Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°12

GUÍA DE AUDITORÍA PARA LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DE CONTROLES EN AWS

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°12: Guía de Auditoría para la Seguridad de la Información y Ciberseguridad – Controles en AWS.

Esta guía es parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos y herramientas a los Auditores Internos y Servicios Públicos que les permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente.

Santiago, abril 2025.

Daniela Caldana Fulss
Auditora General de Gobierno

Nota

INTRODUCCIÓN

La computación en la nube se basa en un modelo de procesamiento paralelo y distribuido, conformado por un conjunto de equipos interconectados y virtualizados que se aprovisionan de manera dinámica. Dichos recursos se presentan como una o varias unidades de cómputo unificadas, sujetas a acuerdos de nivel de servicio (SLA) que definen tanto el proveedor como el cliente. Esta virtualización permite reconfigurar la infraestructura con rapidez frente a fluctuaciones de carga, logrando aprovechar los recursos de forma más eficaz.

Por otro lado, la computación en la nube ha evolucionado gracias a distintos avances tecnológicos. Entre ellos, el desarrollo de hardware especializado (como la virtualización y los procesadores multinúcleo), la aparición de herramientas web y arquitecturas orientadas a servicios (SOA, Web 2.0), el crecimiento de la computación distribuida (clústeres, grids) y la mejora de la administración de sistemas (computación autónoma, automatización de centros de datos).

Al preparar una lista de verificación para auditorías en entornos de Amazon Web Services, conviene considerar estos fundamentos de computación en la nube y los factores que impulsaron su madurez. En la práctica, una checklist sólida debe revisar aspectos como la correcta configuración de servicios, la aplicación de controles de acceso (IAM), la activación de registros y seguimiento de eventos (CloudTrail, CloudWatch), la encriptación de datos en reposo y en tránsito, así como el cumplimiento de políticas y normativas vigentes (por ejemplo, ISO 27001, PCI DSS o GDPR).
También es importante evaluar la segmentación de redes (VPC), las estrategias de alta disponibilidad y recuperación de desastres (usando zonas de disponibilidad o regiones), y el uso responsable de automatización y orquestación (CloudFormation, Terraform). De igual manera, conviene examinar prácticas de gobernanza que promuevan una gestión clara de costos, versiones y acceso privilegiado. Todos estos puntos garantizan una infraestructura en la nube estable, confiable y alineada con las mejores prácticas de seguridad y cumplimiento.

A continuación, se presenta un checklist que se basa en el trabajo de U.S. Security and Exchange Comission’s (SEC) Office of Compliance Inspections and Examinations (OCIE) (2015), Prácticas recomendadas para la seguridad, la identidad y el cumplimiento – AWS y la Guía de Auditoría para la Seguridad de la Información y la Ciberseguridad N°7 Seguridad en la Nube.

Capítulo 1

PRÁCTICAS DE GOBIERNO

1. PRÁCTICAS DE GOBIERNO

	CHECKLIST SEC OCIE		CHECKLIST GASIC	DÓNDE REVISAR
Objetivo y alcance del uso de AWS	¿Se ha realizado un análisis para comprender el uso de AWS dentro de la organización?		N/A	El objetivo y modelo de uso de AWS es, por sobre todo, la planificación de la organización sobre el uso e integración de los recursos de AWS en los procesos organizacionales. Revise toda la documentación externa que describe la arquitectura y la planificación de uso, incluido registros contables y de control de gestión (en especial de departamentos TI). **Fuera de AWS** Revisar documentación interna (documentación de diseño de infraestructura, inventarios de servicios activos y proveedores, procesos y procedimientos y otra documentación similar) Realizar entrevistas con los equipos de TI y desarrollo. Analizar registros de red y pruebas de penetración. **Dentro de AWS** Consultar informes financieros y pagos de órdenes de compra relacionados con AWS. Verificar accesos en AWS Organizations y AWS IAM. Consultar documentación interna sobre los procesos de negocio y su alineación con TI, considerar los servicios en AWS Service Catalogue. Obtener y analizar informes de auditoría anteriores y sus planes de corrección. Revisar registros en AWS CloudTrail para evaluar problemas pendientes y su resolución.
	¿Se han llevado a cabo entrevistas o encuestas con los equipos de TI y desarrollo para identificar los servicios de AWS en uso?			
	¿Se han realizado escaneos de red o pruebas de penetración para detectar instancias o servicios de AWS activos?			
	¿Se han revisado los informes de gastos y pagos de órdenes de compra (PO) para identificar costos asociados a AWS?			
	¿Se ha considerado que algunos empleados pueden haber registrado cuentas de AWS con sus credenciales personales?			
	¿Se ha definido el alcance de la revisión de los servicios de AWS en su organización?			
	¿Se ha obtenido una descripción de los servicios de AWS que se están utilizando o que se consideran para su uso?			
	¿Se ha determinado qué servicios y soluciones empresariales se incluirán en la revisión tras identificar los servicios de AWS en uso?			
	¿Se han obtenido y revisado informes de auditorías anteriores, incluyendo los planes de corrección?			
	¿Se han identificado problemas pendientes en informes de auditorías anteriores y se han evaluado las actualizaciones de los documentos relacionados con estos problemas?			

	CHECKLIST SEC OCIE		CHECKLIST GASIC		DÓNDE REVISAR
Políticas de Seguridad	¿Se han evaluado y revisado las políticas de seguridad, privacidad y clasificación de datos de la organización para determinar su aplicabilidad al entorno de servicios de AWS?		¿Se ha definido una política de seguridad de la información específica de computación en la nube? Verifique la aprobación y fecha de implementación de la política de seguridad de la información para la computación en la nube, asegurándose de que esté actualizada y vigente. Evalúe los detalles de la Política, contestando:		La Política es un documento de alto nivel que en las organizaciones con sistemas de gestión establecidos deben documentar y almacenar. Al interior de los servicios de software las "políticas" hace referencia a una regla o conjunto de reglas que se deben respetar a la hora de ejecutar un programa. Revisar políticas internas de la organización y documentación en AWS Config y AWS Organizations. Verificar la aprobación, fecha de implementación y revisiones de las políticas, asegurando que estén firmadas por el CISO, CTO, CIO u otro miembro de alta dirección. Consultar el historial de cambios, comunicados internos, boletines y emails oficiales sobre la implementación. Cuando sea requerido: Para la gestión de accesos y privilegios, revisar configuraciones en AWS IAM, auditorías en AWS CloudTrail y cumplimiento en AWS Security Hub. Evaluar la segregación de ambientes en AWS VPC y el almacenamiento de datos en AWS S3 Bucket Policies y AWS Data Residency. Validar la gestión de activos en la nube mediante AWS Service Catalog, AWS Systems Manager y AWS Well-Architected Tool. Verificar políticas de retención y respaldo en AWS Backup y AWS S3 Lifecycle Policies, además de auditorías de pruebas de recuperación. Para la concienciación y capacitación en seguridad, revisar registros internos de formación y, si aplica, utilizar AWS Security Awareness Training.
	¿Existe una política o un proceso formal para la adquisición de servicios de AWS que autorice las compras de estos servicios?				
	¿Los procesos y políticas de administración de cambios de la organización incluyen la consideración de los servicios de AWS?		¿La política en la nube es de la temática específica del cliente que requiere del servicio en la nube?		
			¿Y es consistente con los niveles aceptables de riesgos de seguridad de la información de la organización? Revise registros de evaluaciones de riesgos para confirmar que la política se alinea con los niveles aceptables de riesgo definidos.		
			¿En la política se definen y comunican los \roles y responsabilidades de los usuarios que interactúan con servicios en la nube?		
			¿Aborda las consideraciones geográficas de la ubicación del proveedor de servicios en la nube y el almacenamiento de datos del cliente?		
			¿La política de seguridad de la información aborda adecuadamente el acceso y la gestión de la información almacenada en el entorno de computación en la nube por parte del proveedor de servicios en la nube?		
			¿Se tienen medidas específicas en la política para gestionar el acceso privilegiado de los administradores de servicios en la nube del cliente? Verifique acuerdos contractuales y registros que indiquen la implementación de la política en cuanto a la ubicación geográfica del proveedor de servicios en la nube y el almacenamiento de datos del cliente.		
			¿La política disciplinaria está claramente comunicada a los empleados? ¿Están actualizadas y refleja las medidas disciplinarias actuales?		
			¿Las políticas y procedimientos se informan claramente a los empleados sobre las medidas que podrían tomarse en caso de una infracción?		
			¿Se ha solicitado información al proveedor del servicio en la nube sobre el uso de procedimientos y prácticas de desarrollo seguro?		
			¿El proveedor de servicios en la nube está incluido como un tipo de proveedor en la política de seguridad de la información para las relaciones con los proveedores?		
			Verifique la existencia de un programa formal de revisiones periódicas en la documentación: ¿La alta dirección realiza análisis regulares de las políticas implementadas para verificar su eficacia?		
			¿Existe un proceso formalizado para la revisión y el análisis de las políticas implementadas? Revise registros de los cambios implementados para evaluar si indican mejoras en la eficacia o precisión de la política.		

	CHECKLIST SEC OCIE		CHECKLIST GASIC		DÓNDE REVISAR
Identificación de Riesgos	¿Se ha realizado una evaluación de riesgos para los activos aplicables en el entorno de AWS?		¿Se ha levantado un inventario de todos los servicios de AWS en uso, incluidos EC2, buckets, S3 , VPCs, IAM, bases de datos, Lambda, ¿etc.?		**Fuera de AWS:** Revisar que las matrices de riesgos TI, matrices de ciber-riesgos y matrices de riesgos organizacionales consideran los activos e infraestructura en la nube como vector de riesgo. Revisar el apetito y tolerancia al riesgo y su alineamiento con el nivel de uso de la tecnología y que AWS esté incorporado como activo en la matriz de riesgos corporativo. Revisar el proceso de gestión de riesgos y reportes formales, independiente del estándar que la organización adopte (IRM, ISO 27005, PCI DSS, NIST ERM, COSO, etc.). **En AWS:** Revise los reportes de cumplimiento de estándares (como SOC2, ISO 27001, PCI) dentro de AWS Artifact Revise potenciales vulnerabilidades utilizando Amazon Inspector, asegúrese de incluir sus instancias EC2, contenedores de imágenes Amazon ECR, funciones Lambda y cualquier otro componente relevante. Revise el resultado del monitoreo y escaneo en AWS CloudTrail para el análisis del uso de APIs de alto riesgo y AWS Security Hub para las alertas de seguridad (que se originan en Amazon Inspector, GuardDuty, etc.) y el estado de cumplimiento y adherencia a los estándares y mejores prácticas definidos. Revise el estado de la configuración en AWS Config y la herramienta de diseño para determinar si se encuentra en línea con los controles y criterios determinados Considere los logs de monitoreo y logging para el registro del tráfico de red con indicadores de potenciales amenazas. Revise las alertas y contenido de AWS IAM y AWS Access Analyzer para identificar potenciales riesgos de seguridad en el entorno AWS asociados al control de acceso. Revise los riesgos de arquitectura en el pilar de seguridad de AWS Well-Architected Tool.
	¿Reflejan el entorno actual de la organización?		¿Se han identificado los aspectos técnicos y vulnerabilidades que afectan los servicios en la nube? Revise informes de evaluación de riesgos o auditorías internas que muestren la identificación de aspectos técnicos y vulnerabilidades		
	¿Describen con precisión el entorno de riesgo residual?				
	¿Se ha revisado la documentación de riesgos de la organización?				
	¿Después de cada elemento de la revisión, se han revisado los planes de tratamiento de riesgos?		¿Se han implementado controles criptográficos cuando el análisis de riesgos lo justifica?		
	¿Se han comparado los plazos y hitos de los planes de tratamiento de riesgos con las políticas y procedimientos de gestión de riesgos de la organización?		Verifique que la evaluación de riesgos esté alineada con la gestión de riesgos empresariales, examinando documentos de políticas y procedimientos relacionados con ERM.		
	¿Se ha considerado la tolerancia al riesgo de la organización al evaluar estos datos?		¿Los controles implementados son lo suficientemente sólidos para mitigar los riesgos identificados, ya sea proporcionados por el cliente o el proveedor del servicio en la nube?		
	¿Están los activos de AWS identificados en el programa formal de evaluación de riesgos de la organización?				
	¿Se han asignado objetivos de protección a los activos de AWS según sus perfiles de riesgo?				
	¿Se han identificado los riesgos empresariales asociados con el uso de AWS y se han designado a los propietarios y partes interesadas?				
	¿Los riesgos empresariales están alineados y clasificados según los criterios de seguridad de la organización para proteger la confidencialidad, integridad y disponibilidad en el contexto de AWS?				
	¿Se han revisado auditorías anteriores relacionadas con los servicios de AWS, como SOC, PCI, NIST 800-53 u otras auditorías relevantes?				
	¿Se han abordado adecuadamente los riesgos identificados en auditorías anteriores?				
	¿Se ha evaluado el factor de riesgo general al realizar la revisión de AWS?				
	¿Se han identificado cambios en el alcance de la auditoría basados en la evaluación de riesgos?				
	¿Se han discutido los riesgos con la gerencia de TI y ajustado la evaluación de riesgos en consecuencia?				

	CHECKLIST SEC OCIE		CHECKLIST GASIC	DÓNDE REVISAR
Documentación e Inventario	¿Está completamente documentada la red de AWS y todos los sistemas críticos de AWS están incluidos en el inventario de la organización?		N/A	**En AWS** Revise AWS Config para ver el historial y el estado de configuración de los recursos, en específico: - AWS Config / Resources: Lista de recursos - AWS Config / Timeline: Historial de cambios en configuraciones - AWS Config / Compliance: Cumplimiento respecto a reglas definidas por la organización. Revise AWS Resource Groups para ver y organizar los recursos por etiquetas para relacionarlos con aplicaciones. Revise AWS Tag Editor para ver y organizar los recursos por etiquetas a través de búsquedas de recursos según etiquetas clave-valor. En AWS System Manager Inventory puede recolectar datos de configuración de las instancias EC2 y recursos levantados. Revise las políticas asociadas a los grupos, usuarios, y roles que accedan a los recursos y documentos que se alojen en S3, las políticas de bucket y las alertas de S3 Access Analyzer para identificar accesos indebidos. Para los flujos de datos, revise AWS Architecture Diagram dentro de AWS Perspective Tool para identificar los esquemas arquitectónicos actuales, AWS VPC Flow Logs para el tráfico de red; AWS X-Ray para el flujo de llamadas entre microservicios. Con AWS VPN Connections, AWS Transit Gateway y CloudWatch Logs se obtiene información sobre la conectividad de la red local. **Fuera de AWS** Revise el repositorio oficial (en físico o digital, por ejemplo, en Confluence o Sharepoint) con el diseño de la red e inventario de recursos / activos.
	¿Se ha verificado que la documentación del inventario tiene acceso limitado a personal autorizado?			
	¿Se ha revisado el inventario de recursos en AWS Config y el historial de configuración de estos recursos?			
	¿Están los recursos correctamente etiquetados y asociados a los datos de la aplicación?			
	¿Se ha revisado la arquitectura de la aplicación para identificar los flujos de datos, la conectividad planificada entre los componentes de la aplicación y los recursos que contienen datos?			
	\¿Se ha revisado toda la conectividad entre su red y la plataforma de AWS, incluyendo conexiones VPN y privadas de Direct Connect?			
	¿Se han verificado las direcciones IP públicas locales de los clientes asignadas a las puertas de enlace de los clientes en las VPC del cliente?			

	CHECKLIST SEC OCIE	CHECKLIST GASIC		DÓNDE REVISAR
Entorno Legal y Regulatorio	N/A	Identificar las autoridades pertinentes para la operación combinada del cliente del servicio y del proveedor del servicio en la nube.		**Fuera de AWS** Revise los contratos de servicio (SLA o MSA) para determinar las autoridades pertinentes para la operación y la relación cliente-proveedor. Puede revisar también matrices RACI del sistema de gobierno o políticas donde se establezcan los roles y responsabilidades. Consulte y valide el modelo de responsabilidad compartida en AWS con el responsable de la organización. Revise las actividades y directrices de los procedimientos de gestión de licencias de software en las políticas internas y componentes de GRC. Cuando sea necesario, revise las políticas BYOL. Revise los pasos de validación de las políticas en los sistemas de workflows internos. (por ejemplo: Jira) Revise las políticas internas sobre el tratamiento de datos personales, uso de cláusulas contractuales especiales. **Dentro de AWS** Revise AWS License Mananger para rastreas el uso de las licencias. Revise los informes de compliance en AWS Artif.
		Confirmar las funciones y responsabilidades de seguridad de la información relacionadas con el servicio en la nube, como se describe en el acuerdo de servicio.		
		Tener un procedimiento para identificar los requisitos de licencia específicos de la nube antes de permitir que se instale cualquier software con licencia en un servicio en la nube		
		¿Se han identificado claramente las autoridades pertinentes para la operación combinada del cliente del servicio en la nube y del proveedor del servicio en la nube?		
		¿Se tiene implementado un procedimiento para identificar los requisitos de licencia antes de permitir que se instale software con licencia?		
		¿El procedimiento establece claramente quién es responsable de la identificación de requisitos de licencia antes de la instalación en la nube?		
		¿El procedimiento incluye pasos claros para evaluar y verificar la conformidad de los requisitos de licencia del software con las políticas de la nube antes de la instalación?		
		¿Se lleva a cabo formación y concientización periódica para aquellos responsables de identificar requisitos de licencia antes de instalar software en la nube?		
		¿Se documentan claramente las obligaciones del responsable del tratamiento de la información personal en términos de leyes, reglamentos o contratos?		
		¿La organización considera las leyes y regulaciones pertinentes de las jurisdicciones que rigen tanto al proveedor de servicios en la nube como al cliente del servicio en la nube?		
		¿Cuándo se aplican acuerdos contractuales específicos a la transferencia internacional de datos, como Cláusulas Contractuales Modelo, Normas Corporativas Vinculantes o Normas de Privacidad Transfronteriza, se identifican adecuadamente los acuerdos y los países o circunstancias a los que se aplican?		
		¿Las obligaciones del responsable del tratamiento de la PII respecto a las leyes, reglamentos o contratos están claramente definidas y se incorporan en asuntos en los que el cliente utiliza servicios en la nube pública?		
		¿El encargado del tratamiento de la PII en la nube pública ha desarrollado y aplicado una política sobre la eliminación de la información personal identificable (IIP) y la ha puesto a disposición del cliente del servicio en la nube?		

	CHECKLIST SEC OCIE	CHECKLIST GASIC		DÓNDE REVISAR
Entorno Legal y Regulatorio`	N/A	¿Se han solicitado pruebas del cumplimiento por parte del proveedor del servicio en la nube con las regulaciones y estándares relevantes para el negocio del cliente?		**Fuera de AWS** Revise los contratos de servicio (SLA o MSA) para determinar las autoridades pertinentes para la operación y la relación cliente-proveedor. Puede revisar también matrices RACI del sistema de gobierno o políticas donde se establezcan los roles y responsabilidades. Consulte y valide el modelo de responsabilidad compartida en AWS con el responsable de la organización. Revise las actividades y directrices de los procedimientos de gestión de licencias de software en las políticas internas y componentes de GRC. Cuando sea necesario, revise las políticas BYOL. Revise los pasos de validación de las políticas en los sistemas de workflows internos. (por ejemplo: Jira) Revise las políticas internas sobre el tratamiento de datos personales, uso de cláusulas contractuales especiales. **Dentro de AWS** Revise AWS License Mananger para rastreas el uso de las licencias. Revise los informes de compliance en AWS Artif.
		¿Existen controles de seguimiento implementados para garantizar el cumplimiento de las obligaciones contractuales con el proveedor del servicio en la nube?		
		¿Existe un proceso para identificar los países o circunstancias en los que se aplican estos acuerdos?		
		Revise los contratos y acuerdos con el proveedor del servicio en la nube para identificar cláusulas específicas relacionadas con el cumplimiento y los controles de seguimiento.		
		¿Se aplican sanciones de manera consistente según los controles de seguimiento para garantizar el cumplimiento de las obligaciones contractuales?		
		Revise los registros de sanciones aplicadas en situaciones específicas donde se violaron las obligaciones contractuales. Comparar estas sanciones con los controles de seguimiento establecidos en la política de la empresa.		
		¿Se realiza mejora y verificación a través de pruebas para evaluar el cumplimiento del proveedor del servicio en la nube con las regulaciones y estándares pertinentes?		

Capítulo 2

CONFIGURACIÓN Y SEGURIDAD EN LA RED

	CHECKLIST SEC OCIE		CHECKLIST GASIC	DÓNDE REVISAR
Segmentación de Red	Revise la implementación de AWS Security Group, AWS Direct Connect y la configuración de Amazon VPN para obtener información sobre la implementación adecuada de la segmentación de red y la configuración de ACL y firewall o los servicios de AWS.		N/A	**Dentro de AWS** Revise las reglas de entrada y salida de los grupos en AWS Management Console / EC2 / Security Groups. Revise las configuraciones de redundancia y seguridad de conexión en AWS Management Console / Direct Connect / Connections Servicio AWS VPC, revisión de los elementos de Secutiry group, Network ACL, VPN, Tablas de ruta, at gateways e Internet gateways, End points. Revise la configuración de separación de entornos en AWS Organizations y las reglas de enrutamiento y ACLs en AWS VPC. Revise las reglas de seguridad de tráfico, subredes y VPC en AWS Security Cloud y NACLs. Revise la solución de defensa DDoS en capas que se ejecuta y que opera directamente en AWS, revisando los componentes que se aprovechan como parte de una solución DDoS, como: • Configuración de Amazon CloudFront • Configuración de Amazon S3 • AWS Route 53 • Configuración de ELB **Fuera de AWS** Revise los procedimientos para otorgar acceso remoto a los empleados vía canales de internet o VPN.
	Compruebe que dispone de un procedimiento para conceder acceso remoto, a Internet o VPN a los empleados para el acceso a la consola de AWS y el acceso remoto a las redes y sistemas de Amazon EC2.			
	Revise lo siguiente para mantener un entorno de pruebas y desarrollo de software y aplicaciones que sea independiente de su entorno empresarial: El aislamiento de VPC se implementa entre el entorno empresarial y los entornos utilizados para pruebas y desarrollo.			
	Al revisar la interconexión de VPC entre VPC para garantizar que se implemente el aislamiento de red entre las VPC			
	El aislamiento de subred se implementa entre el entorno empresarial y los entornos utilizados para pruebas y desarrollo.			
	Revisando las NACL asociadas a las subredes en las que se encuentran los entornos de negocio y de prueba/desarrollo para garantizar que se implemente el aislamiento de la red.			
	El aislamiento de instancias de Amazon EC2 se implementa entre el entorno empresarial y los entornos utilizados para pruebas y desarrollo.			
	Revisando los grupos de seguridad asociados a 1 o más instancias asociadas a entornos empresariales, de prueba o de desarrollo para garantizar que se implemente el aislamiento de red entre las instancias de Amazon EC2			

Capítulo 3

CONFIGURACIÓN Y GESTIÓN DE ACTIVOS

	CHECKLIST SEC OCIE		CHECKLIST GASIC	DÓNDE REVISAR
Identificación de Activos	¿Se han identificado los activos asociados a las cuentas de AWS dentro de la organización?		N/A	**En AWS** Revise AWS Config para ver el historial y el estado de configuración de los recursos, en específico: - AWS Config / Resources: Lista de recursos - AWS Config / Timeline: Historial de cambios en configuraciones - AWS Config / Compliance: Cumplimiento respecto a reglas definidas por la organización. Revise AWS Resource Groups para ver y organizar los recursos por etiquetas para relacionarlos con aplicaciones. Revise AWS Tag Editor para ver y organizar los recursos por etiquetas a través de búsquedas de recursos según etiquetas clave-valor. En AWS System Manager Inventory puede recolectar datos de configuración de las instancias EC2 y recursos levantados. Para los flujos de datos, revise AWS Architecture Diagram dentro de AWS Perspective Tool para identificar los esquemas arquitectónicos actuales, AWS VPC Flow Logs para el tráfico de red; AWS X-Ray para el flujo de llamadas entre microservicios. Con AWS VPN Connections, AWS Transit Gateway y CloudWatch Logs se obtiene información sobre la conectividad de la red local. **Fuera de AWS** Revise el repositorio oficial (en físico o digital, por ejemplo, en Confluence o Sharepoint) con el diseño de la red e inventario de recursos y activos.
	¿Se ha revisado la dirección de correo electrónico de contacto de cada cuenta de AWS para identificar a los propietarios?			
	¿Se ha considerado que algunas cuentas pueden estar registradas con proveedores de correo público?			
	¿Se han realizado reuniones con los propietarios de cuentas o activos de AWS para comprender su uso y administración?			
	¿Se ha evaluado cómo los activos de AWS están alineados con las políticas, procedimientos y estándares de seguridad de la organización?			
	¿Se ha entrevistado tanto a los responsables financieros como a los equipos de TI involucrados en la implementación y administración de AWS?			

	CHECKLIST SEC OCIE		CHECKLIST GASIC	DÓNDE REVISAR
Documentación e inventario	¿Está completamente documentada la red de AWS y todos los sistemas críticos de AWS están incluidos en el inventario de la organización?		N/A	**En AWS** Revise AWS Config para ver el historial y el estado de configuración de los recursos, en específico: - AWS Config / Resources: Lista de recursos - AWS Config / Timeline: Historial de cambios en configuraciones - AWS Config / Compliance: Cumplimiento respecto a reglas definidas por la organización. Revise AWS Resource Groups para ver y organizar los recursos por etiquetas para relacionarlos con aplicaciones. Revise AWS Tag Editor para ver y organizar los recursos por etiquetas a través de búsquedas de recursos según etiquetas clave-valor. En AWS System Manager Inventory puede recolectar datos de configuración de las instancias EC2 y recursos levantados. Revise las políticas asociadas a los grupos, usuarios, y roles que accedan a los recursos y documentos que se alojen en S3, las políticas de bucket y las alertas de S3 Access Analyzer para identificar accesos indebidos. Para los flujos de datos, revise AWS Architecture Diagram dentro de AWS Perspective Tool para identificar los esquemas arquitectónicos actuales, AWS VPC Flow Logs para el tráfico de red; AWS X-Ray para el flujo de llamadas entre microservicios. Con AWS VPN Connections, AWS Transit Gateway y CloudWatch Logs se obtiene información sobre la conectividad de la red local. **Fuera de AWS** Revise el repositorio oficial (en físico o digital, por ejemplo, en Confluence o Sharepoint) con el diseño de la red e inventario de recursos / activos.
	¿Se ha verificado que la documentación del inventario tiene acceso limitado a personal autorizado?			
	¿Se ha revisado el inventario de recursos en AWS Config y el historial de configuración de estos recursos?			
	¿Están los recursos correctamente etiquetados y asociados a los datos de la aplicación?			
	¿Se ha revisado la arquitectura de la aplicación para identificar los flujos de datos, la conectividad planificada entre los componentes de la aplicación y los recursos que contienen datos?			
	¿Se ha revisado toda la conectividad entre su red y la plataforma de AWS, incluyendo conexiones VPN y privadas de Direct Connect?			
	¿Se han verificado las direcciones IP públicas locales de los clientes asignadas a las puertas de enlace de los clientes en las VPC del cliente?			

	CHECKLIST SEC OCIE		CHECKLIST GASIC		DÓNDE REVISAR
Evaluación de la Configuración de Activos	Evalúe la gestión de la configuración. Verifique el uso de sus prácticas de administración de configuración para todos los componentes del sistema de AWS y valide que estos estándares cumplan con las configuraciones de referencia.		¿Se ha implementado una política de seguridad para restringir solo los puertos, protocolos y servicios necesarios en las máquinas virtuales?		**En AWS** Analice el sistema de administración de accesos. (AWS IAM) Revise las herramientas de Inspector y Security Hub para escanear los entornos y detectar vulnerabilidades. Revisar la frecuencia de los análisis y los informes de hallazgos. Revise la segmentación de recursos críticos en las ACL y los grupos de seguridad definidos. Revise la estructura de VPC.
			¿Se han reforzado los aspectos apropiados de las máquinas virtuales utilizadas en la nube?		
	Revise el procedimiento para llevar a cabo un procedimiento de borrado especializado antes de eliminar el volumen para verificar que cumpla con los requisitos establecidos.		Verifique que se hayan implementado medidas técnicas apropiadas, como soluciones antimalware y logging, en cada máquina virtual según lo establecido en los procedimientos de configuración.		
	Revise su sistema de administración de acceso a identidades (que se puede utilizar para permitir el acceso autenticado a las aplicaciones alojadas en la parte superior de los servicios de AWS).		¿Existe un análisis de los riesgos asociados a los puertos, protocolos abiertos y elementos CI? ¿Se han desactivado servicios y CI no esenciales para reducir la superficie de ataque?		
	Confirme que se han completado las pruebas de penetración.		¿Hay procesos automáticos para la detección y respuesta a posibles amenazas?		
			¿Se han aplicado parches y actualizaciones de seguridad de manera regular en las máquinas virtuales?		
			¿El proveedor de servicios en la nube ofrece capacidades de monitoreo detalladas para las máquinas virtuales utilizadas? Consulte la documentación del proveedor de servicios en la nube para verificar la disponibilidad y alcance de las capacidades de monitoreo ofrecidas.		
			Realice pruebas de monitoreo en tiempo real para evaluar la efectividad y la profundidad del monitoreo proporcionado por el proveedor.		

	CHECKLIST SEC OCIE		CHECKLIST GASIC		DÓNDE REVISAR
Evaluación de la Gestión de Cambios	Controles de gestión de cambios. Asegúrese de que el uso de los servicios de AWS siga los mismos procesos de control de cambios que las series internas.		N/A		**En AWS** Revise las herramientas y servicios que AWS ha definido para la gestión de cambios, que incluye: - AWS CloudFormation - AWS CodePipeline - AWS CodeCommit Revise AWS System Manager y Patch Manager para determinar la aplicación de actualizaciones. Revise AWS Manitenance Windows para analizar los procedimientos de mantenimiento programados.
	Verifique que los servicios de AWS estén incluidos en un proceso interno de administración de parches. Revise el proceso documentado para la configuración y la aplicación de parches de las instancias de Amazon EC2: o Imágenes de máquina de Amazon (AMI) o Sistemas operativos o Aplicaciones				
	Revise las llamadas a la API para los servicios dentro del ámbito de las llamadas de eliminación para asegurarse de que los activos de TI se hayan eliminado correctamente.				

Capítulo 4

CONTROL DE ACCESOS

	CHECKLIST SEC OCIE		CHECKLIST GASIC		DÓNDE REVISAR
Gestión de Accesos	Gestión de accesos, autenticación y autorización. Asegúrese de que existan políticas y procedimientos internos para administrar el acceso a los servicios de AWS y a las instancias de Amazon EC2.		¿Cómo se gestiona la creación, modificación y eliminación de identidades de usuario en los servicios de la nube?		**Fuera de AWS** Revise que existan las políticas y procedimientos documentados que regulen el acceso a AWS. Revise los procesos de creación, modificación y eliminación de cuentas de usuario. Revise los procesos y métodos implementados para supervisar las actividades y accesos a las cuentas y roles IAM **Dentro de AWS** Revise la lista de usuarios, grupos y permisos en AWS Identity and Access Management Revise la gestión centralizada de las cuentas en AWS Organizations. Revise la descripción de identidades y permisos en Amazon IAM. Revise la lista de recursos, grupos de seguridad, VPN y permisos en Amazon IAM. Revise la especificidad de los medios de autenticación y acceso (por ejemplo, nativos de AWS o a través de SAML) y verifique que sea concordante con las políticas y controles de seguridad. Utilice AWS IAM Access Analyzer para revisar los permisos e identificar los accesos no utilizados o innecesarios. Verifique que los el multifactor de autenticación (MFA), los sistemas de autenticación basados en roles (RBAC) y la gestión de accesos centralizados (SSO) se encuentran habilitados según lo definido en los controles y políticas de seguridad.
	Garantice la documentación del uso y la configuración de los controles de acceso de AWS, los ejemplos y las opciones que se describen a continuación:		¿Se han abordado de manera adecuada los procedimientos para el registro y la baja de usuarios en situaciones donde el control de acceso se ve comprometido, como la corrupción o el compromiso de contraseñas u otros datos de registro? ¿Los procedimientos de registro y baja de usuarios incluyen medidas de auditoría para rastrear las acciones tomadas durante estas operaciones?		
	Descripción de cómo se utiliza Amazon IAM para la administración de acceso.				
	Lista de controles que se utiliza para administrar Amazon IAM: administración de recursos, grupos de seguridad, VPN, permisos de objetos, etc.		¿Se realiza una revisión periódica y actualización de los requisitos de acceso de los usuarios a los servicios de nube? ¿Se sigue un proceso de revisión regular para garantizar la precisión de las identidades?		
	Uso de controles de acceso nativos de AWS, o si el acceso se administra a través de la autenticación federada, que aprovecha el estándar abierto Security Assertion Markup Language (SAML) 2.0.		Revise los registros de revisiones periódicas de los requisitos de acceso a los servicios de nube, asegurándose de que estas revisiones se realicen según la frecuencia especificada en la política de control de acceso.		
	Lista de cuentas, roles, grupos y usuarios de AWS, políticas y adjuntos de políticas a usuarios, grupos y roles.		¿Se implementa un sistema de autorización que limite el acceso a recursos específicos basándose en roles y necesidades?		
	Una descripción de las cuentas y roles de Amazon IAM, así como de los métodos de monitorización.		¿Existe un plan de respuesta a incidentes específico para situaciones en las que el control de acceso de los usuarios se ve comprometido?		
	Descripción y configuración de los sistemas dentro de EC2		¿Cuáles son los métodos de autenticación utilizados para acceder a los servicios en la nube?		
			¿Se implementan medidas de control de acceso, para garantizar que la información registrada solo se utilice para los fines previstos?		
			¿Se gestiona el acceso de los usuarios del servicio de nube bajo el control del cliente, proporcionando derechos administrativos para gestionar o cancelar el acceso? o Revise la documentación de gestión de acceso del servicio de nube para confirmar la asignación de derechos administrativos a los usuarios bajo el control del cliente.		
			¿Se utiliza inicio de sesión único y autenticación abierta en lugar de tecnologías de autenticación patentadas por los proveedores de servicios?		
			Revise la existencia de registros de acceso que permitan identificar cualquier intento o instancia de acceso no autorizado a recursos de la nube. Estos registros deben incluir información detallada sobre el usuario, la hora, el tipo de acceso y cualquier actividad sospechosa.		
			¿Existen indicadores para medir el cumplimiento de la política de control de acceso a la nube?		
			¿Se ha realizado un análisis de datos para evaluar el cumplimiento del control de acceso a la nube?		
			¿Las mejoras identificadas durante el análisis de datos se aplican de manera efectiva?		

	CHECKLIST SEC OCIE		CHECKLIST GASIC	DÓNDE REVISAR
Gestión de Acceso Remoto	Acceso remoto. Asegúrese de que haya un proceso de aprobación, un proceso de registro o controles para evitar el acceso remoto no autorizado. Nota: Todo el acceso a las instancias de AWS y Amazon EC2 es de "acceso remoto" por definición, a menos que se haya configurado Direct Connect.		N/A	**En AWS** Revise los registros de AWS CloudTrail para registrar y Monitorear las llamadas API de serviciso AWS. Revise los registros de "quien" y "donde" se realizan estas llamadas. Revise logs de registros de actividades y de detección de anomalías en Amazon CloudWatch. Revise las políticas de IAM y de buckets S3, revise su adecuación a las políticas organizacionales. Revise las listas de control de acceso y tablas de enrutamiento para controlar el tráfico hacia AWS, o en AWS Directo Connect.
	Proceso de revisión para evitar el acceso no autorizado, que puede incluir: AWS CloudTrail para el registro de llamadas a la API de nivel de servicio.			
	Registros de AWS CloudWatch para cumplir con los objetivos de registro.			
	Políticas de IAM, políticas de bucket de S3, grupos de seguridad para controles que eviten el acceso no autorizado.			
	Revise la conectividad entre la red de la empresa y AWS: o Conexión VPN entre la VPC y la red de la empresa. o Conexión directa (conexión cruzada e interfaces privadas) entre la empresa y AWS. o Grupos de seguridad definidos, listas de control de acceso a la red y tablas de enrutamiento para controlar el acceso entre AWS y la red.			

Capítulo 5

SEGURIDAD OPERACIONAL EN ENTORNOS CLOUD

	CHECKLIST SEC OCIE		CHECKLIST GASIC		DÓNDE REVISAR
Encriptación	Asegúrese de que existan controles adecuados para proteger la información confidencial en el transporte mientras se utilizan los servicios de AWS.		Identificar las claves criptográficas para cada servicio en la nube e implementar procedimientos para la gestión de claves.		**En AWS** Revise las conexiones a la consola de AWS y a las API de administración utilicen HTTPS (TLS) para cifrar los datos en tránsito. Revise la configuración HTTPS en Amazon S3 Revise las conexiones a las bases de datos RDS que utilicen SSL/TLS en Amazon RDS. Revise las conexiones VPN en Amazon EC2 VPN. Revise la configuración de AWS Key Management Service (KMS). Revise los módulos de seguridad de hardware (HSM) en AWS CloudHSM. Revise la criptografía utilizada en los EBS del servicio Amazon EC2.
	Revise los métodos de conexión a la consola de AWS, la API de administración, S3, RDS y Amazon EC2 VPN para la aplicación del cifrado.		Asegurar que se refuercen los aspectos apropiados (Por ejemplo: Solo aquellos puertos, protocolos y servicios que sean necesarios) Y de que existan las medidas técnicas apropiadas (Por ejemplo: antimalware, logging) para cada máquina virtual utilizada al momento de configurar máquinas virtuales.		
	Revise las políticas y los procedimientos internos para la administración de claves, incluidos los servicios de AWS y las instancias de Amazon EC2.				
	Revise los métodos de cifrado utilizados, si los hay, para proteger los PIN en reposo: AWS ofrece una serie de servicios de administración de claves, como KMS, CloudHSM y cifrado del lado del servidor para S3, que podrían usarse para ayudar con el cifrado de datos en reposo.		Revisar cualquier información proporcionada por el proveedor de servicios en la nube cuando ofrece criptografía para confirmar si las capacidades criptográficas: 2.1 Cumplen con los requisitos de política del cliente del servicio en la nube.		
			2.2 Son compatibles con cualquier otra protección criptográfica utilizada por el cliente del servicio en la nube.		
			2.3 Se aplican a los datos en reposo y en tránsito hacia, desde y dentro del servicio en la nube.		

Capítulo 6

REGISTRO Y SUPERVISIÓN DE SEGURIDAD

	CHECKLIST SEC OCIE		CHECKLIST GASIC		DÓNDE REVISAR
Revisión y Supervisión de Seguridad	Registro, evaluación y seguimiento: Revise las políticas y los procedimientos de registro y monitoreo para determinar la adecuación, la retención, los umbrales definidos y el mantenimiento seguro, específicamente para detectar actividades no autorizadas en los servicios de AWS.		Auditar y revisar los informes, registros y servicios de terceros, a intervalos planificados, para regir y mantener el cumplimiento de los acuerdos de prestación de servicios.		**En AWS** Revise los servicios AWS en el monitoreo: - Revise las instancias EC2 con CloudWatch para recopilar y monitorear el sistema de aplicaciones de instancias EC2. - Revise los accesos de registro en los balanceadores de carga (ELB) para monitorear las solicitudes recibidas. - Revise la configuración de registros estándar o en tiempo real para monitorear las solicitudes a distribuciones en CloudFront. - Revise los servicios de AWS y verifique que existe un depósito de información centralizado. En general, toda la infraestructura de AWS contiene opciones de monitoreo, incluido pero no limitado a: Flujos VPC, Amazon CloudWatch, AWS Config, AWS IAM, AWS CloudTrail, CloudFront y ELB.
			Especificar los requisitos para el acceso de los usuarios a cada servicio de nube separado que se utilice dentro de la política de control de acceso para el uso de servicios de red.		
	Revise las políticas y los procedimientos de registro y monitoreo, y garantice la inclusión de los servicios de AWS, incluidas las instancias de Amazon EC2, para eventos relacionados con la seguridad.				
	Verifique que los mecanismos de registro estén configurados para enviar registros a un servidor centralizado y asegúrese de que, en el caso de las instancias de Amazon EC2, se conserven el tipo y el formato adecuados de los registros de forma similar a los sistemas físicos.				
	En el caso de los clientes que utilizan AWS CloudWatch, revise el proceso y el registro del uso de la monitorización de red.				
	Asegúrese de que los análisis de eventos se utilicen para mejorar las medidas y políticas defensivas.				
	Revise el informe de credenciales de AWS IAM para usuarios no autorizados, AWS Config y etiquetado de recursos para dispositivos no autorizados.				
	Confirme la agregación y correlación de datos de eventos de varias fuentes mediante servicios de AWS, como:				
	Registros de flujo de VPC para identificar los paquetes de red aceptados/rechazados que ingresan a la VPC.				
	AWS CloudTrail para identificar llamadas a la API autenticadas y no autenticadas a los servicios de AWS.				
	ELB Logging: registro del equilibrador de carga.				
	AWS CloudFront Logging: registro de distribuciones de CDN.				