Recursos sin uso en nube AWS: Identificación de recursos sin uso que puedan significar foco de ataque cibernético.

Jovan Alejandro Zambrano Bello

Ingeniería de Sistemas

Asesor(es)

Catalina Maria Cespedes Toro, Especialista en Gerencia de Proyectos

Eliana Maritza Ospina Salazar, Analista

Universidad de Antioquia

Facultad de Ingeniería

Departamento Ingeniería de Sistemas

Medellín

2024

Cita	Zambrano Bello [1]
Referencia Estilo IEEE (2020)	[1] J. A. Zambrano Bello, “Recursos sin uso en nube AWS: Identificación de recursos sin uso que puedan significar foco de ataque cibernético.”, Semestre de Industria, Pregrado, Universidad de Antioquia, Medellín, 2024.

Agradecimiento a Bancolombia S.A y al equipo Security Team por apoyar y permitir la elaboración de este proyecto.

Dedicatoria

A Michael y Bryan, quienes son mi ejemplo de perseverancia y sacrificio. Este logro es también suyo.

A Martín, por ser la luz del alma mía.

A Karen, la vida mía, por acompañarme en los mejores y peores momentos.

A mi Padre, por hacerme entender la importancia de nunca darme por vencido.

A mi Madre y a César, porque cada uno de mis pasos llevan su nombre.

Agradecimientos

A Luis y Eliana, porque su acompañamiento fue más allá de lo profesional.

A la profesora Catalina, por transmitir tranquilidad y sabiduría durante el proceso.

Tabla de contenido

LISTA DE TABLAS

LISTA DE FIGURAS

SIGLAS, ACRÓNIMOS Y ABREVIATURAS

IEEE	Institute of Electrical and Electronics Engineers
UdeA	Universidad de Antioquia
AWS	Amazon Web Services
KMS	Key Management Service
EC2	Elastic Compute Cloud
EBS	Elastic Block Store
ACM	AWS Certificate Manager
RDS	Relational DataBase
ELB	Elastic Load Balancer

RESUMEN

Amazon Web Services (AWS) es la nube más completa y adoptada del mundo, que ofrece más de 200 servicios integrales de centro de datos a nivel mundial. Cuando una organización adquiere dichos servicios de nube, toda la información que se guarde allí en nube debe ser protegida. Muchas de las entidades financieras en la actualidad están manejando la migración de sus aplicaciones y su información a nube y está expuesta a diferentes amenazas que pueden atentar contra su seguridad. En esta nueva visión de las tecnologías en la nube, se hace necesario identificar cómo reducir riesgos de seguridad identificando recursos sin uso en AWS que puedan ser aprovechados por personas mal intencionadas para materializar los riesgos importantes de ciberseguridad.

Palabras clave **— AWS, Ciberseguridad, nube, servicios, recursos, riesgos.**

ABSTRACT

Amazon Web Services (AWS) is the world's most comprehensive and widely adopted cloud, offering more than 200 comprehensive data center services worldwide. When an organization purchases such cloud services, all information stored there in the cloud must be protected. Many financial institutions are currently managing the migration of their applications and information to the cloud and are exposed to different threats that can threaten their security. This new visualization of cloud technologies makes it necessary to identify how to reduce security risks by identifying unused resources in AWS that can be exploited by malicious individuals to materialize significant cybersecurity risks.

Keywords **— AWS, security, cloud technologies, migration to cloud.**

I. INTRODUCCIÓN

Actualmente como lo recomienda la buena práctica, no se tiene una solución integral para identificar recursos en la nube AWS que no están siendo utilizados y que puedan ser aprovechados por los atacantes para explotar cualquier vulnerabilidad. En este proyecto se desarrollará una solución para identificar los recursos que la organización tiene desplegados en la nube de AWS y que no estén siendo usados por un tiempo mínimo de 3 meses (90 días) para la posterior notificación a los equipos dueños de esos recursos para su gestión (borrado o justificación de frecuencia de uso), de esta manera se busca mitigar los riesgos de ciberseguridad asociados a recursos huérfanos.

II. OBJETIVOS

A. Objetivo general

Desarrollar una solución para identificar recursos que la organización tiene desplegados en la nube de AWS y que no estén siendo usados por más de 90 días para mitigar riesgos de ciberseguridad.

B. Objetivos específicos

- Establecer los recursos más prioritarios para análisis.
- Definir una arquitectura para la identificación de los recursos sin uso donde se vea involucrado el servicio de Continous Compliance y la notificación de los hallazgos a los equipos dueños de cada recurso.
- Construir un documento con el prototipo de desarrollo para iniciar servicios en ambiente de pruebas.
- Desarrollar la funcionalidad principal que identifique todos los recursos sin uso por más de 90 días en Continous Compliance.
- Implementar pruebas unitarias a los desarrollos con una aprobación del 80%.
- Desplegar los artefactos funcionales en ambiente de pruebas y producción con su respectiva documentación para la gestión de los recursos.

III. MARCO TEÓRICO

El proyecto en cuestión se basa en tres pilares fundamentales para su desarrollo y ejecución efectiva: la infraestructura de la Nube de Amazon Web Services (AWS), la implementación de buenas prácticas específicas de AWS y el cumplimiento de estándares de seguridad de la Cloud Security Alliance (CSA). Estos elementos proporcionan un marco sólido para la gestión eficiente de recursos, la seguridad y la optimización del rendimiento dentro del entorno de la nube.

- **AWS**

Amazon Web Services (AWS) es la nube más adoptada y completa en el mundo, que ofrece más de 200 servicios integrales de centros de datos a nivel global. Millones de clientes, incluso las empresas emergentes que crecen más rápido, las compañías más grandes y los organismos gubernamentales líderes, están usando AWS para reducir los costos, aumentar su agilidad e innovar de forma más rápida.

AWS cuenta con una cantidad de servicios y de características incluidas en ellos que supera la de cualquier otro proveedor de la nube, ofreciendo desde tecnologías de infraestructura como cómputo, almacenamiento y bases de datos hasta tecnologías emergentes como aprendizaje automático e inteligencia artificial, lagos de datos y análisis e internet de las cosas. Esto hace que llevar las aplicaciones existentes a la nube sea más rápido, fácil y rentable y permite crear casi cualquier cosa que se pueda imaginar.

AWS está diseñado para ser el entorno de informática en la nube más flexible y seguro disponible en la actualidad. Cuenta con el respaldado de un amplio conjunto de herramientas de seguridad en la nube, con más de 300 servicios y funciones de seguridad, conformidad y gobernanza, así como compatibilidad con 143 normas de seguridad y certificaciones de conformidad. [1]

- **Buenas prácticas AWS (AWS Well-Architected Framework)**

AWS Well-Architected ayuda a los arquitectos de la nube a crear una infraestructura segura, de alto rendimiento, resistente y eficiente para una variedad de aplicaciones y cargas de trabajo. Este marco, creado en torno a seis pilares (excelencia operativa, seguridad, fiabilidad, eficiencia de rendimiento, optimización de costos y sostenibilidad), ofrece un enfoque coherente para que los clientes y los socios evalúen las arquitecturas e implementen diseños escalables.

AWS Well-Architected Framework incluye enfoques de dominios específicos, laboratorios prácticos y AWS Well-Architected Tool. AWS Well-Architected Tool, disponible sin costo alguno en la consola de administración de AWS, proporciona un mecanismo para evaluar regularmente las cargas de trabajo, identificar los problemas de alto riesgo y registrar las mejoras.

AWS Well-Architected Framework es un marco de trabajo que describe los conceptos clave, los principios de diseño y las prácticas recomendadas de arquitectura para diseñar y ejecutar cargas de trabajo en la nube. Responde ante un conjunto de preguntas básicas para descubrir hasta qué punto las arquitecturas están en consonancia con las prácticas recomendadas en la nube y así obtener una orientación para mejorarla.

- **CSA(Cloud Security Alliance)**

Es una organización sin ánimo de lucro cuyo objetivo es "promover el uso de prácticas recomendadas para ofrecer garantías de seguridad en el ámbito de la informática en la nube, así como proporcionar información sobre los usos de la informática en la nube a efectos de ayudar a proteger todas las demás formas de la informática". [3]

- **ISO 27001 para seguridad en la Nube**

Las normas ISO 27001 son normas establecidas por la Organización Internacional de Normalización (ISO) que describen de manera correcta la gestión de la seguridad de la información al interior de una empresa. Es una norma de seguridad a nivel global para el manejo de la información. Su eje central es el Sistema de Gestión de la Seguridad de la Información(SGSI) en el cual se establece que todos los empleados han de contribuir al establecimiento de la norma. La norma apunta a que las organizaciones conozcan los riesgos asociados al manejo de información, haciéndolos mínimos y gestionarlos por medio de un

proceso documentado, sistemático, estructurado, eficiente, repetible y adaptable a los eventuales cambios que pudieran presentar los riesgos, el entorno y la tecnología. [4]

- **OWASP**

Es la documentación estándar de concientización para desarrolladores y para la seguridad de aplicaciones. Representa un amplio consenso sobre los riesgos de seguridad más críticos para las aplicaciones. Los 10 riesgos principales de OWASP pueden abordarse con las herramientas y la orientación proporcionadas por AWS, por ejemplo, el pilar de seguridad de Well Architected Framework ayuda a las empresas a crear diseños seguros. [5]

IV. METODOLOGÍA

El equipo de Ciberseguridad se encarga de habilitar y transformar ideas en productos excepcionales para facilitar la implementación de los controles de seguridad sobre las soluciones de los equipos que gestionan tecnologías en la organización para la cual se desarrolla este proyecto. En compañía de este equipo se trabaja continuamente para diseñar, construir y publicar la solución y el producto final de los recursos sin uso que le permita a los usuarios conocer el estado de seguridad de los recursos en la nube y de esta manera conectarse con el objetivo de la organización.

El equipo funciona de manera transversal ofreciendo productos y artefactos a los diferentes equipos que componen el entorno, apoyándose en marcos ágiles como medio de comunicación para afrontar y dar la entrega de valor que requiere la organización, trabajando de forma colaborativa entre todos los miembros del equipo.

Los eventos ágiles que ayudan a mejorar la comunicación entre los miembros se presentan de la siguiente manera:

- Daily de 30 minutos donde se presentan inconvenientes y el plan del día.
- Review quincenal donde se presentan los avances que se han tenido en el sprint.
- Sprint de duración de 15 días donde se trabajan en las diferentes ideas plasmadas en historias de usuario.
- Planning quincenal donde se debaten las diferentes ideas y los objetivos del sprint venidero. Dentro de este espacio se realiza Retrospectiva del equipo para revisar los cambios y las anotaciones importantes del sprint.

La metodología, mejor explicada en la Figura 1, se implementará durante todo el proceso de solución del proyecto de prácticas.

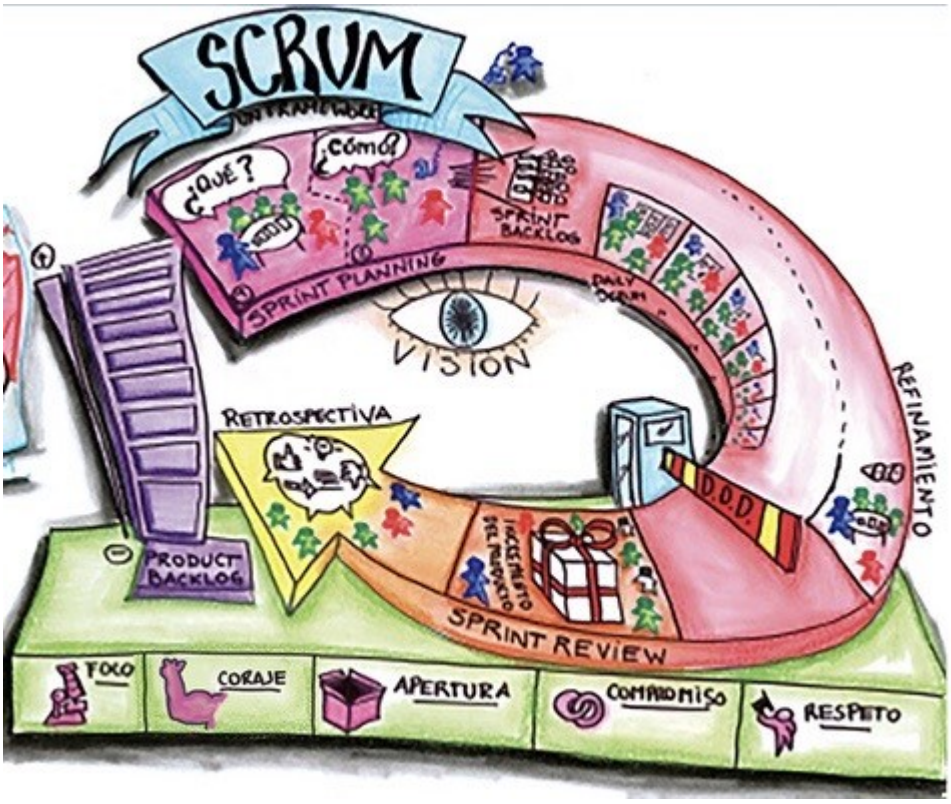

Fig. 1. Imagen alusiva a la metodología Scrum utilizada en el equipo de trabajo

Cronograma de actividades

El cronograma que se detalla a continuación se alinea con el plan de trabajo elaborado en compañía de la asesora externa en el cual se establecen los objetivos mes a mes desde el inicio del proyecto.

Febrero: Contextualización del problema. Elección de los servicios prioritarios que se necesitan en revisión. Etapa de estudio y familiarización. Aspectos técnicos de la nube. Diseño de arquitectura de solución.

Marzo: Documento del diseño de prototipo dónde se describe cómo se tratará la evaluación de cada uno de los servicios.

Abril-Junio: Inicio de implementación de ambiente de pruebas. Análisis y monitoreo para identificar cambios posibles y que las soluciones propuestas se comporten de la manera correcta. Una vez se reporte que las funciones trabajen de manera correcta, hacer despliegue en ambientes de producción.

Junio-Julio: Documentación de la solución. Pruebas unitarias a las funciones con 80% de cobertura.

Fig. 2. Diagrama de Hitos - Cronograma de Actividades

V. RESULTADOS

Durante el desarrollo del proyecto, se dedicó a identificar aquellos recursos en la nube de AWS que no estuvieran en uso. Se investigó el impacto que esto tendría en términos de riesgos en la ciberseguridad y, finalmente, se propuso una solución para optimizar la usabilidad de estos recursos.

En un primer momento, se inició con la contextualización del problema, donde se resolvieron preguntas tales como: ¿A qué se están enfrentando? ¿Con qué propósito se resuelve el proyecto? ¿Qué herramientas se utilizarán para brindar la solución? Aquí se dieron los primeros pasos, apoyándose en los marcos de trabajo de Seguridad y Nube. Se observó que, como recomiendan las buenas prácticas de seguridad a nivel mundial, no se tiene una solución integral para identificar recursos que no tienen uso en la nube y que pueden ser aprovechados por atacantes para explotar vulnerabilidades. A partir de allí, se comenzó la definición de aquellos servicios que son prioritarios para la seguridad. Como se observa en la TABLA I, se definieron diez (10) servicios de diferentes tipos que pueden ser aprovechados por atacantes ya sea por falta de uso o de actualización. A su vez, se definió cuáles son de alta prioridad (que requieren acción inmediata) y media prioridad (que no requieren acción inmediata). También se estableció que el umbral para la evaluación sería de **90 días** (3 meses).

TABLA I
Recursos prioritarios

Recurso	Tipo de Recurso	Prioridad
KMS	Seguridad	Alta
EC2	Cómputo	Alta
Secret Manager	Seguridad	Alta
Bases de Datos RDS	Bases de Datos	Media
Balanceador ELB	Enrutamiento	Media
Distribución CloudFront	Enrutamiento	Alta
Volumen EBS	Almacenamiento	Media
Certificados ACM	Seguridad	Alta
Funciones Lambda	Cómputo	Media
Security Groups	Seguridad	Alta

Nota: Dichos servicios se priorizaron con los dueños de servicio y asesora externa.

En un segundo momento, para asegurar la implementación efectiva y bien estructurada de la solución propuesta, se elaboró un documento de prototipo y una arquitectura detallada. Este documento describe cómo se integran y utilizan todos los servicios de la nube necesarios para el

proyecto, proporcionando una guía clara sobre la configuración y la conexión de los recursos. La arquitectura diseñada garantiza que cada servicio de AWS seleccionado contribuya de manera óptima al soporte y la seguridad de la solución, facilitando así su desarrollo y despliegue. Con las estructuras definidas, se inició el proceso de despliegue de los recursos necesarios.

En un tercer momento, se enfocó en desarrollar y establecer las conexiones entre los diversos servicios en la nube según la arquitectura previamente diseñada. Se buscó que dicha implementación fuera automática, utilizando funciones Lambda personalizadas que centralizan la información recibida de los servicios anteriormente priorizados y la envían a los servicios desplegados mencionados en la arquitectura. Estas funciones están programadas en lenguaje Python, ya que el equipo de trabajo estableció este lenguaje de programación como el preferido.

Uno de los servicios más utilizados, además de las funciones Lambda, fueron las reglas AWS Config personalizadas, encargadas de recibir la información de los recursos que no estaban en uso y enviar automáticamente estos hallazgos a Security Hub tal como se muestra en la Figura 3. Security Hub es un servicio de seguridad de la nube de AWS que se encarga de almacenar y facilitar la gestión de los cumplimientos de las reglas o políticas establecidas en la nube, permitiendo observar todos los hallazgos de los servicios que no están en uso.

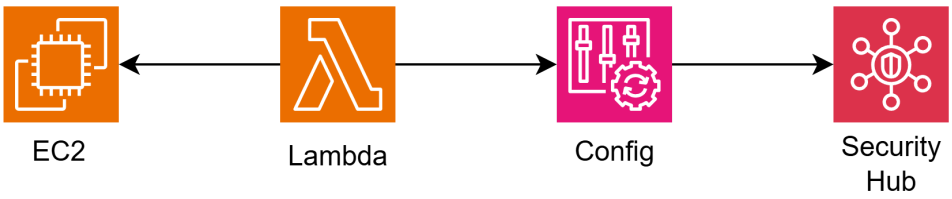

Fig. 3. Mínima unidad de la Arquitectura Final.

Se realizaron pruebas unitarias al código para validar la funcionalidad y la seguridad de la solución, asegurándose de que todos los componentes funcionan correctamente bajo diferentes escenarios de uso. Además, se llevó a cabo una recolección sistemática de resultados utilizando

herramientas de monitoreo y logging de AWS, lo que permitió evaluar el rendimiento y detectar posibles áreas de mejora.

En la fase final del proyecto, se realizó un análisis de los hallazgos obtenidos almacenados en Security Hub, lo cual proporcionó una visión clara del impacto y la efectividad de la solución implementada. Se recopilaron los datos que reflejan la cantidad de recursos en la nube que fueron identificados como sin uso. Cada dato se almacenó en una tabla de Excel y se graficaron para cada servicio tal como se muestra en la figura 3.

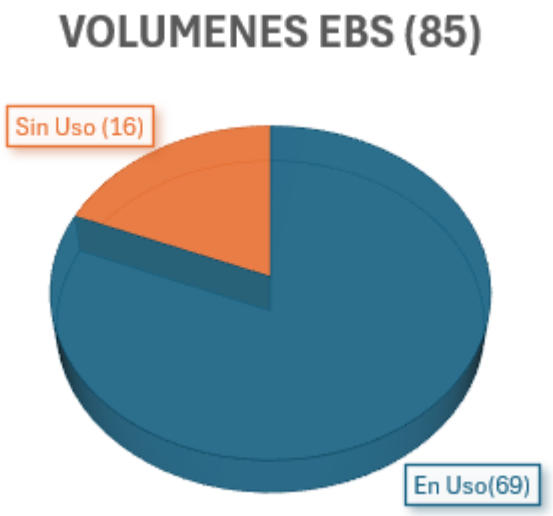

Fig. 4. Métricas obtenidas para Volúmenes EBS.

Nota. Solo se muestra para un servicio debido a que, por confidencialidad, no se pueden compartir los demás.

Así, finalmente, se obtuvieron todos los datos necesarios para comenzar la mitigación de riesgos. Se decidió que, para efectuar la reducción de los recursos sin uso, se realizaría mediante la modalidad de notificación vía correo electrónico. Mediante la configuración de cada servicio, se descubrió quién era el dueño directo del servicio, y se le enviaba un correo indicando que actuará de acuerdo con la prioridad definida al principio.

VI. ANÁLISIS

La implementación de la solución propuesta trajo consigo una serie de beneficios significativos, tanto en términos de optimización de recursos como de mejora en la ciberseguridad. Uno de los beneficios más destacados fue la reducción de recursos en la nube sin uso, lo que no solo disminuyó los costos, sino que también mitigó posibles riesgos de seguridad asociados con estos recursos no gestionados o huérfanos. La automatización de procesos mediante funciones Lambda y reglas AWS Config personalizadas permitió una gestión más eficiente y efectiva de los recursos, asegurando que se mantuvieran actualizados y en uso constante, evitando así posibles vulnerabilidades explotables por atacantes.

La modalidad de notificación vía correo electrónico jugó un papel crucial en la mitigación de riesgos. Al identificar los dueños directos de los servicios y notificarles de manera oportuna, se garantiza que se tomarán las acciones necesarias de acuerdo con la prioridad establecida. Este enfoque no solo facilitó una respuesta rápida y eficiente, sino que también promovió una mayor responsabilidad y colaboración entre los distintos equipos de trabajo, fortaleciendo así la cultura de seguridad dentro de la organización. Las notificaciones claras y específicas permitieron a los propietarios de los servicios entender la importancia y urgencia de las acciones requeridas, contribuyendo a una reducción efectiva de los riesgos.

Además de los beneficios inmediatos, el proyecto también incluyó la elaboración de una documentación detallada que describe todos los aspectos de la implementación y configuración de los servicios. Esta documentación abarca desde la arquitectura del sistema hasta los procedimientos operativos, proporcionando una guía clara y comprensible para futuros desarrolladores. La existencia de esta documentación asegura la continuidad del proyecto, facilitando el mantenimiento y la reducción de riesgos de seguridad a lo largo del tiempo.

VII. CONCLUSIONES

El proyecto logró cumplir satisfactoriamente con el objetivo general de desarrollar una solución para identificar recursos desplegados en la nube de AWS que no estuvieran siendo utilizados por más de 90 días, con el fin de mitigar riesgos de ciberseguridad. Al abordar este objetivo, se establecieron claramente los recursos más prioritarios para análisis, lo que permitió una focalización eficiente de los esfuerzos y recursos del equipo. La identificación de estos recursos críticos no solo facilitó la gestión de los mismos, sino que también ayudó a priorizar las acciones necesarias para garantizar la seguridad y el cumplimiento continuo.

La definición de una arquitectura detallada y regida por el marco de las buenas prácticas de AWS para la identificación de recursos sin uso, que incluyó el servicio de Continuous Compliance y un sistema de notificación de hallazgos a los equipos dueños de cada recurso, fue fundamental para el éxito del proyecto. Esta arquitectura no sólo proporcionó un marco estructurado y organizado para la implementación de la solución, sino que también aseguró que todas las partes involucradas estuvieran informadas y pudieran tomar las acciones necesarias de manera oportuna. La creación de un documento con el prototipo de desarrollo y su posterior implementación en un ambiente de pruebas permitieron validar la funcionalidad de la solución antes de su despliegue en producción, asegurando así su efectividad y eficiencia.

El desarrollo de la funcionalidad principal para identificar todos los recursos sin uso por más de 90 días en Continuous Compliance y la implementación de pruebas unitarias con una cobertura del 80% demostraron el rigor y la meticulosidad del enfoque adoptado por el equipo. Estas pruebas garantizan que la solución funcionará correctamente bajo diferentes escenarios y condiciones, minimizando así posibles errores y fallos. Finalmente, el despliegue de los artefactos funcionales en ambientes de pruebas y producción, acompañado de la documentación adecuada para la gestión de los recursos, asegura la sostenibilidad y continuidad del proyecto a largo plazo. Este enfoque integral no solo contribuye a la mejora continua de la gestión de recursos en la nube, sino que también establece un precedente para futuros proyectos de seguridad y optimización de recursos en la organización.

REFERENCIAS

[1] what-is-aws. (s. f.). [Web]. Amazon Web Services, Inc. https://aws.amazon.com/es/what-is-aws/?nc1=f_cc

[2] Reliance Steel and Aluminum Uses AWS Well-Architected Framework to Build Better in the Cloud. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc&wa-guidance-whitepapers.sort-by=item.additionalFields.sortDate&wa-guidance-whitepapers.sort-order=desc

[3] CSA - Amazon Web Services (AWS). (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/compliance/csa/

[4] C. Torres. "¿Qué son las normas ISO para la ciberseguridad en la nube? | Webdox CLM". Software de gestión del ciclo de vida de contratos | Webdox CLM. Accedido el 8 de julio de 2024. [En línea]. Disponible: https://www.webdoxclm.com/blog/normas-iso-de-ciberseguridad-27001-27701-27017-27018-27032

[5] "Solución de los 10 riesgos principales de OWASP". Amazon Web Services, Inc. Accedido el 8 de julio de 2024. [En línea]. Disponible: https://aws.amazon.com/es/developer/application-security-performance/articles/addressing-owasp-top-10-risks/