos, procedimientos y medidas para utilizar claves comprometidas para cifrar información solo en circunstancias controladas, y, a partir de entonces, exclusivamente para descifrar datos y nunca para cifrar datos, que incluyen disposiciones para los requisitos legales y reglamentarios.	Microsoft Cloud App Security: Monitorea y controla el uso de claves comprometidas. Netskope Security Cloud: Restringe el uso de claves comprometidas a operaciones de descifrado.	AWS Key Management Service (KMS): Gestiona claves comprometidas, limitando su uso al descifrado. Azure Key Vault: Aplica políticas para el uso restringido de claves comprometidas.	Palo Alto Networks Prisma Cloud: Administra claves, incluido el manejo de claves comprometidas. Symantec Cloud Workload Protection: Controla el uso de claves en situaciones de compromiso.
Criptografía, Encriptación y Gestión de Claves	Recuperación de claves	**CEK-20**	Definir, implementar y evaluar procesos, procedimientos y medidas para evaluar el riesgo para la continuidad operativa frente al riesgo de material de clave y la información que protege que se expone si el control de se pierde el material de codificación, que incluye disposiciones legales y reglamentarias Requisitos.			
Criptografía, Encriptación y Gestión de Claves	Gestión de inventario clave	**CEK-21**	Definir, implementar y evaluar procesos, procedimientos y para que el sistema de gestión de claves rastree e informe de todos los materiales y cambios en el estado, que incluyen disposiciones legales y reglamentarias Requisitos			
Datacenter Security - DCS						
Seguridad del centro de datos	Política y Procedimientos de Eliminación de Equipos Fuera del Sitio	**DCS-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la eliminación segura de equipos utilizados fuera del locales de la organización. Si el equipo no se destruye físicamente, un dato procedimiento de destrucción que imposibilite la recuperación de la información aplicado. Revisar y actualizar las políticas y procedimientos al menos una vez al año	Forcepoint CASB: Supervisa la eliminación segura de datos en dispositivos externos. CipherCloud CASB+: Implementa y audita políticas de eliminación de datos en dispositivos fuera del sitio.	Google Cloud Security Command Center: Verifica la eliminación de datos en dispositivos gestionados en Google Cloud. IBM Cloud Security and Compliance Center: Supervisa la eliminación de datos conforme a políticas en dispositivos externos.	Blancco Data Eraser: Soluciones de borrado de datos certificadas para evitar la recuperación de datos. WipeDrive: Destruye datos en almacenamientos para cumplir con requisitos de seguridad.
Seguridad del centro de datos	Política y Procedimientos de Autorización de Transferencia Fuera del Sitio	**DCS-02**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la reubicación o transferencia de hardware, software, o datos/información a una ubicación externa o alternativa. La reubicación o transferencia requiere la autorización escrita o verificable criptográficamente. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	Forcepoint CASB: Supervisa transferencias de datos a ubicaciones externas con autorización requerida. CipherCloud CASB+: Gestiona seguridad en transferencias de datos, con auditorías criptográficas.	Google Cloud Security Command Center: Monitorea y controla las transferencias de activos cloud. IBM Cloud Security and Compliance Center: Asegura cumplimiento en transferencias de activos conforme a políticas.	Varonis Data Security Platform: Audita y controla transferencias de datos autorizadas. Digital Guardian: Vigila y verifica autorización en el movimiento de datos sensibles.

Seguridad del centro de datos	Política y procedimientos de área segura	**DCS-03**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para mantener un entorno de trabajo seguro y protegido en oficinas, habitaciones e instalaciones. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	Forcepoint CASB: Implementa políticas de seguridad aplicables a entornos físicos. CipherCloud CASB+: Garantiza la conformidad con políticas de seguridad en accesos físicos a recursos en la nube.	Google Cloud Security Command Center: Influencia la seguridad física al integrar sistemas de seguridad física con infraestructuras en la nube. IBM Cloud Security and Compliance Center: Supervisa la aplicación de políticas de seguridad que incluyen aspectos físicos.	Honeywell Building Technologies: Sistemas de seguridad integrados para oficinas y facilidades. Bosch Security Systems: Soluciones de seguridad y vigilancia para proteger espacios físicos.
Seguridad del centro de datos	Política y procedimientos de transporte seguro de medios	**DCS-04**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para el transporte seguro de medios físicos. Revisión y actualizar las políticas y procedimientos al menos una vez al año.	Forcepoint CASB: Supervisa la transferencia segura de datos, aplicable también a medios físicos. CipherCloud CASB+: Asegura la implementación de políticas para proteger datos en medios durante el transporte.	Google Cloud Security Command Center: Ayuda a aplicar políticas de seguridad durante el transporte de medios relacionados con la nube. IBM Cloud Security and Compliance Center: Garantiza el cumplimiento de políticas de seguridad en el transporte de datos.	Iron Mountain: Provee servicios de transporte y gestión segura de medios físicos. ArmorSafe Technologies: Ofrece soluciones para el transporte y almacenamiento seguro de medios.
Seguridad del centro de datos	Clasificación de Activos	**DCS-05**	Clasificar y documentar los activos físicos y lógicos (por ejemplo, aplicaciones) basado en el riesgo de negocio de la organización.	Forcepoint CASB: Identifica y clasifica datos en la nube basándose en el riesgo. CipherCloud CASB+: Clasifica y protege datos en la nube según su nivel de riesgo.	Google Cloud Security Command Center: Clasifica y evalúa activos en Google Cloud. IBM Cloud Security and Compliance Center: Herramientas para clasificar activos según el riesgo empresarial.	Symantec Asset Management Suite: Gestiona la clasificación de activos por riesgo. ServiceNow IT Asset Management: Clasifica y rastrea activos basándose en su importancia
Seguridad del centro de datos	Catalogación y seguimiento de activos	**DCS-06**	Catalogar y realizar un seguimiento de todos los activos físicos y lógicos relevantes ubicados en todos los sitios del CSP dentro de un sistema seguro.	Forcepoint CASB: Proporciona monitoreo y catalogación de activos en la nube. CipherCloud CASB+: Facilita el control y la catalogación de activos en la nube	Google Cloud Security Command Center: Herramientas para catalogar y seguir activos en Google Cloud. AWS Config: Automatiza el inventario de activos en AWS.	ServiceNow IT Asset Management: Plataforma integral para la gestión de activos. BMC Helix Discovery: Automatiza la detección y gestión de activos en múltiples entornos.
Seguridad del centro de datos	Puntos de acceso controlado	**DCS-07**	Implementar perímetros de seguridad física para salvaguardar al personal, los datos, y sistemas de información. Establecer perímetros de seguridad física entre el las áreas administrativas y de negocio y las instalaciones de almacenamiento y procesamiento de datos Áreas.	Forcepoint CASB: Apoya en la implementación de políticas de seguridad, incluyendo accesos físicos. CipherCloud CASB+: Soporta la gestión de control de acceso físico mediante políticas de seguridad.	Google Cloud Security Command Center: Puede extender políticas de seguridad a controles físicos. AWS Config: Configuración de políticas de seguridad que pueden influir en accesos físicos	Honeywell Building Technologies: Sistemas para control de acceso y seguridad de perímetros. Bosch Security Systems: Soluciones para la seguridad perimetral y control de acceso en áreas críticas.

Seguridad del centro de datos	Identificación de equipos	**DCS-08**	Utilice la identificación del equipo como método para la autenticación de la conexión.	Forcepoint CASB: Gestiona la autenticación de dispositivos para acceso a recursos en la nube. CipherCloud CASB+: Asegura la identificación precisa y autenticación de dispositivos.	Google Cloud Security Command Center: Integra la identificación de dispositivos en políticas de acceso. AWS Config: Controla la autenticación de dispositivos en AWS.	Microsoft Azure Active Directory: Maneja identidad y autenticación de dispositivos. Okta Identity Management: Proporciona autenticación robusta de dispositivos para acceso seguro.
Seguridad del centro de datos	Autorización de área segura	**DCS-09**	Permitir el acceso exclusivo del personal autorizado a las áreas seguras, con todas las puntos de entrada y salida restringidos, documentados y supervisados por mecanismos de control de acceso. Conserve los registros de control de acceso de forma periódica según lo considere apropiado la organización.	Forcepoint CASB: Monitorea y controla el acceso a recursos, aplicable a áreas físicas seguras. CipherCloud CASB+: Supervisa y controla accesos, adaptable a controles físicos.	Google Cloud Security Command Center: Aplica políticas de acceso a la gestión de áreas seguras. AWS Config: Configura políticas de acceso que reflejan prácticas de seguridad física.	Honeywell Building Technologies: Sistemas de control de acceso para áreas restringidas. Bosch Security Systems: Tecnología que asegura acceso solo a personal autorizado y registra entradas y salidas.
Seguridad del centro de datos	Sistema de vigilancia	**DCS-10**	Implementar, mantener y operar sistemas de vigilancia de centros de datos en el perímetro externo y en todos los puntos de entrada y salida para detectar Intentos de entrada y salida no autorizados.			
Seguridad del centro de datos	Capacitación en respuesta a accesos no autorizados	**DCS-11**	Capacitar al personal del centro de datos para responder a la entrada no autorizada o Intentos de salida	Forcepoint CASB: Ofrece recursos para la formación en manejo de accesos no autorizados. CipherCloud CASB+: Proporciona informes útiles para entrenar al personal en la identificación y respuesta a incidentes de seguridad.	Google Cloud Security Command Center: Aporta datos de incidentes para capacitaciones de seguridad. AWS Config: Suministra alertas y registros que son esenciales para la formación en detección y respuesta a accesos.	SANS Institute: Cursos y certificaciones en seguridad física y respuesta a incidentes. ISC2: Formación y certificaciones sobre cómo responder adecuadamente a incidentes y accesos no autorizados.
Seguridad del centro de datos	Seguridad del cableado	**DCS-12**	Definir, implementar y evaluar procesos, procedimientos y medidas que garanticen una protección de la energía y las telecomunicaciones basada en el riesgo cables de una amenaza de interceptación, interferencia o daño en todas las instalaciones, Oficinas y habitaciones	Forcepoint CASB: Puede alertar sobre amenazas a infraestructuras físicas, incluyendo cableado. CipherCloud CASB+: Ofrece análisis adaptativos para monitorear la integridad del cableado.	Google Cloud Security Command Center: Configura alertas para monitorear la seguridad del cableado. AWS Config: Administra configuraciones de seguridad que protegen infraestructuras de cableado.	Panduit Physical Infrastructure Manager: Gestiona y protege la infraestructura de cableado. CommScope Automated Infrastructure Management: Asegura y monitorea la integridad del cableado.

Seguridad del centro de datos	Sistemas Ambientales	**DCS-13**	Implementar y mantener sistemas de control ambiental del centro de datos que monitorean, mantienen y prueban la eficacia continua de la temperatura y condiciones de humedad dentro de los estándares aceptados de la industria.	Forcepoint CASB: Puede integrar alertas sobre condiciones ambientales en su monitoreo de seguridad. CipherCloud CASB+: Adapta su supervisión a variables ambientales críticas.	Google Cloud Security Command Center: Configura políticas para mantener estándares ambientales. AWS Config: Gestiona directrices de control ambiental para centros de datos.	Schneider Electric EcoStruxure: Monitoriza y gestiona el ambiente en centros de datos. Emerson Network Power Liebert: Especializa en el control de condiciones ambientales para optimizar la operación de centros de datos.
Seguridad del centro de datos	Utilidades seguras	**DCS-14**	Asegure, supervise, mantenga y pruebe los servicios públicos de forma continua eficacia a intervalos planificados.	Forcepoint CASB: Monitorea servicios públicos dentro de su plataforma de seguridad. CipherCloud CASB+: Incluye supervisión de servicios públicos en su monitoreo de seguridad.	Google Cloud Security Command Center: Ayuda a configurar y monitorear la seguridad de servicios públicos. AWS Config: Gestiona la seguridad y operación de infraestructuras de servicios públicos en AWS.	Schneider Electric Building Management Systems: Proporciona gestión y monitoreo para servicios públicos. Johnson Controls Facility Management: Ofrece monitoreo y mantenimiento para optimizar la seguridad y eficacia de servicios públicos.
Seguridad del centro de datos	Ubicación del equipo	**DCS-15**	Mantenga los equipos críticos para el negocio alejados de lugares sujetos a probabilidad de eventos de riesgo ambiental.	Forcepoint CASB y CipherCloud CASB+: Aunque centrados en la seguridad de datos, no abordan directamente la ubicación física de equipos.	Google Cloud Security Command Center y AWS Config: Monitorean recursos en la nube pero no están enfocados en la ubicación física de equipos críticos.	AutoCAD Architecture: Ayuda a diseñar instalaciones estratégicamente para evitar zonas de riesgo ambiental. ArcGIS: Proporciona análisis geoespacial para planificar la ubicación de equipos críticos lejos de áreas de riesgo.
Data Security and Privacy Lifecycle Management - DSP						
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Política y procedimientos de seguridad y privacidad	**DSP-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para la clasificación, protección y tratamiento de datos a lo largo de su ciclo de vida, y de acuerdo con todas las leyes y reglamentos aplicables, estándares y nivel de riesgo. Revisar y actualizar las políticas y procedimientos en al menos una vez al año.	Forcepoint CASB: Implementa y monitorea políticas de seguridad y privacidad en la nube. CipherCloud CASB+: Gestiona la protección de datos y privacidad conforme a estándares y regulaciones.	Google Cloud Security Command Center: Configura y revisa políticas de seguridad y privacidad en Google Cloud. AWS Config: Asegura el cumplimiento de políticas y procedimientos actualizados en AWS.	OneTrust: Plataforma para gestionar el cumplimiento de privacidad y seguridad de datos. RSA Archer: Ayuda en la gestión de riesgos y cumplimiento relacionados con la seguridad y privacidad de datos.

Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Eliminación segura	**DSP-02**	Aplicar métodos aceptados por la industria para la eliminación segura de datos de medios de almacenamiento de tal manera que los datos no sean recuperables por ningún medio forense.	Forcepoint CASB: Implementa políticas para la eliminación segura de datos en la nube. CipherCloud CASB+: Asegura que la eliminación de datos en la nube cumpla con métodos seguros.	Google Cloud Security Command Center: Aplica políticas de eliminación segura en Google Cloud. AWS Config: Verifica que los procedimientos de eliminación en AWS sean irrecuperables.	Blancco Data Eraser: Soluciones certificadas para el borrado seguro de datos. WipeDrive: Software que cumple con estándares internacionales para asegurar que los datos eliminados no sean recuperables.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Inventario de datos	**DSP-03**	Crear y mantener un inventario de datos, al menos para cualquier datos y datos personales.	Forcepoint CASB: Identifica y clasifica datos en la nube para mantener un inventario actualizado. CipherCloud CASB+: Proporciona visibilidad y control sobre datos sensibles en la nube, facilitando la gestión del inventario.	Google Cloud Security Command Center: Monitorea y cataloga datos en Google Cloud, incluyendo datos personales. AWS Config: Permite configurar políticas para gestionar inventarios de datos sensibles.	Varonis Data Classification Framework: Identifica y clasifica datos sensibles para mantener un inventario preciso. Commvault Data Governance: Ofrece soluciones para gestionar y proteger datos sensibles, asegurando el cumplimiento normativo.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Clasificación de datos	**DSP-04**	Clasifique los datos según su tipo y nivel de sensibilidad.	Forcepoint CASB: Clasifica datos en la nube para aplicar políticas de seguridad. CipherCloud CASB+: Identifica y clasifica datos sensibles en la nube.	Google Cloud Security Command Center: Clasifica datos en Google Cloud para aplicar controles de seguridad. AWS Config: Facilita la clasificación y aplicación de políticas de seguridad en AWS.	Varonis Data Classification Framework: Clasifica datos automáticamente según su contenido y sensibilidad. Microsoft Azure Information Protection: Etiqueta y clasifica datos en Azure según políticas predefinidas.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Documentación del flujo de datos	**DSP-05**	Crear documentación de flujo de datos para identificar qué datos se procesan, almacenados o transmitidos dónde. Revisar la documentación del flujo de datos a intervalos definidos, al menos una vez al año, y después de cualquier cambio.	Netskope CASB: Documenta y visualiza el flujo de datos en la nube, identificando su origen y destino. McAfee MVISION Cloud: Permite documentar y auditar el flujo de datos en entornos en la nube.	Azure Security Center: Ayuda a documentar y auditar el flujo de datos en Azure, identificando su origen y destino. AWS Security Hub: Proporciona capacidades para documentar y visualizar el flujo de datos en AWS.	Varonis Data Risk Assessment: Facilita la documentación del flujo de datos en entornos locales y en la nube. DataSunrise Database Security: Permite auditar y documentar el movimiento de datos en bases de datos.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Propiedad y administración de datos	**DSP-06**	Documentar la propiedad y la administración de todo el personal documentado relevante y datos sensibles. Realizar la revisión al menos una vez al año.	Bitglass CASB: Permite asignar propietarios a datos sensibles en la nube y gestionar su acceso. Symantec CloudSOC CASB: Facilita la identificación de propietarios de datos y la gestión de su acceso en entornos en la nube.	Azure Purview: Ayuda a identificar y asignar propietarios a conjuntos de datos en Azure, facilitando su gestión. AWS IAM (Identity and Access Management): Permite definir y gestionar roles y permisos de acceso a datos en AWS.	Informatica Axon Data Governance: Permite documentar la propiedad de datos y establecer políticas de acceso y uso. Collibra Data Governance: Facilita la documentación de la propiedad de datos y la gestión de su acceso en toda la organización.

Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Protección de datos desde el diseño y por defecto	**DSP-07**	Desarrollar sistemas, productos y prácticas comerciales basadas en un principio de seguridad por diseño y mejores prácticas de la industria.	Cisco Cloudlock: Proporciona herramientas para integrar políticas de seguridad desde el diseño en aplicaciones en la nube. Netskope CASB: Ofrece funcionalidades para aplicar políticas de protección de datos desde el diseño en entornos en la nube.	Google Cloud Security Command Center: Permite implementar prácticas de seguridad por defecto en servicios de Google Cloud. AWS Security Hub: Facilita la configuración de políticas de seguridad predeterminadas en servicios de AWS.	OWASP Application Security Verification Standard (ASVS): Ofrece directrices para integrar seguridad desde el diseño en aplicaciones. Microsoft Secure Development Lifecycle (SDL): Proporciona un marco para desarrollar software con seguridad integrada desde el inicio.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Privacidad de datos desde el diseño y por defecto	**DSP-08**	Desarrollar sistemas, productos y prácticas comerciales basadas en un principio de privacidad por diseño y las mejores prácticas de la industria. Garantizar la privacidad de los sistemas Los ajustes se configuran de forma predeterminada, de acuerdo con todas las leyes y regulaciones aplicables.	McAfee MVISION Cloud: Herramientas para políticas de privacidad desde el diseño. Symantec CloudSOC CASB: Configuración de ajustes predeterminados para privacidad en la nube.	Azure Privacy and Compliance: Establecimiento de ajustes predeterminados en Azure. AWS Config: Configuraciones para cumplimiento de regulaciones de privacidad en AWS.	GDPR Privacy by Design Framework: Directrices para integrar privacidad desde el diseño. ISO/IEC 27701: Marco para gestionar privacidad de la información.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Evaluación de impacto de la protección de datos	**DSP-09**	Llevar a cabo una evaluación de impacto de la protección de datos (EIPD) para origen, naturaleza, particularidad y gravedad de los riesgos sobre el tratamiento de datos personales, de acuerdo con las leyes, reglamentos y la industria aplicables mejores prácticas.	Netskope CASB: Evalúa el impacto de protección de datos en la nube. Microsoft Cloud App Security: Identifica riesgos de tratamiento de datos en aplicaciones en la nube.	Google Cloud Security Command Center: Evalúa riesgos y cumplimiento en Google Cloud. AWS Security Hub: Realiza evaluaciones de impacto de protección de datos en entornos de AWS.	OneTrust PIA: Facilita evaluaciones de impacto de protección de datos para cumplir con regulaciones como el GDPR. TrustArc Data Inventory & Mapping: Identifica riesgos de tratamiento de datos para cumplir con diversas regulaciones de privacidad.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Transferencia de datos confidenciales	**DSP-10**	Definir, implementar y evaluar procesos, procedimientos y Medidas que garanticen la protección de cualquier transferencia de datos personales o sensibles acceso no autorizado y solo se procesan dentro del alcance permitido por la leyes y reglamentos respectivos.	Bitglass CASB: Controles para proteger la transferencia de datos en la nube. Cisco Cloudlock: Define políticas de seguridad para la transferencia de datos.	Azure Information Protection: Cifra datos confidenciales durante la transferencia en Azure. AWS KMS: Cifra datos sensibles para proteger la transferencia en AWS.	Symantec DLP: Protege datos mediante cifrado y control de acceso. McAfee Total Protection: Cifra datos para una transferencia segura en diversos entornos.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Acceso, reversión, rectificación y supresión de datos personales	**DSP-11**	Definir e implementar procesos, procedimientos y medidas técnicas para permitir que los interesados soliciten el acceso, la modificación o la eliminación de sus datos personales, de acuerdo con las leyes y reglamentos aplicables.	Netskope CASB: Controla el acceso y la eliminación de datos personales en la nube. McAfee MVISION Cloud: Configura políticas para gestionar solicitudes de acceso y eliminación de datos.	Microsoft Compliance Manager: Gestiona solicitudes de acceso y eliminación de datos en Microsoft Azure. Google Cloud DLP: Identifica y elimina datos personales automáticamente en Google Cloud.	OneTrust: Administra solicitudes de acceso y eliminación de datos para cumplir con las regulaciones de privacidad. TrustArc: Gestiona solicitudes de datos personales y garantiza el cumplimiento normativo.

Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Limitación de la finalidad en el tratamiento de datos personales	**DSP-12**	Definir, implementar y evaluar procesos, procedimientos y medidas para garantizar que los datos personales se procesen de acuerdo con las leyes y reglamentos y para los fines declarados al interesado.	Symantec CloudSOC CASB: Supervisa y controla el procesamiento de datos personales en la nube para cumplir con normativas.	McAfee MVISION Cloud: Define y hace cumplir políticas de uso de datos en la nube para asegurar su utilización conforme a los fines declarados.	OneTrust Privacy Management Platform: Gestiona políticas de tratamiento de datos para garantizar su uso autorizado. TrustArc Data Privacy Management Platform: Establece procesos para asegurar el tratamiento correcto de datos personales según las leyes y regulaciones.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Subtratamiento de datos personales	**DSP-13**	Definir, implementar y evaluar procesos, procedimientos y Medidas para la transferencia y el subprocesamiento de datos personales dentro del Servicio cadena de suministro, de acuerdo con las leyes y regulaciones aplicables.	DivvyCloud by Rapid7: Identificación y corrección de configuraciones inseguras.	Prisma Cloud Compute Security by Palo Alto Networks: Monitoreo y protección de cargas de trabajo en la nube.	No Aplica
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Divulgación de los subencargados del tratamiento de datos	**DSP-14**	Definir, implementar y evaluar procesos, procedimientos y medidas para divulgar los detalles de cualquier dato personal o sensible al que accedan subencargados del tratamiento al titular de los datos antes del inicio de dicho tratamiento	Dome9 by Check Point: Supervisión de la configuración de los subencargados para garantizar la privacidad de los datos.	CloudHealth by VMware: Seguimiento y evaluación de la actividad de los subencargados para el cumplimiento normativo.	No Aplica
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Limitación del uso de datos de producción	**DSP-15**	Obtener la autorización de los propietarios de los datos y gestionar el riesgo asociado antes de replicar o utilizar datos de producción en entornos que no sean de producción.	Symantec CloudSOC - Controla acceso y uso de datos de producción mediante autorización y auditoría. Microsoft Cloud App Security - Configura políticas para el uso autorizado de datos de producción.	AWS Config - Audita y monitorea el uso de datos en AWS, asegurando autorización. Azure Security Center - Gestiona riesgos y autorizaciones para datos de producción en Azure.	No Aplica
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Retención y eliminación de datos	**DSP-16**	La retención, el archivo y la eliminación de datos se gestionan de acuerdo con requisitos comerciales, leyes y regulaciones aplicables.	McAfee MVISION Cloud - Gestiona políticas de retención y eliminación de datos según regulaciones legales. Netskope Security Cloud - Implementa controles para la retención y eliminación de datos, asegurando cumplimiento normativo.	IBM Cloud Security and Compliance Center - Administra la retención y eliminación de datos en conformidad con leyes. Google Cloud Security Command Center - Controla y audita la retención y eliminación de datos de acuerdo a normativas.	No Aplica

Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Protección de datos sensibles	**DSP-17**	Definir e implementar procesos, procedimientos y medidas técnicas para proteger los datos confidenciales a lo largo de su ciclo de vida.	Symantec CloudSOC - Encripta y controla el acceso a datos sensibles. Microsoft Cloud App Security - Clasifica y protege datos confidenciales mediante políticas de seguridad.	Palo Alto Networks Prisma Cloud - Monitorea configuraciones y políticas de seguridad para proteger datos sensibles. Trend Micro Cloud One - Inspecciona y asegura el cumplimiento para la protección de datos sensibles.	Symantec Data Center Security - Ofrece protección integral para datos sensibles en cargas de trabajo en la nube. McAfee Cloud Workload Security - Protege datos confidenciales en entornos virtuales y en la nube.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Notificación de divulgación	**DSP-18**	El CSP debe contar con el procedimiento para gestionar y responder a las solicitudes de divulgación de datos personales por parte de las fuerzas del orden Autoridades de acuerdo con las leyes y reglamentos aplicables. El CSP debe dar especial atención al procedimiento de notificación a los CSC interesados, a menos que se indique lo contrario prohibida, como la prohibición en virtud del derecho penal de preservar la confidencialidad de una investigación policial.	McAfee MVISION Cloud - Gestiona respuestas a solicitudes legales de acceso a datos, asegurando cumplimiento y confidencialidad. Microsoft Cloud App Security - Administra la divulgación de datos a autoridades, cumpliendo con normativas y manteniendo la confidencialidad.	Palo Alto Networks Prisma Cloud - Herramientas para gestionar respuestas legales y notificar a los clientes conforme a la ley. IBM Cloud Security and Compliance Center - Maneja solicitudes legales y notifica a los interesados de forma segura y conforme a la ley.	Symantec Data Center Security - Responde a solicitudes legales preservando la confidencialidad donde sea necesario. Trend Micro Deep Security - Responde a solicitudes de autoridades garantizando cumplimiento y notificación adecuada a clientes.
Gestión del ciclo de vida de la seguridad y la privacidad de los datos	Ubicación de los datos	**DSP-19**	Definir e implementar procesos, procedimientos y medidas técnicas para especificar y documentar las ubicaciones físicas de los datos, incluidas las ubicaciones en el que se procesan o respaldan los datos.	Netskope Security Cloud - Proporciona visibilidad y documentación de las ubicaciones de datos en la nube. Microsoft Cloud App Security - Monitorea y documenta las ubicaciones de datos en aplicaciones de nube.	AWS Config - Visualiza y documenta ubicaciones de datos en AWS. Azure Security Center - Identifica y documenta ubicaciones de datos en Azure.	VMware Carbon Black Cloud - Visualiza y controla ubicaciones de datos en nube y servidores físicos. McAfee Cloud Workload Security - Identifica y documenta ubicaciones de datos en entornos de nube y virtuales.
Governance, Risk and Compliance - GRC						
Gobernanza, Riesgo y Cumplimiento	Política y procedimientos del programa de gobernanza	**GRC-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para un programa de gobierno de la información, que está patrocinado por el liderazgo de la organización. Revisar y actualizar las políticas y procedimientos al menos una vez al año..	McAfee MVISION Cloud - Gestiona políticas de seguridad y cumplimiento, asegurando revisiones regulares. Netskope Security Cloud - Implementa y administra políticas de seguridad en la nube, con actualizaciones continuas.	IBM Cloud Security and Compliance Center - Proporciona un marco para establecer y revisar políticas de seguridad y cumplimiento. Palo Alto Networks Prisma Cloud - Documenta, aplica y revisa políticas y procedimientos de seguridad en la nube.	VMware Carbon Black Cloud - Establece y revisa políticas de seguridad para cargas de trabajo en la nube. Trend Micro Deep Security - Crea y mantiene políticas de seguridad, asegurando su revisión y cumplimiento continuo.

Gobernanza, Riesgo y Cumplimiento	Programa de Gestión de Riesgos	**GRC-02**	Establecer una empresa formal, documentada y patrocinada por el liderazgo Programa de Gestión de Riesgos (ERM, por sus siglas en inglés) que incluye políticas y procedimientos para la identificación, Evaluación, propiedad, tratamiento y aceptación de la seguridad y privacidad en la nube Riesgos.	Microsoft Cloud App Security - Gestiona riesgos en aplicaciones de nube. Netskope Security Cloud - Identifica y maneja riesgos en la nube.	Qualys Cloud Platform - Evalúa y gestiona riesgos de seguridad en la nube. Palo Alto Networks Prisma Cloud - Herramientas para mitigar riesgos en la nube.	VMware Carbon Black Cloud - Gestión de riesgos para cargas de trabajo en la nube. McAfee Cloud Workload Security - Maneja riesgos en entornos virtuales y en la nube.
Gobernanza, Riesgo y Cumplimiento	Revisiones de políticas organizacionales	**GRC-03**	Revisar todas las políticas relevantes de la organización y los procedimientos asociados al menos una vez al año o cuando se produzca un cambio sustancial dentro de la organización.	Microsoft Cloud App Security - Monitoriza y actualiza políticas de seguridad continuamente. Netskope Security Cloud - Gestiona y revisa automáticamente políticas y procedimientos.	AWS Config - Rastrea y audita cambios en políticas de seguridad. Azure Security Center - Revisa continuamente políticas y procedimientos de seguridad.	VMware Carbon Black Cloud - Evalúa y revisa políticas de seguridad para cargas de trabajo. McAfee Cloud Workload Security - Gestiona y actualiza políticas de seguridad para cargas de trabajo.
Gobernanza, Riesgo y Cumplimiento	Proceso de excepción de directiva	**GRC-04**	Establecer y seguir un proceso de excepción aprobado según lo dispuesto por el el programa de gobernanza cada vez que se produce una desviación de una política establecida.	Microsoft Cloud App Security - Gestiona excepciones a políticas de seguridad en la nube. Netskope Security Cloud - Crea y supervisa excepciones a políticas según la gobernanza.	AWS Config - Configura y gestiona excepciones en políticas de seguridad. Palo Alto Networks Prisma Cloud - Administra excepciones dentro del marco de seguridad y gobernanza.	VMware Carbon Black Cloud - Gestiona excepciones en políticas de seguridad para cargas de trabajo. McAfee Cloud Workload Security - Administra excepciones a políticas de seguridad, alineadas con la gobernanza.
Gobernanza, Riesgo y Cumplimiento	Programa de Seguridad de la Información	**GRC-05**	Desarrollar e implementar un Programa de Seguridad de la Información, que incluya programas para todos los dominios relevantes del MCP.	Symantec CloudSOC - Gestiona seguridad en la nube cubriendo múltiples dominios. Netskope Security Cloud - Ofrece seguridad integral para varios dominios de información en la nube	Palo Alto Networks Prisma Cloud - Proporciona seguridad y cumplimiento en múltiples dominios de la nube. AWS Security Hub - Centraliza la gestión de seguridad y cumplimiento para dominios de AWS	VMware Carbon Black Cloud - Unifica la seguridad de cargas de trabajo en la nube, abarcando varios dominios. McAfee Cloud Workload Security - Asegura cargas de trabajo en la nube a través de múltiples dominios.
Gobernanza, Riesgo y Cumplimiento	Modelo de Responsabilidad de Gobernanza	**GRC-06**	Definir y documentar las funciones y responsabilidades para la planificación, implementación, Operar, evaluar y mejorar los programas de gobernanza.	Microsoft Cloud App Security - Gestiona roles y responsabilidades en la seguridad de aplicaciones en la nube. Netskope Security Cloud - Asigna y documenta responsabilidades en políticas de seguridad en la nube.	Cisco Secure Cloud Insights - Herramientas para gestionar responsabilidades en la seguridad de la infraestructura de la nube. Azure Security Center - Define y documenta roles y responsabilidades en seguridad Azure.	VMware Carbon Black Cloud - Marco para definir responsabilidades en protección de cargas de trabajo en la nube. McAfee Cloud Workload Security - Clarifica roles y responsabilidades en la seguridad de entornos en la nube.

Gobernanza, Riesgo y Cumplimiento	Mapeo Regulatorio del Sistema de Información	**GRC-07**	Identificar y documentar todas las normas, reglamentos, y los requisitos legales, que son aplicables a su organización	McAfee MVISION Cloud - Identifica y aplica requisitos regulatorios para datos en la nube. Netskope Security Cloud - Analiza y asegura el cumplimiento normativo en servicios de nube.	IBM Cloud Security and Compliance Center - Herramientas para gestionar requisitos regulatorios en la nube. Palo Alto Networks Prisma Cloud - Sistema para mapear y cumplir normativas en configuraciones de nube.	VMware Carbon Black Cloud - Cumple requisitos regulatorios en protección de cargas de trabajo en la nube. McAfee Cloud Workload Security - Identifica y cumple regulaciones en entornos de nube y virtuales.
Gobernanza, Riesgo y Cumplimiento	Grupos de Interés Especial	**GRC-08**	Establecer y mantener contacto con personas de interés especial relacionadas con la nube grupos y otras entidades pertinentes en consonancia con el contexto empresarial	Microsoft Cloud App Security - Comunicación segura con grupos de interés. Netskope Security Cloud - Interacción segura con partes interesadas en la nube.	AWS Security Hub - Colaboración para seguridad en la nube. Cisco Secure Cloud Insights - Conexión con partes interesadas para gestión de riesgos.	VMware Carbon Black Cloud - Coordinación con grupos interesados en seguridad de cargas de trabajo en la nube. McAfee Cloud Workload Security - Colaboración en seguridad de cargas de trabajo en entornos de nube.
Human Resources - HRS						
Recursos humanos	Política y procedimientos de investigación de antecedentes	**HRS-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la verificación de antecedentes de todos los nuevos empleados (incluyendo pero no limitado a empleados remotos, contratistas y terceros) de acuerdo con a las leyes, reglamentos, normas éticas y contractuales locales, así como a las a la clasificación de los datos a los que se va a acceder, a los requisitos empresariales y a los riesgo. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	Netskope Security Cloud - Implementa y gestiona políticas de verificación de antecedentes para usuarios remotos y contratistas en la nube. McAfee MVISION Cloud - Integra controles de acceso con procesos de verificación de antecedentes para cumplir con regulaciones y proteger datos en la nube.	Azure Security Center - Configura políticas de seguridad, incluida la verificación de antecedentes, para usuarios en entornos de nube Azure. AWS IAM - Establece políticas de acceso y verificación de antecedentes para usuarios y recursos en infraestructuras AWS.	VMware Carbon Black Cloud - Aplica políticas de verificación de antecedentes para usuarios autorizados en cargas de trabajo en la nube. McAfee Cloud Workload Security - Proporciona controles avanzados de seguridad, incluyendo verificación de antecedentes, para proteger cargas de trabajo en entornos de nube.
Recursos humanos	Política y procedimientos de uso aceptable de la tecnología	**HRS-02**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para definir las concesiones y condiciones para la Uso de activos de propiedad o gestión de la organización. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	Netskope Security Cloud - Gestiona políticas de uso aceptable para activos en la nube. Microsoft Cloud App Security - Aplica políticas de uso aceptable en aplicaciones en la nube.	AWS Config - Define y aplica políticas de uso aceptable para recursos en la nube de AWS. Azure Policy - Crea y aplica políticas de uso aceptable para entornos de nube Azure.	VMware Carbon Black Cloud - Implementa políticas de uso aceptable para cargas de trabajo en la nube. Trend Micro Cloud One - Define y aplica políticas de uso aceptable para cargas de trabajo en la nube.

Recursos humanos	Política y Procedimientos de Escritorio Limpio	**HRS-03**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos que requieren que los espacios de trabajo desatendidos no tengan datos confidenciales visibles. Revisar y actualizar las políticas y procedimientos en al menos una vez al año.	Netskope Security Cloud - Evita la visibilidad de datos confidenciales en escritorios desatendidos. McAfee MVISION Cloud - Previene la exposición de datos confidenciales en espacios de trabajo no supervisados.	AWS Config - Configura políticas para proteger datos confidenciales en la nube de AWS. Azure Security Center - Monitorea y protege espacios de trabajo para evitar la visibilidad de datos sensibles.	VMware Carbon Black Cloud - Protege datos confidenciales en cargas de trabajo en la nube, incluidos los escritorios desatendidos. Trend Micro Cloud One - Aplica controles avanzados para prevenir la exposición de datos confidenciales en la nube.
Recursos humanos	Política y procedimientos de trabajo remoto y en casa	**HRS-04**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para proteger la información a la que se accede, se procesa o se almacena en sitios y ubicaciones remotas. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	McAfee MVISION Cloud - Establece políticas de acceso para proteger la información en ubicaciones remotas. Microsoft Cloud App Security - Detecta y previene la pérdida de datos en sitios y ubicaciones remotos.	AWS Security Hub - Implementa políticas de seguridad para proteger la información en entornos de nube de AWS, incluidos los sitios de trabajo remoto. Azure Security Center - Monitorea y protege la información en ubicaciones remotas en entornos de nube Azure.	VMware Carbon Black Cloud - Aplica controles de seguridad avanzados para proteger la información en cargas de trabajo en la nube, incluido el trabajo remoto. Trend Micro Cloud One - Protege datos en ubicaciones remotas en la nube, garantizando la seguridad y el cumplimiento de las políticas.
Recursos humanos	Rentabilidad de activos	**HRS-05**	Establecer y documentar los procedimientos para la devolución de los bienes propiedad de la organización activos de los empleados despedidos.	McAfee MVISION Cloud: Monitorea y controla el acceso a recursos en la nube, asegurando la devolución de accesos al terminar relaciones laborales. Microsoft Cloud App Security: Permite el monitoreo de actividad y gestión del acceso a la nube para facilitar la revocación de accesos a ex-empleados.	Palo Alto Networks Prisma Cloud: Proporciona visibilidad y control de configuraciones en la nube para cumplir políticas de seguridad en la devolución de activos. Checkpoint CloudGuard: Automatiza auditorías de configuraciones de seguridad en la nube, verificando la adherencia a políticas de devolución de activos.	No Aplica
Recursos humanos	Terminación de la relación laboral	**HRS-06**	Establecer, documentar y comunicar a todo el personal los procedimientos esbozando las funciones y responsabilidades relativas a los cambios en el empleo.	Cisco Cloudlock: Gestiona y automatiza políticas de seguridad y procedimientos de terminación laboral. Forcepoint CASB: Implementa y monitoriza políticas de acceso y comunicación de	Tenable.io: Proporciona visibilidad y control sobre las configuraciones de seguridad, facilitando la gestión de cambios en el empleo. Google Cloud Security Command Center: Supervisa la postura de seguridad y	No Aplica

				procedimientos de terminación.	ayuda en la comunicación de procedimientos de seguridad laboral.	
Recursos humanos	Proceso de Contrato de Empleo	**HRS-07**	Los empleados firman el acuerdo de empleado antes de que se les conceda el acceso a los sistemas, recursos y activos de información de la organización.	Microsoft Cloud App Security: Implementa acceso condicional basado en la firma de acuerdos. Netskope Security Cloud: Controla el acceso basado en políticas de cumplimiento de acuerdos.	Azure Security Center: Configura políticas de seguridad que requieren verificación de acuerdos firmados. AWS Security Hub: Asegura el cumplimiento de acuerdos antes de permitir acceso a AWS.	No Aplica
Recursos humanos	Contenido del contrato de trabajo	**HRS-08**	La organización incluye dentro de los contratos de trabajo disposiciones y/o términos para el cumplimiento de la gobernanza y seguridad de la información establecida políticas.	McAfee MVISION Cloud: Asegura el cumplimiento de políticas de seguridad en la nube. Symantec CloudSOC CASB: Monitoriza el acceso y uso de datos en la nube según las políticas contractuales.	Qualys Cloud Platform: Evalúa la conformidad con las políticas de seguridad continuamente. Dome9 (de Check Point): Gestiona la seguridad en la nube y verifica el cumplimiento con las políticas de los contratos.	No Aplica
Recursos humanos	Funciones y responsabilidades del personal	**HRS-09**	Documentar y comunicar las funciones y responsabilidades de los empleados, en lo que se refiere a los activos de información y la seguridad.	Microsoft Cloud App Security: Gestiona y asegura la claridad en las responsabilidades del personal en la nube. Cisco Cloudlock: Automatiza la gobernanza de seguridad y la comunicación de responsabilidades.	AWS Security Hub: Ofrece visibilidad y control sobre las políticas de seguridad, apoyando la documentación de responsabilidades. Azure Security Center: Ayuda a monitorizar y gestionar la seguridad, facilitando la definición de responsabilidades del personal.	Trend Micro Deep Security: Ayuda a asegurar el cumplimiento de responsabilidades en entornos de servidor y nube.
Recursos humanos	Acuerdos de confidencialidad	**HRS-10**	Identificar, documentar y revisar, a intervalos planificados, los requisitos acuerdos de no divulgación/confidencialidad que reflejen la necesidades de protección de datos y detalles operativos.	Netskope Security Cloud: Controla datos sensibles en la nube, apoyando el cumplimiento de acuerdos de confidencialidad. Symantec CloudSOC CASB: Supervisa el acceso a datos confidenciales, asegurando el respeto a los acuerdos.	Qualys Cloud Platform: Gestiona la conformidad y revisa las políticas de seguridad, incluyendo acuerdos de confidencialidad. Palo Alto Networks Prisma Cloud: Evalúa la seguridad y la conformidad continuamente para mantener acuerdos de confidencialidad efectivos.	No Aplica

Recursos humanos	Capacitación en concientización sobre seguridad	**HRS-11**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Un programa de formación en materia de seguridad para todos los empleados de la organización. y proporcionar actualizaciones periódicas de la formación.	Microsoft Cloud App Security: Monitorea la adhesión a las políticas de seguridad impartidas en capacitaciones. McAfee MVISION Cloud: Implementa y controla políticas de seguridad relacionadas con la capacitación.	IBM Cloud Security and Compliance Center: Gestiona y audita las políticas de seguridad enseñadas en las capacitaciones. Azure Security Center: Refuerza la formación continua y asegura la implementación de políticas de seguridad.	Trend Micro Deep Security: Integra principios de seguridad en la protección de cargas de trabajo en la nube.
Recursos humanos	Concientización y capacitación sobre datos personales y confidenciales	**HRS-12**	Proporcionar a todos los empleados acceso a información confidencial de la organización y datos personales con una formación adecuada en materia de seguridad y actualizaciones periódicas en los procedimientos, procesos y políticas organizacionales relacionados con sus función relativa a la organización.	Netskope Security Cloud: Controla el acceso y asegura que solo personal capacitado acceda a datos sensibles. Symantec CloudSOC CASB: Supervisa el uso de datos confidenciales y refuerza las políticas de seguridad.	Cisco Cloud Security: Administra y audita políticas de seguridad relacionadas con la capacitación. AWS Security Hub: Refuerza la formación y la implementación de políticas de seguridad	VMware Carbon Black Cloud: Aplica principios de seguridad de datos en entornos de carga de trabajo.
Recursos humanos	Cumplimiento de la responsabilidad del usuario	**HRS-13**	Hacer que los empleados sean conscientes de sus funciones y responsabilidades para el mantenimiento conocimiento y cumplimiento de las políticas y procedimientos establecidos y obligaciones de cumplimiento legal, estatutario o reglamentario.	Microsoft Cloud App Security: Monitorea el cumplimiento de políticas de seguridad y uso de recursos en la nube. Netskope Security Cloud: Controla el acceso y actividades en la nube, asegurando el cumplimiento de normativas.	AWS Security Hub: Gestiona y audita el cumplimiento de políticas y normativas. Azure Security Center: Monitorea y mejora la seguridad, facilitando la concientización sobre responsabilidades.	Trend Micro Deep Security: Aplica controles de seguridad consistentes en las cargas de trabajo en la nube.
Identity & Access Management - IAM						
Gestión de identidades y accesos	Política y procedimientos de administración de identidades y accesos	**IAM-01**	Establecer, documentar, aprobar, comunicar, implementar, aplicar, evaluar y mantener políticas y procedimientos para la gestión de identidades y accesos. Revisión y actualizar las políticas y procedimientos al menos una vez al año.	Okta Identity Cloud: Gestiona la autenticación de usuarios y el acceso seguro a servicios en la nube. Microsoft Cloud App Security: Integra y aplica políticas de acceso, proporcionando análisis de gestión de identidad.	Cisco Secure Access by Duo: Refuerza políticas de seguridad de acceso como la autenticación de dos factores. IBM Security Verify: Audita y gestiona el cumplimiento de políticas de identidad y acceso.	Palo Alto Networks Prisma Cloud: Apoya la aplicación de políticas de identidad y acceso en la nube.

Gestión de identidades y accesos	Política y procedimientos de contraseñas seguras	**IAM-02**	Establecer, documentar, aprobar, comunicar, implementar, aplicar, evaluar y mantener políticas y procedimientos de contraseñas seguras. Revise y actualice el archivo políticas y procedimientos al menos una vez al año.	LastPass Enterprise: Gestiona y refuerza políticas de contraseñas seguras. Dashlane Business: Proporciona herramientas para implementar y monitorear políticas de contraseñas robustas.	CyberArk Privileged Access Security: Especializado en seguridad de contraseñas para cuentas privilegiadas. Thycotic Secret Server: Aplica y audita políticas de contraseñas fuertes en accesos privilegiados.	No Aplica
Gestión de identidades y accesos	Inventario de identidad	**IAM-03**	Administrar, almacenar y revisar la información de las identidades del sistema, y nivel de acceso	SailPoint IdentityNow: Gestiona y monitorea identidades y accesos en sistemas y aplicaciones en la nube. OneLogin: Ofrece administración centralizada de identidades y niveles de acceso en la nube.	IBM Security Verify: Ayuda a revisar y gestionar identidades y accesos en entornos de nube. Azure Active Directory: Facilita la administración de identidades y control de accesos en Azure.	Palo Alto Networks Prisma Cloud: Integra la gestión de identidades y control de accesos en la protección de cargas de trabajo.
Gestión de identidades y accesos	Separación de funciones	**IAM-04**	Emplear el principio de separación de funciones al implementar la información acceso al sistema.	Microsoft Cloud App Security: Configura políticas de acceso para asegurar la segregación de funciones. Netskope Security Cloud: Controla el acceso basado en roles, fortaleciendo la separación de funciones.	Cisco Secure Access by Duo: Gestiona autenticación y acceso basado en roles, facilitando la separación de funciones. AWS Identity and Access Management (IAM): Define políticas de acceso granulares para separar roles y responsabilidades en AWS.	Palo Alto Networks Prisma Cloud: Aplica la gestión de acceso basada en roles y políticas en la protección de cargas de trabajo en la nube.
Gestión de identidades y accesos	Privilegios mínimos	**IAM-05**	Emplear el principio de privilegios mínimos al implementar información acceso al sistema.	Microsoft Cloud App Security: Implementa políticas de acceso condicional que restringen los privilegios según necesidades del rol. Netskope Security Cloud: Ofrece control de acceso detallado y granular, limitando los privilegios al mínimo necesario.	AWS Identity and Access Management (IAM): Crea políticas de acceso que confieren solo los privilegios esenciales para las funciones del usuario. Azure Security Center: Define y aplica políticas de acceso mínimo necesario en la nube.	Palo Alto Networks Prisma Cloud: Aplica gestión de acceso basada en mínimos privilegios para cargas de trabajo en la nube.
Gestión de identidades y accesos	Aprovisionamiento de acceso de usuarios	**IAM-06**	Definir e implementar un proceso de aprovisionamiento de acceso de usuarios que autorice, registra y comunica los cambios de acceso a los datos y activos	Okta Identity Cloud: Facilita el aprovisionamiento automático de acceso con autorización, registro y comunicación efectiva. OneLogin: Implementa flujos de trabajo	SailPoint IdentityNow: Ofrece gestión de identidades con capacidades de registro y auditoría de cambios de acceso. Cisco ISE (Identity Services Engine): Proporciona gestión de acceso a la red y	CyberArk Privileged Access Security: Gestiona el acceso privilegiado asegurando autorización, registro y comunicación adecuados.

				automatizados de aprovisionamiento y desaprovisionamiento de acceso.	recursos, con funciones de registro y reporte.	
Gestión de identidades y accesos	Cambios y revocación de acceso de usuario	**IAM-07**	Dar de baja o, respectivamente, modificar el acceso de los que se trasladan/abandonan o cambios en la identidad del sistema de manera oportuna con el fin de adoptar y Comunicar las políticas de gestión de identidades y accesos.	Microsoft Cloud App Security: Configura políticas automáticas para ajustar o revocar accesos alineados con políticas corporativas. Netskope Security Cloud: Proporciona control dinámico y granular sobre el acceso a recursos en la nube.	AWS Identity and Access Management (IAM): Gestiona y modifica derechos de acceso a recursos de AWS. Azure Active Directory: Asegura la gestión eficiente y segura de cambios en el acceso.	CyberArk Privileged Access Security: Maneja accesos privilegiados garantizando cambios o revocaciones seguras y oportunas.
Gestión de identidades y accesos	Revisión del acceso del usuario	**IAM-08**	Revise y vuelva a validar el acceso de los usuarios para obtener privilegios mínimos y separación de tareas con una frecuencia proporcional a la tolerancia al riesgo de la organización.	Microsoft Cloud App Security: Ajusta permisos para asegurar privilegios mínimos y separación de funciones. Netskope Security Cloud: Monitorea y revisa accesos para cumplir con políticas de seguridad.	AWS IAM: Revisa y ajusta permisos de usuario según necesidades de seguridad. Azure Security Center: Implementa y revisa políticas para garantizar acceso adecuado.	Palo Alto Networks Prisma Cloud: Continúa revisando accesos en la nube para mantener la seguridad.
Gestión de identidades y accesos	Segregación de roles de acceso privilegiado	**IAM-09**	Definir, implementar y evaluar procesos, procedimientos y medidas para la segregación de las funciones de acceso privilegiado, de modo que las Acceso a datos, capacidades de cifrado y gestión de claves y capacidades de registro son distintas y separadas.	Symantec CloudSOC CASB: Controla y segmenta el acceso basado en roles detallados para diferentes funciones. McAfee MVISION Cloud: Monitoriza y regula el acceso privilegiado, asegurando la segregación de roles.	Thycotic Secret Server: Gestiona accesos privilegiados y segrega funciones de administración de claves y acceso a datos. CyberArk Privileged Access Security: Implementa políticas de segregación de roles para datos sensibles y gestión de claves.	Palo Alto Networks Prisma Cloud: Aplica control de accesos basado en roles, segregando operaciones de registro y gestión de claves.
Gestión de identidades y accesos	Administración de roles de acceso privilegiado	**IAM-10**	Definir e implementar un proceso de acceso para garantizar el acceso privilegiado Los roles y derechos se otorgan por un período de tiempo limitado e implementan procedimientos para evitar la culminación del acceso privilegiado segregado.	Microsoft Cloud App Security: Configura políticas para limitar temporalmente el acceso privilegiado y revisar permisos periódicamente. Netskope Security Cloud: Gestiona accesos privilegiados con controles detallados y limitaciones temporales.	CyberArk Privileged Access Security: Ofrece gestión temporal de accesos privilegiados y auditorías regulares. Thycotic Secret Server: Limita la duración del acceso privilegiado y realiza auditorías para prevenir acumulaciones.	Palo Alto Networks Prisma Cloud: Aplica políticas de acceso temporal y monitorea el cumplimiento para evitar acumulaciones indebidas.

Gestión de identidades y accesos	Aprobación de CSC para roles de acceso privilegiado acordados	**IAM-11**	Definir, implementar y evaluar procesos y procedimientos para los clientes participar, en su caso, en la concesión de acceso a los Roles de acceso privilegiado de riesgo (tal y como se definen en la evaluación de riesgos de la organización).	McAfee MVISION Cloud: Configura flujos de trabajo de aprobación que incluyen a clientes, garantizando transparencia y cumplimiento. Netskope Security Cloud: Gestiona identidades y accesos con la posibilidad de integrar a clientes en los procesos de aprobación.	CyberArk Privileged Access Security: Ofrece un marco para gestionar accesos privilegiados con participación de clientes en aprobaciones. SailPoint IdentityNow: Permite colaboración de clientes en decisiones de aprobación de acceso privilegiado.	Palo Alto Networks Prisma Cloud: Adapta flujos de aprobación para incluir participación de clientes en la concesión de accesos privilegiados.
Gestión de identidades y accesos	Proteja la integridad de los registros	**IAM-12**	Definir, implementar y evaluar procesos, procedimientos y Medidas para garantizar que la infraestructura de registro sea de solo lectura para todos los usuarios con acceso, incluidos los roles de acceso privilegiado, y que la capacidad de deshabilitarlo se controla a través de un procedimiento que garantiza la segregación de funciones y Procedimientos de rotura de cristales.	Netskope Security Cloud: Asegura que los registros sean de solo lectura con controles avanzados para acceso privilegiado. McAfee MVISION Cloud: Protege la integridad de los registros, manteniéndolos inmutables y de solo lectura.	AWS CloudTrail y AWS IAM: Juntos, permiten políticas de solo lectura para registros y controlan quién puede desactivarlos. Azure Monitor y Azure Policy: Combinados para asegurar registros de solo lectura y limitar quién puede modificar o desactivar los registros.	Symantec Cloud Workload Protection: Mantiene registros seguros y de solo lectura, con controles estrictos sobre modificaciones.
Gestión de identidades y accesos	Usuarios identificables de forma única	**IAM-13**	Definir, implementar y evaluar procesos, procedimientos y medidas que garanticen la identificación de los usuarios a través de identificaciones únicas o que puedan asociar a las personas al uso de los ID de usuario.	Microsoft Cloud App Security: Asocia usuarios con actividades mediante integración con Azure AD. Netskope Security Cloud: Identifica usuarios de forma única y monitoriza sus acciones en la nube.	AWS IAM: Asigna identidades únicas y supervisa acciones en la nube. Azure Active Directory: Gestiona identidades únicas y su uso en Azure.	Symantec Cloud Workload Protection: Identifica y asocia usuarios con actividades en cargas de trabajo en la nube. Trend Micro Cloud One - Workload Security: Identifica usuarios y monitoriza sus acciones en cargas de trabajo.
Gestión de identidades y accesos	Autenticación fuerte	**IAM-14**	Definir, implementar y evaluar procesos, procedimientos y medidas para autenticar el acceso a los sistemas, las aplicaciones y los activos de datos, incluida la autenticación multifactor para al menos un usuario privilegiado y acceso a los datos. Adoptar certificados digitales o alternativas que logren una nivel de seguridad para las identidades del sistema.	Microsoft Cloud App Security: Aplica políticas de acceso con MFA para usuarios privilegiados y datos sensibles. Netskope Security Cloud: Implementa MFA y monitorea la autenticación en la nube para un acceso seguro a datos.	AWS IAM y Azure Active Directory: Configuran MFA para usuarios privilegiados y acceso a recursos, fortaleciendo la autenticación.	Palo Alto Networks Prisma Cloud y Symantec Cloud Workload Protection: Ofrecen MFA para proteger el acceso a cargas de trabajo y datos en la nube.

Gestión de identidades y accesos	Gestión de contraseñas	**IAM-15**	Definir, implementar y evaluar procesos, procedimientos y Medidas para la gestión segura de contraseñas.	McAfee MVISION Cloud: Gestiona políticas avanzadas de contraseñas y acceso seguro a aplicaciones en la nube. Microsoft Cloud App Security: Monitorea y maneja accesos y contraseñas en aplicaciones de nube.	AWS IAM: Implementa políticas robustas de contraseñas en AWS. Azure Security Center: Establece políticas de seguridad para la gestión de contraseñas en Azure.	No Aplica
Gestión de identidades y accesos	Mecanismos de autorización	**IAM-16**	Definir, implementar y evaluar procesos, procedimientos y medidas para verificar el acceso a los datos y a las funciones del sistema.	Netskope Security Cloud: Implementa políticas de autorización granulares para controlar el acceso a datos en la nube. Palo Alto Networks Prisma Access: Ofrece control de acceso basado en la identidad y el contexto del usuario.	Cisco Secure Access by Duo: Gestiona el acceso seguro y las políticas de autorización basadas en la identidad. IBM Cloud Security and Compliance Center: Permite definir y revisar políticas de acceso para asegurar la autorización adecuada.	Symantec Cloud Workload Protection: Proporciona controles de autorización para proteger las cargas de trabajo en la nube. VMware Carbon Black Cloud: Utiliza políticas de seguridad para controlar el acceso a aplicaciones y datos.
Interoperability & Portability - IPY						
Interoperabilidad y portabilidad	Política y Procedimientos de Interoperabilidad y Portabilidad	**IPY-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos de interoperabilidad y portabilidad, incluidos los siguientes: Requisitos para: un. Comunicaciones entre interfaces de aplicación b. Interoperabilidad en el procesamiento de la información c. Portabilidad del desarrollo de aplicaciones d. Intercambio de información/datos, uso, portabilidad, integridad y persistencia Revisar y actualizar las políticas y procedimientos al menos una vez al año.	McAfee MVISION Cloud: Gestiona la seguridad de las comunicaciones entre interfaces de aplicaciones. Netskope Security Cloud: Soporta políticas de seguridad que aseguran la interoperabilidad y portabilidad.	Microsoft Azure Policy: Define y aplica políticas de interoperabilidad y portabilidad. AWS Config: Evalúa la configuración de recursos para cumplir con estándares de interoperabilidad.	No Aplica

Interoperabilidad y portabilidad	Disponibilidad de la interfaz de la aplicación	**IPY-02**	Proporcione interfaces de aplicación a los CSC para que programen recuperar sus datos para permitir la interoperabilidad y la portabilidad.	Netskope Security Cloud: Asegura el acceso seguro y controlado a interfaces de aplicación. Microsoft Cloud App Security: Supervisa y controla el uso de interfaces para garantizar acceso seguro a datos.	AWS Config: Configura y asegura interfaces de aplicación en AWS. Azure Security Center: Monitorea y protege interfaces de aplicación en Azure.	Palo Alto Networks Prisma Cloud: Protege y monitorea interfaces de aplicación en la nube. Trend Micro Cloud One - Workload Security: Facilita la seguridad en el acceso a interfaces de aplicación.
Interoperabilidad y portabilidad	Gestión segura de la interoperabilidad y la portabilidad	**IPY-03**	Implemente protocolos de red criptográficamente seguros y estandarizados para la gestión, importación y exportación de datos.	McAfee MVISION Cloud: Asegura las transferencias de datos con protocolos de encriptación avanzados. Symantec CloudSOC: Utiliza protocolos criptográficos estándar para monitorear y controlar la transferencia de datos en la nube.	AWS Key Management Service (KMS): Gestiona claves de cifrado para encriptar datos. Azure Security Center: Asegura que se utilicen protocolos de red seguros en la transferencia de datos.	Palo Alto Networks Prisma Cloud: Implementa protocolos de encriptación para proteger las cargas de trabajo en la nube. Trend Micro Cloud One - Workload Security: Protege la transferencia de datos en la nube usando protocolos criptográficos seguros.
Interoperabilidad y portabilidad	Obligaciones contractuales de portabilidad de datos	**IPY-04**	Los acuerdos deben incluir disposiciones que especifiquen el acceso de los CSC a los datos a la terminación del contrato e incluirá: a. Formato de los datos b. Período de tiempo que se almacenarán los datos c. Alcance de los datos conservados y puestos a disposición de los CSC d. Política de eliminación de datos	Netskope Security Cloud: Controla y asegura el cumplimiento de las políticas contractuales sobre el acceso y formato de datos. Microsoft Cloud App Security: Implementa políticas de acceso y seguridad que cumplen con los requisitos contractuales de retención y formato de datos.	AWS Config: Monitoriza y audita configuraciones para cumplir con las políticas de retención y eliminación de datos. Azure Policy: Gestiona políticas de gobernanza que aseguran el cumplimiento del formato, retención y eliminación de datos.	Palo Alto Networks Prisma Cloud: Protege datos y asegura que los requisitos contractuales sobre el alcance y retención de datos se cumplan. Symantec Cloud Workload Protection: Aplica políticas de seguridad que incluyen la retención y eliminación de datos conforme a los acuerdos contractuales.
Infrastructure & Virtualization Security - IVS						
Seguridad de infraestructura y virtualización	Política y procedimientos de seguridad de infraestructura y virtualización	**IVS-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para la seguridad de la infraestructura y la virtualización. Revisión y actualizar las políticas y procedimientos al menos una vez al año.	McAfee MVISION Cloud: Monitorea y aplica políticas de seguridad en entornos de nube. Microsoft Cloud App Security: Proporciona control y visibilidad sobre aplicaciones en la nube, facilitando la seguridad.	AWS Security Hub: Gestiona la seguridad y las configuraciones en AWS. Azure Security Center: Ofrece herramientas para mejorar la seguridad en infraestructuras Azure.	Palo Alto Networks Prisma Cloud: Protege cargas de trabajo en la nube, incluyendo contenedores y VMs. Symantec Cloud Workload Protection: Asegura cargas de trabajo y ambientes virtualizados.

Seguridad de infraestructura y virtualización	Planificación de la capacidad y los recursos	**IVS-02**	Planificar y supervisar la disponibilidad, la calidad y la capacidad adecuada de recursos con el fin de ofrecer el rendimiento requerido del sistema según lo determinado por parte de la empresa.	Netskope Security Cloud: Proporciona visibilidad sobre el uso de recursos en la nube. Microsoft Cloud App Security: Ofrece análisis y reportes para gestionar el uso de recursos en la nube.	AWS Cost Management Tools: Herramientas para monitorizar y gestionar el uso y costos de recursos en AWS. Azure Monitor: Proporciona datos sobre rendimiento y utilización de recursos en Azure.	VMware Tanzu Observability by Wavefront: Ofrece análisis profundos para planificar la capacidad y gestionar recursos eficientemente. Datadog: Monitoriza cargas de trabajo en la nube en tiempo real, apoyando la planificación de capacidad.
Seguridad de infraestructura y virtualización	Seguridad de la red	**IVS-03**	Supervise, cifre y restrinja las comunicaciones entre entornos solo a conexiones autenticadas y autorizadas, según lo justifique la empresa. Revise estas configuraciones al menos una vez al año y apóyelas mediante un Justificación de todos los servicios, protocolos, puertos y controles compensatorios permitidos.	McAfee MVISION Cloud: Controla y cifra el tráfico de red en la nube, asegurando conexiones autenticadas. Netskope Security Cloud: Monitorea y restringe el acceso de red a conexiones autorizadas.	Palo Alto Networks Prisma Cloud: Supervisa las configuraciones de red, aplicando restricciones a conexiones autorizadas. Cisco Secure Workload: Utiliza microsegmentación y análisis de flujo para garantizar que solo el tráfico autorizado se mueva entre servicios.	Symantec Cloud Workload Protection: Monitoriza y controla el acceso a la red en cargas de trabajo en la nube. Trend Micro Deep Security: Proporciona inspección de intrusiones y monitorización del tráfico, asegurando conexiones seguras y autorizadas.
Seguridad de infraestructura y virtualización	Protección del sistema operativo y controles básicos	**IVS-04**	Refuerce el sistema operativo host e invitado, el hipervisor o el plano de control de la infraestructura de acuerdo con sus respectivas mejores prácticas, y con el apoyo de controles técnicos, como parte de una línea base de seguridad	McAfee MVISION Cloud: Proporciona visibilidad y control para asegurar configuraciones de seguridad en entornos de nube. Microsoft Cloud App Security: Ayuda a monitorear y asegurar las configuraciones de sistemas operativos y hipervisores.	AWS Systems Manager: Automatiza la configuración y mantenimiento de sistemas operativos según mejores prácticas. Azure Security Center: Ofrece recomendaciones para reforzar sistemas operativos y hipervisores en Azure.	Symantec Cloud Workload Protection: Aplica políticas de seguridad y detecta amenazas en sistemas operativos. Trend Micro Deep Security: Brinda protección integral incluyendo antimalware y control de integridad para sistemas en la nube y locales.
Seguridad de infraestructura y virtualización	Entornos de producción y no producción	**IVS-05**	Separe los entornos de producción y los que no lo son.	Netskope Security Cloud: Monitorea y controla el tráfico entre entornos en la nube para asegurar segregación. Microsoft Cloud App Security: Proporciona visibilidad y políticas para mantener separados los entornos de producción y no producción.	AWS Organizations: Gestiona políticas de seguridad en múltiples cuentas de AWS para separar entornos. Azure Policy: Aplica políticas de gobernanza y seguridad para mantener la separación entre entornos.	Palo Alto Networks Prisma Cloud: Protege cargas de trabajo en la nube asegurando segregación de entornos. Symantec Cloud Workload Protection: Implementa políticas de seguridad específicas para cada tipo de entorno.

Seguridad de infraestructura y virtualización	Segmentación y segregación	**IVS-06**	Diseñar, desarrollar, desplegar y configurar aplicaciones e infraestructuras de modo que el acceso de usuario de CSP y CSC (inquilino) y el acceso dentro del inquilino sean adecuados segmentados y segregados, monitoreados y restringidos de otros inquilinos.	Netskope Security Cloud: Controla y monitoriza el acceso para asegurar segregación entre inquilinos. Microsoft Cloud App Security: Supervisa las actividades y el acceso en aplicaciones de nube para mantener la separación entre inquilinos.	Cisco Secure Workload: Implementa microsegmentación para controlar el acceso entre y dentro de inquilinos. Azure Security Center: Aplica políticas de seguridad para garantizar la segregación adecuada en entornos Azure.	Palo Alto Networks Prisma Cloud: Ofrece segmentación de redes y control de acceso para proteger cada inquilino. Symantec Cloud Workload Protection: Asegura cargas de trabajo en la nube mediante políticas de seguridad que mantienen la separación entre inquilinos.
Seguridad de infraestructura y virtualización	Migración a entornos en la nube	**IVS-07**	Utilice canales de comunicación seguros y encriptados al migrar servidores, servicios, aplicaciones o datos en entornos de nube. Dichos canales deben incluir: solo protocolos actualizados y aprobados.	McAfee MVISION Cloud: Protege las transferencias de datos hacia la nube mediante encriptación y protocolos seguros. Microsoft Cloud App Security: Asegura que las transferencias de datos usen canales seguros y protocolos aprobados.	AWS Certificate Manager: Gestiona certificados SSL/TLS para cifrar datos en tránsito hacia AWS. Azure Security Center: Monitorea que las comunicaciones en Azure utilicen canales cifrados y protocolos seguros.	Palo Alto Networks Prisma Cloud: Protege cargas de trabajo en la nube, ofreciendo evaluación de vulnerabilidades y protección contra amenazas en tiempo real. Symantec Cloud Workload Protection: Asegura cargas de trabajo en la nube con detección de intrusos y gestión de la integridad de la seguridad, incluyendo protección para contenedores.
Seguridad de infraestructura y virtualización	Documentación de la arquitectura de red	**IVS-08**	Identifique y documente los entornos de alto riesgo.	No Aplica	AWS Network Firewall: Permite documentar y controlar el tráfico de red en los entornos de AWS, facilitando la identificación y documentación de entornos de alto riesgo. Azure Security Center: Proporciona capacidades de visualización y análisis de red que ayudan a identificar y documentar áreas de alto riesgo en entornos Azure.	No Aplica

Seguridad de infraestructura y virtualización	Defensa de la red	**IVS-09**	Definir, implementar y evaluar procesos, procedimientos y defensa en profundidad Técnicas de protección, detección y respuesta oportuna a ataques basados en la red.	McAfee MVISION Cloud: Mejora la visibilidad de la actividad en la nube y ofrece detección de amenazas y respuesta a incidentes. Netskope Security Cloud: Proporciona protección avanzada contra amenazas y detección de anomalías en la nube.	Palo Alto Networks Prisma Cloud: Incluye detección de amenazas y respuesta automática para cargas de trabajo en la nube. Azure Defender: Ofrece detección de amenazas y recomendaciones de seguridad para fortalecer la infraestructura de red.	Symantec Cloud Workload Protection: Proporciona detección de amenazas y respuesta para cargas de trabajo en la nube. Trend Micro Deep Security: Incluye defensa contra intrusiones, monitorización de integridad y protección antimalware.
Logging and Monitoring - LOG						
Registro y monitoreo	Política y procedimientos de registro y supervisión	**LOG-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para el registro y el monitoreo. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	McAfee MVISION Cloud: Proporciona capacidades avanzadas para registro y monitoreo en la nube. Microsoft Cloud App Security: Ofrece herramientas detalladas para el registro de actividades y la supervisión en la nube.	AWS CloudTrail y AWS Config: Permiten un registro detallado y la gestión de configuraciones en AWS. Azure Monitor y Azure Log Analytics: Facilitan el registro y análisis exhaustivo de actividades en Azure.	Palo Alto Networks Prisma Cloud: Incluye funciones de registro y monitoreo para cargas de trabajo en la nube. Splunk Enterprise Security: Se usa para la agregación y análisis de logs, apoyando la seguridad y el cumplimiento.
Registro y monitoreo	Protección de registros de auditoría	**LOG-02**	Definir, implementar y evaluar procesos, procedimientos y medidas para garantizar la seguridad y la conservación de los registros de auditoría.	Netskope Security Cloud: Asegura registros de auditoría con cifrado y controles de acceso. McAfee MVISION Cloud: Protege registros mediante cifrado y políticas de acceso granulares.	AWS CloudTrail: Gestiona y almacena de forma segura registros de auditoría en AWS. Azure Security Center: Monitorea y protege registros de auditoría en Azure.	Symantec Cloud Workload Protection: Cifra y controla el acceso a registros de auditoría. Palo Alto Networks Prisma Cloud: Implementa políticas de seguridad para proteger registros de auditoría.
Registro y monitoreo	Monitoreo y alertas de seguridad	**LOG-03**	Identifique y supervise los eventos relacionados con la seguridad dentro de las aplicaciones y la infraestructura subyacente. Definir e implementar un sistema para generar Alertas a las partes interesadas responsables en función de dichos eventos y las métricas correspondientes.	McAfee MVISION Cloud - Monitoreo y alertas en tiempo real. Netskope Security Cloud - Visibilidad completa y control de actividades en la nube.	Palo Alto Networks Prisma Cloud - Monitoreo continuo y cumplimiento de configuraciones. Check Point CloudGuard - Visibilidad y evaluación de riesgos con alertas automáticas.	Symantec Cloud Workload Protection - Protección y monitoreo de cargas de trabajo en la nube. Trend Micro Deep Security - Protección en tiempo real con monitoreo detallado.
Registro y monitoreo	Acceso y responsabilidad de los registros de auditoría	**LOG-04**	Restrinja el acceso a los registros de auditoría al personal autorizado y mantenga registros que proporcionan una responsabilidad de acceso única.	Microsoft Cloud App Security - Controla acceso y rastrea actividades autorizadas. Cisco Cloudlock - Restringe acceso a registros y asegura trazabilidad.	AWS CloudTrail - Gestiona eventos de auditoría con acceso limitado. Azure Monitor - Proporciona registros detallados con acceso restringido.	

Registro y monitoreo	Supervisión y respuesta de los registros de auditoría	**LOG-05**	Supervise los registros de auditoría de seguridad para detectar actividades fuera de las típicas o patrones esperados. Establecer y seguir un proceso definido para revisar y tomar Acciones apropiadas y oportunas sobre las anomalías detectadas.	Symantec CloudSOC - Monitorea y responde automáticamente a incidentes en registros. Bitglass - Supervisión en tiempo real con respuestas automatizadas.	Splunk Enterprise - Análisis y respuesta automatizada de registros. Google Cloud Security Command Center - Supervisa registros y responde a incidentes.	Aqua Security - Supervisión de actividad en registros con alertas automáticas. VMware Carbon Black Cloud - Vigilancia continua y respuesta a amenazas en tiempo real.
Registro y monitoreo	Sincronización del reloj	**LOG-06**	Utilice una fuente de tiempo confiable para todo el procesamiento de información relevante Sistemas.	No Aplica	AWS Time Sync Service - Sincronización precisa de tiempo para recursos de AWS. Google Cloud's Public NTP - Servicio de sincronización de tiempo en la infraestructura de Google Cloud.	No Aplica
Registro y monitoreo	Ámbito de registro	**LOG-07**	Establecer, documentar e implementar qué sistema de metadatos/metadatos de información Los eventos deben registrarse. Revise y actualice el alcance al menos una vez al año o cada vez que Hay un cambio en el entorno de amenazas.	Netskope Security Cloud - Configuración y revisión de políticas de registro. McAfee MVISION Cloud - Define y actualiza el alcance del registro según cambios ambientales.	IBM Cloud Security and Compliance Center - Establece y documenta eventos a registrar; revisa anualmente. Azure Security Center - Configuración y actualización continua del registro de eventos.	Trend Micro Cloud One - Facilita la definición y documentación de eventos registrables. Symantec Cloud Workload Protection - Configuración y revisión regular del registro de metadatos.
Registro y monitoreo	Registros de registro	**LOG-08**	Genere registros de auditoría que contengan información de seguridad relevante	McAfee MVISION Cloud - Genera registros detallados de auditoría con información de seguridad. Netskope Security Cloud - Capta eventos de seguridad críticos en sus registros de auditoría.	AWS Config - Registra cambios de configuración y detalles de seguridad. Azure Monitor - Recoge registros de auditoría con información de seguridad integrada.	Palo Alto Networks Prisma Cloud - Genera registros de auditoría de seguridad para cargas de trabajo en la nube. Qualys Cloud Platform - Proporciona registros detallados sobre el estado de seguridad de las cargas de trabajo.
Registro y monitoreo	Protección de registros	**LOG-09**	El sistema de información protege los registros de auditoría del acceso no autorizado, modificación y supresión.	Microsoft Cloud App Security - Protege registros con controles de acceso y alertas. Symantec CloudSOC - Cifra y monitoriza registros para evitar modificaciones no autorizadas.	IBM Cloud Security and Compliance Center - Implementa políticas de seguridad para proteger los registros. Splunk Enterprise Security - Gestiona y protege registros contra alteraciones y accesos indebidos.	VMware Carbon Black Cloud - Asegura registros contra modificaciones y eliminaciones no autorizadas. Aqua Security - Controles de acceso granulares y detección de anomalías para proteger registros.

Registro y monitoreo	Monitoreo e informes de cifrado	**LOG-10**	Establecer y mantener una capacidad de supervisión y presentación de informes internos sobre las operaciones de las políticas criptográficas, de cifrado y de gestión de claves, procesos, procedimientos y controles.	Symantec CloudSOC - Supervisa y reporta sobre políticas de cifrado y gestión de claves. Netskope Security Cloud - Reportes detallados sobre uso y eficacia de políticas de cifrado.	CipherCloud - Monitoreo exhaustivo y reportes de políticas de cifrado y gestión de claves. Thales CipherTrust Cloud Key Manager - Reportes detallados sobre uso y seguridad de claves.	HyTrust DataControl - Soluciones de cifrado y reporte detallado sobre gestión de claves. VMware Carbon Black Cloud - Visibilidad y control de políticas de cifrado y seguridad, incluida gestión de claves.
Registro y monitoreo	Registro de transacciones/actividad	**LOG-11**	Registre y supervise los eventos clave de administración del ciclo de vida para habilitar la auditoría e informes sobre el uso de claves criptográficas.	Microsoft Cloud App Security - Registra y supervisa la gestión de claves criptográficas, facilitando la auditoría. McAfee MVISION Cloud - Proporciona registro y monitoreo de eventos de administración de claves.	AWS Key Management Service (KMS) - Ofrece registro y monitoreo detallado de actividades de gestión de claves. Azure Key Vault - Supervisa el uso y administración de claves, con capacidades de informe.	Gemalto SafeNet KeySecure - Registra eventos del ciclo de vida de las claves y supervisa para auditorías. HashiCorp Vault - Gestiona claves con registro y monitoreo de transacciones, apoyando la auditoría y el cumplimiento.
Registro y monitoreo	Registros de control de acceso	**LOG-12**	Supervise y registre el acceso físico mediante un control de acceso auditable sistema.	AWS CloudTrail - Seguimiento de acceso usuario y API en AWS, con registros auditable. Azure Activity Log - Registra actividades de control de acceso, incluido el acceso físico.	AWS CloudTrail - Seguimiento de acceso usuario y API en AWS, con registros auditable. Azure Activity Log - Registra actividades de control de acceso, incluido el acceso físico.	VMware Carbon Black Cloud - Supervisa y registra acceso a sistemas y aplicaciones, con control auditable. Symantec Cloud Workload Protection - Sistema auditable para registrar y supervisar acceso a cargas de trabajo en la nube.
Registro y monitoreo	Informes de fallos y anomalías	**LOG-13**	Definir, implementar y evaluar procesos, procedimientos y Medidas para la notificación de anomalías y fallos del sistema de seguimiento y notificar inmediatamente a la parte responsable.	McAfee MVISION Cloud - Detecta y notifica anomalías y fallos en la nube. Microsoft Cloud App Security - Monitorea anomalías y fallos con notificaciones automáticas.	Splunk Enterprise - Monitoreo en tiempo real de fallos con alertas instantáneas. Datadog Cloud Monitoring - Detecta y notifica comportamientos anómalos y fallos.	Palo Alto Networks Prisma Cloud - Alertas inmediatas para fallos y anomalías en cargas de trabajo. Qualys Cloud Platform - Notifica anomalías y problemas en las cargas de trabajo al momento.
Security Incident Management, E-Discovery, & Cloud Forensics - SEF						
Gestión de incidentes de seguridad, e-Discovery y análisis forense en la nube	Política y procedimientos de gestión de incidentes de seguridad	**SEF-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la gestión de incidentes de seguridad, la exhibición de documentos electrónicos y la nube Forense. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	Netskope Security Cloud - Gestión integral de incidentes con políticas claras y actualizables. Symantec CloudSOC - Marco completo para la gestión de incidentes y análisis forense.	IBM Cloud Pak for Security - Herramientas para establecer y mantener políticas de seguridad y gestión de incidentes. Cisco SecureX - Integra gestión de incidentes con políticas y procedimientos forenses actualizables.	VMware Carbon Black Cloud - Gestión de incidentes de seguridad y herramientas forenses con políticas documentadas. CrowdStrike Falcon Platform - Solución integral para la gestión de incidentes y forense, con políticas actualizables.

Gestión de incidentes de seguridad, e-Discovery y análisis forense en la nube	Política y procedimientos de gestión de servicios	**SEF-02**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para la gestión oportuna de incidentes de seguridad. Revisión y actualizar las políticas y procedimientos al menos una vez al año.	McAfee MVISION Cloud - Gestiona y documenta políticas de incidentes con comunicación efectiva. Microsoft Cloud App Security - Permite actualización y aplicación efectiva de políticas de seguridad.	Tenable.io - Sistema para gestionar y mantener políticas de seguridad actualizadas. Splunk Enterprise Security - Implementa y monitorea políticas, facilitando evaluaciones regulares.	CrowdStrike Falcon Platform - Gestión avanzada de incidentes con políticas y procedimientos claros. Palo Alto Networks Prisma Cloud - Enfoque integrado para la gestión de políticas y procedimientos en la nube, con revisión anual.
Gestión de incidentes de seguridad, e-Discovery y análisis forense en la nube	Planes de respuesta a incidentes	**SEF-03**	«Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Un plan de respuesta a incidentes de seguridad, que incluye, entre otros: departamentos internos, CSC afectados y otras relaciones críticas para el negocio (como la cadena de suministro) que puedan verse afectadas».	Cisco Cloudlock - Gestiona planes de respuesta e integra departamentos y partes externas. Netskope Security Cloud - Avanzada gestión de respuesta con integración de cadena de suministro.	IBM Resilient - Plataforma para documentar y aplicar planes de respuesta, integrando stakeholders. Azure Sentinel - Automatiza y ejecuta planes de respuesta, colaborando con varios departamentos.	CrowdStrike Falcon - Respuesta rápida a incidentes con colaboración interdepartamental. VMware Carbon Black Cloud - Sistemático en la respuesta a incidentes, coordinando con partes internas y externas.
Gestión de incidentes de seguridad, e-Discovery y análisis forense en la nube	Pruebas de respuesta a incidentes	**SEF-04**	Pruebe y actualice según sea necesario los planes de respuesta a incidentes a intervalos planificados o en caso de cambios significativos en la organización o el entorno para su eficacia	Proofpoint CASB - Pruebas regulares y actualizaciones de planes de respuesta a incidentes. McAfee MVISION Cloud - Simulaciones y pruebas para evaluar y ajustar planes de respuesta.	Tenable.io - Capacidades para probar y ajustar planes de respuesta basados en evaluaciones de vulnerabilidad. Rapid7 InsightConnect - Automatiza pruebas y actualizaciones de planes de respuesta ante cambios organizacionales.	Red Canary - Marco para probar y ajustar planes de respuesta a incidentes. Palo Alto Networks Prisma Cloud - Herramientas para simular incidentes y probar respuestas, actualizando planes según necesidades.
Gestión de incidentes de seguridad, e-Discovery y análisis forense en la nube	Métricas de respuesta a incidentes	**SEF-05**	Establezca y supervise las métricas de incidentes de seguridad de la información.	Netskope Security Cloud - Análisis y métricas detalladas sobre incidentes de seguridad. Symantec CloudSOC - Medición y análisis de la respuesta a incidentes en la nube.	Splunk Enterprise Security - Establece y analiza métricas de incidentes de seguridad en tiempo real. Datadog Security Monitoring - Monitorea métricas de seguridad y ofrece respuesta rápida.	CrowdStrike Falcon - Provee métricas avanzadas para mejorar la respuesta a incidentes. VMware Carbon Black Cloud - Herramientas de análisis y reporte para métricas de respuesta a incidentes.
Gestión de incidentes de seguridad, e-Discovery y análisis forense en la nube	Procesos de clasificación de eventos	**SEF-06**	Definir, implementar y evaluar procesos, procedimientos y Medidas de apoyo a los procesos de negocio para clasificar los eventos relacionados con la seguridad.	Cisco Cloudlock - Clasifica eventos de seguridad según severidad e impacto en negocios. Microsoft Cloud App Security - Automatiza la clasificación de eventos de seguridad, priorizando según importancia	IBM QRadar on Cloud - Sistema avanzado para clasificar eventos según impacto empresarial. AWS Security Hub - Prioriza alertas de seguridad basándose en su importancia para procesos de negocio.	Palo Alto Networks Prisma Cloud - Clasificación de eventos de seguridad alineada con decisiones de negocio. Qualys Cloud Platform - Evalúa y clasifica eventos de seguridad según relevancia y urgencia para

				empresarial.		el negocio.
Gestión de incidentes de seguridad, e-Discovery y análisis forense en la nube	Notificación de violación de seguridad	**SEF-07**	Definir e implementar procesos, procedimientos y medidas técnicas para notificaciones de brechas de seguridad. Informar de las brechas de seguridad y la seguridad asumida incumplimientos, incluidos los incumplimientos relevantes de la cadena de suministro, según los SLA aplicables, leyes y reglamentos.	McAfee MVISION Cloud - Detecta y notifica rápidamente brechas de seguridad, cumpliendo con SLA y regulaciones. Netskope Security Cloud - Identifica y notifica brechas de seguridad según requisitos legales y contractuales.	Splunk Enterprise - Monitorea y notifica brechas de seguridad inmediatamente, asegurando cumplimiento con SLA y leyes. Tenable.io - Notifica violaciones de seguridad con reportes ajustados a SLA y regulaciones.	CrowdStrike Falcon - Detección y notificación rápida de brechas, cumpliendo con estándares legales y SLA. VMware Carbon Black Cloud - Detecta y notifica brechas de seguridad conforme a SLA y normativas.
Gestión de incidentes de seguridad, e-Discovery y análisis forense en la nube	Mantenimiento de puntos de contacto	**SEF-08**	Mantener puntos de contacto para las autoridades reguladoras aplicables, las fuerzas del orden nacionales y locales, y otras autoridades jurisdiccionales legales.	Netskope Security Cloud - Gestiona y revisa políticas de seguridad compartida. Microsoft Cloud App Security - Implementa y actualiza políticas dentro del marco de SSRM.	Palo Alto Networks Prisma Cloud - Establece y mantiene políticas de seguridad, evaluando continuamente. AWS Security Hub - Centraliza la gestión de políticas y su revisión.	VMware Carbon Black Cloud - Aplica y revisa políticas de seguridad en cargas de trabajo. Symantec Cloud Workload Protection - Gestiona y asegura el cumplimiento de políticas en la nube.
Supply Chain Management, Transparency, and Accountability - STA						
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Política y procedimientos de SSRM	**STA-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para la aplicación de la Responsabilidad de Seguridad Compartida (SSRM) dentro de la organización. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	Microsoft Cloud App Security - Gestión integral de la SSRM, incluyendo documentación y revisión. Cisco Cloudlock - Implementación y mantenimiento de políticas de SSRM con facilidades para la comunicación y aplicación.	IBM Cloud Security and Compliance Center - Herramientas para establecer, evaluar y revisar políticas de SSRM. Google Cloud Security Command Center - Gestión y actualización de políticas de SSRM, mejorando la postura de seguridad.	CrowdStrike Falcon - Gestión y revisión de políticas de seguridad en el contexto de SSRM para cargas de trabajo en la nube. Trend Micro Deep Security - Aplicación y mantenimiento de políticas de SSRM con evaluación continua.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Cadena de suministro de SSRM	**STA-02**	Aplicar, documentar, implementar y gestionar el SSRM a lo largo de todo el suministro para la oferta de servicios en la nube.	Netskope Security Cloud - Gestiona la seguridad de la cadena de suministro en la nube con políticas de SSRM. McAfee MVISION Cloud - Implementa y documenta SSRM en la cadena de suministro.	AWS Security Hub - Integra políticas de SSRM en la gestión de seguridad de la cadena de suministro. Microsoft Azure Security Center - Monitorea y gestiona la seguridad de la cadena de suministro con aplicación de SSRM.	Palo Alto Networks Prisma Cloud - Aplica y gestiona SSRM en la cadena de suministro de servicios en la nube. Symantec Cloud Workload Protection - Implementa políticas de SSRM protegiendo las cargas de trabajo en la cadena de suministro.

Gestión de la cadena de suministro, transparencia y rendición de cuentas	Guía de SSRM	**STA-03**	Proporcione orientación de SSRM al CSC detallando información sobre el Aplicabilidad de SSRM a lo largo de la cadena de suministro.	Cisco Cloudlock - Provee guías detalladas para implementar SSRM en la nube. Netskope Security Cloud - Ofrece recursos educativos sobre SSRM en la cadena de suministro.	AWS Security Hub - Brinda prácticas y guías sobre SSRM en la cadena de suministro de AWS. Microsoft Azure Security Center - Proporciona documentación y recomendaciones para SSRM en Azure.	VMware Carbon Black Cloud - Ofrece orientación sobre SSRM para proteger cargas de trabajo a lo largo de la cadena de suministro. Symantec Cloud Workload Protection - Da recursos para aplicar SSRM en la cadena de suministro de cargas de trabajo en la nube.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Propiedad del control de SSRM	**STA-04**	Delinear la propiedad compartida y la aplicabilidad de todos los controles de CSA CCM de acuerdo con el SSRM para la oferta de servicios en la nube.	McAfee MVISION Cloud - Proporciona visibilidad sobre la propiedad compartida de los controles de CSA CCM y su aplicabilidad en SSRM. Bitglass - Identifica y delinea la propiedad compartida de los controles de CSA CCM para SSRM.	Trend Micro Cloud One - Gestiona la propiedad compartida de los controles de CSA CCM para SSRM en la oferta de servicios en la nube. DivvyCloud by Rapid7 - Evalúa y gestiona la propiedad compartida de los controles de CSA CCM, asegurando su alineación con SSRM.	CrowdStrike Falcon - Brinda visibilidad y gestión de la propiedad compartida de los controles de CSA CCM para SSRM. Qualys Cloud Platform - Identifica y aplica los controles de CSA CCM de manera efectiva en el contexto de SSRM.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Revisión de la documentación de SSRM	**STA-05**	Revise y valide la documentación de SSRM para todas las ofertas de servicios en la nube que la organización utiliza.	Netskope Security Cloud - Analiza y valida la documentación de SSRM de múltiples servicios en la nube. Microsoft Cloud App Security - Revisa y valida la documentación de SSRM de servicios en la nube de Microsoft.	AWS Security Hub - Facilita la revisión y validación de la documentación de SSRM en AWS. Google Cloud Security Command Center - Permite validar la documentación de SSRM en la nube de Google.	CrowdStrike Falcon - Revisa la documentación de SSRM de cargas de trabajo en la nube. VMware Carbon Black Cloud - Valida la documentación de SSRM de cargas de trabajo en la nube.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Implementación del control SSRM	**STA-06**	Implementar, operar y auditar o evaluar las partes del SSRM de la que es responsable la organización.	McAfee MVISION Cloud - Implementa, opera y audita partes del SSRM bajo responsabilidad de la organización. Cisco Cloudlock - Ayuda en la implementación, operación y auditoría de controles de SSRM internos.	Trend Micro Cloud One - Facilita la implementación, operación y auditoría de partes del SSRM de responsabilidad de la organización. DivvyCloud by Rapid7 - Permite implementar, operar y auditar controles de SSRM internos.	CrowdStrike Falcon - Implementa, opera y audita partes del SSRM bajo responsabilidad de la organización. Qualys Cloud Platform - Ayuda en la implementación, operación y auditoría de controles de SSRM internos.

Gestión de la cadena de suministro, transparencia y rendición de cuentas	Inventario de la cadena de suministro	**STA-07**	Desarrollar y mantener un inventario de todas las relaciones de la cadena de suministro.	Netskope Security Cloud - Identifica y documenta relaciones de la cadena de suministro en la nube. McAfee MVISION Cloud - Desarrolla y mantiene un inventario completo de proveedores y sus conexiones.	Palo Alto Networks Prisma Cloud - Documenta relaciones de la cadena de suministro en la nube. AWS Security Hub - Desarrolla un inventario completo de la cadena de suministro en AWS.	CrowdStrike Falcon - Identifica y documenta relaciones de la cadena de suministro para cargas de trabajo en la nube. VMware Carbon Black Cloud - Desarrolla y mantiene un inventario detallado de relaciones de la cadena de suministro.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Gestión de riesgos de la cadena de suministro	**STA-08**	Los CSP revisan periódicamente los factores de riesgo asociados a todas las organizacione dentro de su cadena de suministro.	Microsoft Cloud App Security - Analiza riesgos de seguridad de proveedores en la cadena de suministro. Cisco Cloudlock - Evalúa y gestiona riesgos de seguridad de organizaciones en la cadena de suministro.	AWS Security Hub - Revisa periódicamente riesgos de seguridad de organizaciones en la cadena de suministro en AWS. Google Cloud Security Command Center - Evalúa riesgos de seguridad de proveedores en la cadena de suministro en Google Cloud.	CrowdStrike Falcon - Gestiona riesgos de seguridad de organizaciones en la cadena de suministro para cargas de trabajo en la nube. Symantec Cloud Workload Protection - Analiza y mitiga riesgos de seguridad de organizaciones en la cadena de suministro.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Servicio Primario y Acuerdo Contractual	**STA-09**	Los acuerdos de servicio entre los CSP y los CSC (inquilinos) deben incorporar al menos las siguientes disposiciones y/o términos mutuamente acordados: • Alcance, características y ubicación de la relación comercial y de los servicios ofrecidos • Requisitos de seguridad de la información (incluido SSRM) • Proceso de gestión del cambio • Capacidad de registro y monitoreo • Gestión de incidencias y procedimientos de comunicación • Derecho a auditoría y evaluación de terceros • Terminación del servicio • Requisitos de interoperabilidad y portabilidad • Privacidad de datos	McAfee MVISION Cloud - Negocia acuerdos de servicio con requisitos de seguridad y privacidad. Cisco Cloudlock - Implementa requisitos de seguridad de la información y SSRM en acuerdos de servicio.	Trend Micro Cloud One - Monitorea el cumplimiento de requisitos de seguridad en acuerdos de servicio. DivvyCloud by Rapid7 - Evalúa requisitos de seguridad y privacidad en acuerdos de servicio para garantizar la conformidad.	CrowdStrike Falcon - Gestiona requisitos de seguridad y privacidad en acuerdos de servicio para proteger cargas de trabajo en la nube. Symantec Cloud Workload Protection - Revisa y negocia acuerdos de servicio con disposiciones de seguridad adecuadas.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Revisión del Acuerdo de la Cadena de Suministro	**STA-10**	Revisar los acuerdos de la cadena de suministro entre los CSP y los CSC al menos una vez al año.	Netskope Security Cloud - Monitorea y audita los acuerdos de la cadena de suministro para identificar brechas de seguridad. Microsoft Cloud App Security - Revisa y valida los acuerdos de la cadena de suministro para	AWS Security Hub - Revisa periódicamente los acuerdos de la cadena de suministro en AWS para identificar riesgos. Google Cloud Security Command Center - Evalúa los acuerdos de la cadena de suministro en Google	CrowdStrike Falcon - Revisa y evalúa los acuerdos de la cadena de suministro para proteger cargas de trabajo en la nube. Symantec Cloud Workload Protection - Ayuda en la revisión y evaluación

				garantizar la conformidad.	Cloud para asegurar la seguridad.	continua de los acuerdos de la cadena de suministro.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Pruebas de cumplimiento interno	**STA-11**	Definir e implementar un proceso para la realización de evaluaciones internas para confirmar la conformidad y eficacia de las normas, políticas, procedimientos, y las actividades de los acuerdos de nivel de servicio al menos una vez al año.	McAfee MVISION Cloud - Evalúa la conformidad interna y la eficacia de los acuerdos de nivel de servicio. Cisco Cloudlock - Implementa procesos para evaluar internamente la conformidad y eficacia de los acuerdos de servicio.	Trend Micro Cloud One - Realiza evaluaciones internas de conformidad con políticas y procedimientos. DivvyCloud by Rapid7 - Ayuda en la implementación de procesos para evaluar internamente el cumplimiento.	CrowdStrike Falcon - Realiza evaluaciones internas de conformidad y eficacia de los acuerdos de nivel de servicio. Symantec Cloud Workload Protection - Define procesos para evaluar internamente el cumplimiento de los acuerdos de servicio.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Cumplimiento del Acuerdo de Servicio de la Cadena de Suministro	**STA-12**	Implementar políticas que exijan a todos los CSP a lo largo de la cadena de suministro para cumplir con la seguridad de la información, la confidencialidad, el control de acceso, la privacidad, auditoría, política de personal y requisitos y normas de nivel de servicio.	Netskope Security Cloud - Monitorea y asegura el cumplimiento de políticas de seguridad e privacidad. Microsoft Cloud App Security - Implementa políticas para control de acceso y auditoría en la cadena de suministro.	AWS Security Hub - Establece políticas de seguridad y cumplimiento en la cadena de suministro en AWS. Google Cloud Security Command Center - Garantiza el cumplimiento de políticas de seguridad y privacidad en Google Cloud.	CrowdStrike Falcon - Implementa políticas de seguridad y cumplimiento en cargas de trabajo en la nube a lo largo de la cadena de suministro. Symantec Cloud Workload Protection - Asegura políticas de seguridad de la información y control de acceso en cargas de trabajo en la nube.
Gestión de la cadena de suministro, transparencia y rendición de cuentas	Revisión de la gobernanza de la cadena de suministro	**STA-13**	Revisar periódicamente la TI de los socios de la cadena de suministro de la organización políticas y procedimientos de gobernanza	McAfee MVISION Cloud - Evalúa y audita políticas de gobernanza de TI de socios de la cadena de suministro. Cisco Cloudlock - Revisa y garantiza el cumplimiento de políticas de gobernanza de TI de socios.	Trend Micro Cloud One - Revisa periódicamente políticas de gobernanza de TI de socios. DivvyCloud by Rapid7 - Evalúa y mejora la gobernanza de TI de socios de la cadena de suministro.	CrowdStrike Falcon - Audita políticas de gobernanza de TI de socios para cargas de trabajo en la nube. Symantec Cloud Workload Protection - Mejora la gobernanza de TI de socios para un entorno seguro.

Gestión de la cadena de suministro, transparencia y rendición de cuentas	Evaluación de la seguridad de los datos de la cadena de suministro	**STA-14**	Definir e implementar un proceso para realizar evaluaciones de seguridad periódicamente para todas las organizaciones dentro de la cadena de suministro.	Netskope Security Cloud - Evalúa la seguridad de los datos de organizaciones en la cadena de suministro. Microsoft Cloud App Security - Implementa procesos para evaluar periódicamente la seguridad de datos en la cadena de suministro.	AWS Security Hub - Realiza evaluaciones periódicas de seguridad para organizaciones en la cadena de suministro en AWS. Google Cloud Security Command Center - Evalúa la seguridad de datos de organizaciones en la cadena de suministro en Google Cloud.	CrowdStrike Falcon - Evalúa la seguridad de los datos para cargas de trabajo en la nube en la cadena de suministro. Symantec Cloud Workload Protection - Realiza evaluaciones periódicas de seguridad de datos en la cadena de suministro.
Threat & Vulnerability Management - TVM						
Gestión de amenazas y vulnerabilidades	Política y procedimientos de gestión de amenazas y vulnerabilidades	**TVM-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener políticas y procedimientos para identificar, informar y priorizar la remediación de vulnerabilidades, con el fin de proteger los sistemas contra la explotación de vulnerabilidades. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	Netskope Security Cloud - Identifica y prioriza la remediación de vulnerabilidades en aplicaciones en la nube. Microsoft Cloud App Security - Detecta y mitiga vulnerabilidades en servicios en la nube, aplicando políticas de seguridad.	AWS Security Hub - Identifica y prioriza la remediación de vulnerabilidades en entornos de AWS, aplicando políticas de seguridad. Google Cloud Security Command Center - Gestiona vulnerabilidades en Google Cloud, aplicando procedimientos de remediación.	CrowdStrike Falcon - Identifica y remedia amenazas en cargas de trabajo en la nube, aplicando políticas de seguridad. Symantec Cloud Workload Protection - Detecta y remedia vulnerabilidades en cargas de trabajo en la nube, garantizando protección continua.
Gestión de amenazas y vulnerabilidades	Política y procedimientos de protección contra malware	**TVM-02**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Políticas y procedimientos para protegerse contra el malware en los activos administrados. Revisión y actualizar las políticas y procedimientos al menos una vez al año.	McAfee MVISION Cloud - Protege activos en la nube contra malware con políticas de seguridad. Cisco Cloudlock - Prevención y detección de malware en entornos en la nube.	Trend Micro Cloud One - Protege contra malware en entornos de nube pública. DivvyCloud by Rapid7 - Prevención y respuesta ante malware en la infraestructura en la nube.	CrowdStrike Falcon - Protección proactiva contra malware en cargas de trabajo en la nube. Symantec Cloud Workload Protection - Defensa contra malware en cargas de trabajo en la nube.
Gestión de amenazas y vulnerabilidades	Programa de corrección de vulnerabilidades	**TVM-03**	Definir, implementar y evaluar procesos, procedimientos y medidas que permitan dar respuestas programadas y de emergencia a la identificación de vulnerabilidades, en función del riesgo identificado	McAfee MVISION Cloud - Identifica y corrige vulnerabilidades en la nube con respuestas programadas y de emergencia. Microsoft Cloud App Security - Gestiona vulnerabilidades en aplicaciones en la nube con correcciones basadas en el riesgo.	AWS Security Hub - Remedia vulnerabilidades en entornos de AWS con acciones de corrección según la criticidad. Google Cloud Security Command Center - Prioriza y aplica correcciones de seguridad en Google Cloud.	CrowdStrike Falcon - Responde a vulnerabilidades en cargas de trabajo con correcciones programadas y de emergencia. Symantec Cloud Workload Protection - Identifica y mitiga vulnerabilidades en cargas de trabajo en la nube.

Gestión de amenazas y vulnerabilidades	Actualizaciones de detección	**TVM-04**	Definir, implementar y evaluar procesos, procedimientos y Medidas para actualizar las herramientas de detección, las firmas de amenazas y los indicadores de compromiso semanalmente, o con mayor frecuencia.	McAfee MVISION Cloud - Actualiza regularmente las herramientas de detección y firmas de amenazas para proteger entornos de nube. Microsoft Cloud App Security - Proporciona actualizaciones frecuentes de detección de amenazas para aplicaciones en la nube.	Trend Micro Cloud One - Actualiza herramientas de detección y firmas de amenazas semanalmente para proteger entornos de nube pública. DivvyCloud by Rapid7 - Implementa actualizaciones regulares de indicadores de compromiso para mejorar la detección y respuesta a amenazas en la nube.	CrowdStrike Falcon - Realiza actualizaciones periódicas de herramientas de detección para proteger cargas de trabajo en la nube contra ataques. Symantec Cloud Workload Protection - Proporciona actualizaciones frecuentes de detección para garantizar protección continua contra amenazas en la nube.
Gestión de amenazas y vulnerabilidades	Vulnerabilidades de bibliotecas externas	**TVM-05**	Definir, implementar y evaluar procesos, procedimientos y medidas para identificar las actualizaciones de las aplicaciones que utilizan bibliotecas de origen de acuerdo con la política de administración de vulnerabilidades de la organización.	Netskope Security Cloud: Identifica y actualiza aplicaciones en la nube con bibliotecas externas. Microsoft Cloud App Security: Supervisa y aplica actualizaciones para aplicaciones en la nube con vulnerabilidades.	Trend Micro Cloud One: Escanea y gestiona actualizaciones para aplicaciones en la nube con bibliotecas externas. DivvyCloud by Rapid7: Proporciona visibilidad y facilita actualizaciones de seguridad en la nube.	CrowdStrike Falcon: Detecta y gestiona actualizaciones de seguridad para aplicaciones en la nube con bibliotecas externas. Symantec Cloud Workload Protection: Supervisa y protege cargas de trabajo en la nube, remediando vulnerabilidades en bibliotecas externas.
Gestión de amenazas y vulnerabilidades	Pruebas de penetración	**TVM-06**	Definir, implementar y evaluar procesos, procedimientos y medidas para la realización periódica de pruebas de penetración por parte de Terceros.	Netskope Security Cloud: Detecta actividades anómalas que podrían indicar una penetración. Microsoft Cloud App Security: Ofrece detección avanzada de amenazas para identificar actividades maliciosas.	Trend Micro Cloud One: Escanea la infraestructura en busca de vulnerabilidades que podrían ser explotadas en una penetración. DivvyCloud by Rapid7: Proporciona visibilidad sobre la infraestructura en la nube para identificar áreas vulnerables.	CrowdStrike Falcon: Detecta actividades maliciosas en las cargas de trabajo en la nube que podrían ser indicativas de una penetración. Symantec Cloud Workload Protection: Ofrece protección adicional para las cargas de trabajo en la nube para prevenir o mitigar los efectos de una penetración.
Gestión de amenazas y vulnerabilidades	Identificación de vulnerabilidades	**TVM-07**	Definir, implementar y evaluar procesos, procedimientos y Medidas para la detección de vulnerabilidades en los activos gestionados por la organización al menos una vez al mes.	McAfee MVISION Cloud: Realiza escaneos de vulnerabilidades en aplicaciones en la nube. Microsoft Cloud App Security: Detecta y evalúa vulnerabilidades en servicios de Microsoft en la nube.	enable.io: Escanea la infraestructura en la nube en busca de vulnerabilidades. Prisma Cloud by Palo Alto Networks: Realiza escaneos continuos de configuraciones y tráfico en la nube.	Qualys Cloud Platform: Escanea y evalúa vulnerabilidades en cargas de trabajo en la nube. Check Point CloudGuard: Realiza escaneos automatizados de vulnerabilidades en cargas de trabajo en la nube.

Gestión de amenazas y vulnerabilidades	Priorización de vulnerabilidades	**TVM-08**	Utilizar un modelo basado en el riesgo para priorizar eficazmente la vulnerabilidad corrección utilizando un marco reconocido por la industria.	McAfee MVISION Cloud: Prioriza vulnerabilidades en aplicaciones en la nube. Netskope Security Cloud: Utiliza modelos de riesgo reconocidos para priorizar correcciones.	Tenable.io: Prioriza vulnerabilidades en la infraestructura en la nube. Prisma Cloud by Palo Alto Networks: Utiliza marcos de la industria para la priorización de correcciones.	Qualys Cloud Platform: Prioriza vulnerabilidades en cargas de trabajo en la nube. CrowdStrike Falcon: Utiliza modelos de riesgo avanzados para priorizar acciones de remediación.
Gestión de amenazas y vulnerabilidades	Informes de gestión de vulnerabilidades	**TVM-09**	Definir e implementar un proceso para el seguimiento y la notificación de vulnerabilidades actividades de identificación y remediación que incluyen la notificación a las partes interesadas.	Bitglass: Proporciona informes detallados sobre actividades de identificación y remediación de vulnerabilidades en la nube. Cisco Cloudlock: Ofrece seguimiento y notificación de vulnerabilidades en entornos en la nube.	DivvyCloud by Rapid7: Permite el seguimiento y la notificación de vulnerabilidades en la infraestructura en la nube. Datadog Security Monitoring: Proporciona informes detallados sobre la gestión de vulnerabilidades en la nube.	Palo Alto Networks Prisma Cloud Compute: Define procesos para el seguimiento y notificación de vulnerabilidades en cargas de trabajo en la nube. Sysdig Secure: Ofrece informes sobre la gestión de vulnerabilidades en entornos de contenedores y cargas de trabajo en la nube.
Gestión de amenazas y vulnerabilidades	Métricas de gestión de vulnerabilidades	**TVM-10**	Establecer, monitorear e informar métricas para la identificación y remediación de vulnerabilidades en intervalos definidos.	Netskope Security Cloud: Proporciona métricas detalladas sobre vulnerabilidades en aplicaciones en la nube. McAfee MVISION Cloud: Ofrece métricas para seguimiento y mejora continua.	Tenable.io: Establece y supervisa métricas de vulnerabilidades en la infraestructura en la nube. Prisma Cloud by Palo Alto Networks: Ofrece métricas detalladas para toma de decisiones informadas.	Qualys Cloud Platform: Proporciona métricas para identificación y corrección de vulnerabilidades en cargas de trabajo en la nube. CrowdStrike Falcon: Ofrece métricas y análisis para evaluar la eficacia de la gestión de vulnerabilidades.
Universal Endpoint Management - UEM						
Gestión universal de endpoints	Directivas y procedimientos de dispositivos de punto final	**UEM-01**	Establecer, documentar, aprobar, comunicar, aplicar, evaluar y mantener Directivas y procedimientos para todos los puntos de conexión. Revisar y actualizar las políticas y procedimientos al menos una vez al año.	McAfee MVISION Cloud: Aplica políticas de seguridad en la nube. Microsoft Cloud App Security: Evalúa y controla aplicaciones en la nube.	Palo Alto Networks Prisma Cloud: Gestiona y fortalece directivas de seguridad. Check Point CloudGuard: Mantiene y evalúa políticas de seguridad en la nube.	No Aplica
Gestión universal de endpoints	Aprobación de aplicaciones y servicios	**UEM-02**	Definir, documentar, aplicar y evaluar una lista de servicios aprobados, Aplicaciones y orígenes de aplicaciones (almacenes) aceptables para su uso por parte de los puntos de conexión al acceder o almacenar datos administrados por la organización.	Netskope Security Cloud: Controla el uso de aplicaciones y servicios en la nube. Symantec CloudSOC CASB: Gestiona la seguridad de aplicaciones en la nube.	Secureworks Cloud Configuration Review: Evalúa configuraciones de servicios en la nube. Sophos Cloud Optix: Asegura la conformidad de aplicaciones y servicios en la nube.	No Aplica

Gestión universal de endpoints	Compatibilidad	**UEM-03**	Definir e implementar un proceso para la validación del endpoint compatibilidad del dispositivo con sistemas operativos y aplicaciones.	Cisco Cloudlock: Asegura la compatibilidad de aplicaciones en la nube. Forcepoint CASB: Valida la compatibilidad de aplicaciones.	Trend Micro Cloud One – Conformity: Verifica la conformidad de configuraciones de cloud. IBM Cloud Security and Compliance Center: Gestiona la conformidad de infraestructuras de cloud.	VMware Carbon Black Cloud: Controla la seguridad de endpoints y su compatibilidad. CrowdStrike Falcon: Protege dispositivos verificando compatibilidad con sistemas.
Gestión universal de endpoints	Inventario de puntos de conexión	**UEM-04**	Mantener un inventario de todos los puntos finales utilizados para almacenar y acceder a la empresa datos.	Bitglass: Visibilidad y control de dispositivos que acceden a datos en la nube. Microsoft Cloud App Security: Catalogación de dispositivos en entornos de nube.	Fugue: Detección automática de recursos en la nube. Dome9 Security (part of Check Point): Gestión de inventario de activos en la nube.	No Aplica
Gestión universal de endpoints	Gestión de endpoints	**UEM-05**	Definir, implementar y evaluar procesos, procedimientos y medidas para hacer cumplir las políticas y los controles para todos los puntos finales a los que se permite el acceso y/o almacenar, transmitir o procesar datos de la organización.	Symantec CloudSOC CASB: Controla accesos y actividades de endpoints Netskope Security Cloud: Gestiona interacciones de endpoints con servicios en la nube.	Trend Micro Cloud One – Conformity: Evalúa la conformidad de configuraciones de seguridad en endpoints. Qualys Cloud Platform: Proporciona gestión de seguridad para endpoints en la nube.	McAfee MVISION Cloud: Aplica políticas en cargas de trabajo en la nube. CrowdStrike Falcon: Protege endpoints con vigilancia en tiempo real.
Gestión universal de endpoints	Pantalla de bloqueo automático	**UEM-06**	Configure todos los puntos de conexión de uso interactivo relevantes para requerir un Pantalla de bloqueo	Microsoft Cloud App Security: Configura políticas de seguridad en dispositivos, incluidas pantallas de bloqueo.	No Aplica	VMware Carbon Black Cloud: Gestiona políticas de seguridad en endpoints, incluidas pantallas de bloqueo. CrowdStrike Falcon: Implementa políticas como incluir pantallas de bloqueo.
Gestión universal de endpoints	Sistemas Operativos	**UEM-07**	Gestionar los cambios en los sistemas operativos de los terminales, los niveles de parches y/o a través de los procesos de gestión del cambio de la empresa.	No Aplica	Qualys Cloud Platform: Automatiza la gestión de parches de sistemas operativos. Tenable.io: Monitorea y gestiona vulnerabilidades de sistemas operativos.	Trend Micro Deep Security: Administra parches y configuraciones de sistemas operativos. Symantec Endpoint Protection: Controla actualizaciones y parches en endpoints.
Gestión universal de endpoints	Cifrado de almacenamiento	**UEM-08**	Proteja la información de la divulgación no autorizada en el endpoint administrado dispositivos con cifrado de almacenamiento.	McAfee MVISION Cloud: Proporciona cifrado para datos en dispositivos de endpoint. Microsoft Cloud App Security: Aplica políticas de cifrado en datos en la nube y dispositivos.	No Aplica	Symantec Endpoint Protection: Ofrece cifrado para proteger datos en dispositivos. VMware Carbon Black Cloud: Implementa cifrado en endpoints gestionados.

Gestión universal de endpoints	Detección y prevención antimalware	**UEM-09**	Configuración de puntos de conexión administrados con detección y prevención antimalware tecnología y servicios.	No Aplica	No Aplica	Symantec Endpoint Protection: Solución antimalware robusta para endpoints. Trend Micro Deep Security: Protección antimalware para endpoints y servidores.
Gestión universal de endpoints	Cortafuegos de software	**UEM-10**	Configure los puntos de conexión administrados con firewalls de software configurados correctamente.	No Aplica	No Aplica	Symantec Endpoint Protection: Gestiona cortafuegos en endpoints. McAfee Endpoint Security: Proporciona firewall robusto para endpoints.
Gestión universal de endpoints	Prevención de pérdida de datos	**UEM-11**	Configuración de puntos de conexión administrados con tecnologías de prevención de pérdida de datos (DLP) y normas de conformidad con una evaluación de riesgos.	McAfee MVISION Cloud: DLP para proteger datos en la nube y endpoints. Microsoft Cloud App Security: Implementa políticas DLP en la nube.	No Aplica	Symantec Endpoint Protection: Integra DLP en endpoints. Digital Guardian: Plataforma de DLP para protección de datos en endpoints.
Gestión universal de endpoints	Localización remota	**UEM-12**	Habilite las capacidades de geolocalización remota para todos los puntos de conexión móviles administrados.	Microsoft Cloud App Security: Monitorea ubicaciones de dispositivos en acceso a la nube.	No Aplica	VMware Carbon Black Cloud: Proporciona visibilidad limitada de la ubicación de dispositivos.
Gestión universal de endpoints	Borrado remoto	**UEM-13**	Definir, implementar y evaluar procesos, procedimientos y Medidas para permitir la eliminación de datos de la empresa de forma remota en el punto final administrado Dispositivos.	Microsoft Cloud App Security: Implementa políticas de borrado remoto en dispositivos. McAfee MVISION Cloud: Controla la eliminación remota de datos en dispositivos de nube.	No Aplica	VMware Carbon Black Cloud: Gestiona borrado remoto de datos en endpoints. Symantec Endpoint Protection: Permite el borrado remoto de datos en dispositivos gestionados.
Gestión universal de endpoints	Postura de seguridad de endpoints de terceros	**UEM-14**	Definir, implementar y evaluar procesos, procedimientos y y/o medidas contractuales para mantener la seguridad adecuada de los puntos finales de terceros con acceso a los activos de la organización.	McAfee MVISION Cloud: Monitorea el acceso de dispositivos de terceros. Netskope Security Cloud: Controla el tráfico de datos entre dispositivos de terceros y la nube.	Cisco Secure Workload: Identifica y corrige configuraciones inseguras. Palo Alto Networks Prisma Cloud: Gestiona la seguridad de endpoints de terceros en la nube.	Trend Micro Deep Security: Protege endpoints de terceros en tiempo real. Symantec Endpoint Protection Cloud: Asegura endpoints de terceros con políticas personalizadas.

Como guía práctica, se ha desarrollado una estrategia para mejorar la postura de seguridad y cumplimiento en entornos cloud multicloud, comenzando con la configuración de herramientas propias de los CSP y los grupos de controles que gestionan. Posteriormente, identificando las herramientas que complementarían a las del CSP, las cuales son esenciales para reforzar la seguridad y el cumplimiento. Finalizando con la descripción de herramientas complementarias, evaluando su importancia y necesidad para cumplir con controles específicos de la Cloud Control Matrix. Esta guía ofrece un enfoque estructurado y detallado para fortalecer la seguridad en entornos multicloud.

1. Herramientas propias del CSP que hay que configurar y qué grupos de controles ayudan a gestionar:

AWS:

- AWS Identity and Access Management (IAM) para gestionar accesos seguros (gestiona controles de IAM).
- AWS Config para realizar el seguimiento de la configuración de los recursos y evaluar contra las políticas deseadas (apoya CSPM).
- AWS Shield para protección contra DDoS (contribuye a controles de protección de la red).

Azure:

- Azure Active Directory para el manejo de identidades y accesos (gestiona controles de IAM).
- Azure Policy para asegurar y monitorizar la postura de cumplimiento de Azure (apoya CSPM).
- Azure Security Center que ofrece funciones avanzadas de protección contra amenazas para cargas de trabajo de máquinas virtuales y otros recursos (funciones de CWPP).

Google Cloud Platform (GCP):

- Google Cloud Identity & Access Management para el control de accesos (gestiona controles de IAM).
- Google Cloud Security Command Center para visibilidad y control sobre la postura de seguridad de Google Cloud (apoya CSPM).
- Google Cloud Armor para la protección contra ataques web y DDoS (contribuye a controles de protección de la red).

2. Herramientas que implementarías para complementar a las del CSP:

CASB:

- McAfee MVISION Cloud: Proporciona visibilidad y control sobre los datos en cualquier nube y protege contra amenazas (útil en AWS, Azure y GCP).
- Microsoft Cloud App Security: Visibilidad de aplicaciones en la nube y control sobre datos con políticas de seguridad en tiempo real (funciona bien con múltiples nubes).

CSPM:

- Palo Alto Networks Prisma Cloud: Ofrece visibilidad completa del entorno de nube y capacidades de cumplimiento continuo (compatible

con AWS, Azure y GCP).
- Tenable.io: Plataforma de visualización y gestión de vulnerabilidades para la nube (útil en entornos multicloud).

CWPP:
- Trend Micro Deep Security: Soluciones de seguridad optimizadas para la nube que protegen cargas de trabajo y aplicaciones (funciona con AWS, Azure y GCP).
- Symantec Cloud Workload Protection: Automatiza la seguridad para cargas de trabajo públicas y privadas (adaptable a diversas plataformas de nube).

3. Herramientas complementarias y su importancia:

Estas herramientas son imprescindibles para cumplir con ciertos controles que las herramientas del CSP no cubren completamente, especialmente en áreas como la protección de datos, cumplimiento normativo más específico, y gestión de amenazas avanzadas.

- Varonis DatAdvantage Cloud: Especialmente útil para DLP (Prevención de Pérdida de Datos) y para cumplir con regulaciones como GDPR y CCPA al proteger y monitorear datos críticos.
- CrowdStrike Falcon: Proporciona detección de amenazas en tiempo real y protección antimalware que puede ser crucial, especialmente en entornos con alto riesgo de ataques cibernéticos.

4. Conclusiones y trabajos futuros

Conclusiones del Trabajo

Los resultados obtenidos de la implementación de herramientas CASB, CSPM y CWPP alineadas con la Cloud Control Matrix para AWS, Azure y GCP, han validado la efectividad de la metodología propuesta. Las herramientas se han demostrado eficaces en mejorar la seguridad y el cumplimiento en los entornos cloud evaluados. Sin embargo, también revelaron desafíos inesperados como las complejidades adicionales en la gestión de múltiples nubes, resaltando la necesidad de adaptación continua y evaluación de nuevas soluciones emergentes en seguridad cloud.

- El proyecto aprovechó la Cloud Control Matrix para asignar herramientas de los grupos CASB, CSPM y CWPP a controles específicos, optimizando la seguridad y cumplimiento en AWS, Azure y GCP. Esta estrategia evitó desarrollar un nuevo checklist, concentrando esfuerzos en la evaluación de herramientas efectivas para la gestión de riesgos y protección de datos.
- De los tres grupos de herramientas evaluados, las CWPP (Cloud Workload Protection Platform) fueron las más difíciles de adaptar debido a su necesidad de integración profunda y técnica con las cargas de trabajo específicas de cada entorno de nube. Estas herramientas requieren configuraciones precisas para manejar políticas de acceso, auditorías, procesos de continuidad del negocio y gestión del ciclo de vida de la información, lo que complica su adaptación y asegura que no comprometan la funcionalidad o el rendimiento del sistema.

- Las diferencias en configuraciones de seguridad y APIs entre distintas plataformas de nube resaltaron la necesidad de estrategias de integración flexibles y adaptables. Este desafío enfatiza la importancia de una gestión de seguridad coherente y eficaz a través de múltiples proveedores.
- La revisión detallada de las capacidades de las herramientas seleccionadas reveló que la combinación de CASB, CSPM y CWPP proporciona una defensa en profundidad. Este enfoque mejora la protección general contra amenazas emergentes y evolucionadas en entornos multicloud, fortaleciendo así la eficiencia operativa y la seguridad general de las organizaciones.

Reflexión Crítica sobre la Consecución de los Objetivos
El análisis ha confirmado que la mayoría de los objetivos iniciales se han alcanzado satisfactoriamente, lo que incluye el desarrollo de un marco de trabajo efectivo para vincular herramientas específicas a los controles de la CCM. No obstante, algunos objetivos, como la integración profunda de consideraciones de diversidad y sostenibilidad, no se exploraron tan exhaustivamente como se planificó debido a la flexibilidad que se requiere.

Análisis Crítico del Seguimiento de la Planificación y Metodología
La metodología fue en gran parte seguida según lo planificado, pero se realizaron ajustes para adaptar el enfoque a los desafíos encontrados, especialmente relacionados con las diferencias entre las plataformas de servicios en la nube. Estos ajustes fueron cruciales para asegurar la relevancia y la aplicabilidad de las soluciones de seguridad en entornos multicloud dinámicos y diversamente configurados.

Impactos Evaluados
Se tomaron en cuenta los impactos ético-sociales, de sostenibilidad y de diversidad desde la concepción del proyecto. Las estrategias implementadas han mitigado efectivamente los posibles impactos negativos y han amplificado los positivos, como el aumento en la conciencia sobre la seguridad en la nube y el compromiso con la adopción de tecnologías responsables. Sin embargo, se identificaron impactos adicionales no previstos, como el interés incrementado en normativas de protección de datos personales, que también fueron abordados mediante ajustes en las estrategias de implementación y divulgación.

Trabajo Futuro
La investigación ha puesto de relieve áreas adicionales que requieren exploración futura, incluyendo la adaptación del marco a plataformas de nube emergentes y la evaluación de la efectividad de las herramientas de seguridad a través de simulaciones de ataques más rigurosas. Estas áreas no solo extenderían la aplicabilidad del marco actual, sino que también profundizarían el entendimiento de las dinámicas de seguridad en configuraciones de nube complejas y cambiantes.

Esta versión expandida abarca de manera completa las conclusiones y reflexiones sobre el trabajo realizado, al tiempo que destaca áreas para futuras investigaciones y mejoras.

5. Glosario

- AWS (Amazon Web Services): Plataforma de servicios en la nube que facilita soluciones de computación, almacenamiento y otros servicios.
- Azure: Plataforma de cloud computing de Microsoft que ofrece soluciones de computación, redes, y almacenamiento.
- CASB (Cloud Access Security Broker): Intermediarios que proporcionan seguridad entre los usuarios y los servicios en la nube.
- CCM (Cloud Control Matrix): Marco de referencia para controles de seguridad en la nube.
- CSP (Cloud Service Provider): Proveedor de recursos de red, aplicaciones o almacenamiento en la nube.
- CSPM (Cloud Security Posture Management): Herramientas para identificar y gestionar riesgos de seguridad en la nube.
- CWPP (Cloud Workload Protection Platform): Soluciones para proteger cargas de trabajo en entornos de nube.
- GCP (Google Cloud Platform): Servicios de computación en la nube ofrecidos por Google.
- Multicloud: Uso de servicios de múltiples proveedores de nube en un entorno.
- Seguridad en la nube: Protección de datos y sistemas en entornos de nube mediante políticas y tecnologías.
- Sostenibilidad: Prácticas que minimizan el impacto ambiental de las operaciones tecnológicas.
- API (Application Programming Interface): Conjunto de rutinas y protocolos que permite la integración y funcionamiento de software independiente.
- DLP (Data Loss Prevention): Estrategias para detectar y prevenir la pérdida de datos críticos.
- IAM (Identity and Access Management): Procesos y tecnologías para gestionar y controlar accesos a recursos de la red.
- Vulnerabilidad: Debilidad en un sistema que puede ser explotada para comprometer la seguridad del sistema.
- Endpoint: Dispositivo final de usuario que se conecta a la red, como PCs, laptops y móviles.

Referencias

[1] MINTIC, «Seguridad y privacidad de la información,» 14 marzo 2016. [En línea]. Available: https://gobiernodigital.mintic.gov.co/692/articles-5482_G12_Seguridad_Nube.pdf. [Último acceso: 2024].

[2] Google cloud, «Qué es IaaS,» 2024. [En línea]. Available: https://cloud.google.com/learn/what-is-iaas?hl=es. [Último acceso: marzo 2024].

[3] Stackscale, «Modelos de servicios cloud,» 01 febrero 2023. [En línea]. Available: https://www.stackscale.com/es/blog/modelos-de-servicio-cloud/. [Último acceso: 2024].

[4] RedHat, «Servicios de nube gerenciados,» 10 Julio 2023. [En línea]. Available: https://www.redhat.com/es/topics/cloud-computing/what-are-cloud-services. [Último acceso: 2024].

[5] F. Zuluaga, «¿Cuáles son los marcos de referencia para la seguridad de la información (ciberseguridad)?,» Ochoa Consulting Holding, 16 febrero 2023. [En línea]. Available: https://www.ochgroup.co/cuales-son-los-marcos-de-referencia-para-la-seguridad-de-la-informacion-ciberseguridad/. [Último acceso: 2024].

[6] National institute of standards and technology, «NIST,» 2024. [En línea]. Available: https://www.nist.gov/. [Último acceso: Marzo 2024].

[7] «Frameworks de ciberseguridad,» agosto 2021. [En línea]. Available: https://protegermipc.net/2021/08/19/frameworks-de-ciberseguridad-y-estandares-que-debes-conocer/. [Último acceso: 2024].

[8] Kinsta, «Riesgos y mejores prácticas cloud,» 22 noviembre 2022. [En línea]. Available: https://kinsta.com/es/blog/seguridad-nube/. [Último acceso: 2024].

[9] Kaspersky, «¿Qué es la seguridad en la nube?,» 2024. [En línea]. Available: https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security. [Último acceso: 2024].

[10] Uptyccs, «CSA's Pandemic 11: Key Cloud Security Dangers & How to Counteract Them,» 31 agosto 2022. [En línea]. Available: https://www.uptycs.com/blog/the-csas-pandemic-11-top-cloud-security-threats-and-what-to-do-about-them. [Último acceso: 2024].

[11] Cloud Security Alliance, «rincipales amenazas a Cloud Computación de Cloud Security Alliance,» 07 Junio 2022. [En línea]. Available: https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning. [Último acceso: 2024].

[12] Packt, «Dominar la gestión de la postura de seguridad en la nube (CSPM),» enero 2024. [En línea]. Available: https://www.packtpub.com/product/mastering-cloud-security-posture-management-cspm/9781837638406. [Último acceso: 2024].

[13] IONOS Digital Guide, «niveles Tier,» 2024. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/know-how/sistemas-de-evaluacion-para-data-centers/. [Último acceso: 2024].

[14] TechTarget, «Seguridad nativa de nube,» ComputerWeekly, 11 febrero 2021. [En línea]. Available: https://www.computerweekly.com/es/consejo/Cuando-usar-y-cuando-no-herramientas-de-seguridad-nativas-de-nube. [Último acceso: 2024].

[15] Seguridad de microsoft, «Definición de Agente de seguridad de acceso a la nube (CASB),» 2024. [En línea]. Available: https://www.microsoft.com/es-co/security/business/security-101/what-is-a-cloud-access-security-broker-casb. [Último acceso: 2024].

[16] Amazon Web Services, «AWS marketplace,» 2024. [En línea]. Available: https://aws.amazon.com/marketplace/solutions/security. [Último acceso: mayo 2024].

[17] Amazon web services, «AWS security HUB,» 203. [En línea]. Available: https://aws.amazon.com/es/security-hub/. [Último acceso: abril 2024].

[18] Google Cloud, «Seguridad y gestión de riesgos en la nube para entornos multinube,» 2024. [En línea]. Available: https://cloud.google.com/security/products/security-command-center?hl=es. [Último acceso: 2024].