Herramienta Centralizada para la Gestión de la postura de Seguridad Multicloud

Paola Hernández
Departamento de Ingeniería de Sistemas y Computación
Universidad de los Andes
Bogotá, Colombia
p.hernandezs@uniandes.edu.co

Resumen - ***Resumen*** **— Este trabajo aborda la problemática en una empresa que brinda servicios BPO e ITO en entidades importantes del gobierno Colombiano, donde se gestionan los activos desplegados en la nube, los cuales enfrentan deficiencias significativas a nivel de control oportuno sobre el estado de su seguridad, lo que conlleva a tener configuraciones inseguras y servicios no optimizados, como servicios abiertos y vulnerables, la exposición no controlada de servicios a Internet, pérdidas de datos sensibles, uso no autorizado de recursos, interrupciones de servicio y hasta la percepción negativa del cliente. Esta situación pone en riesgo la integridad, confidencialidad y disponibilidad de los datos críticos manejados por la empresa BPO, así como la continuidad o renovación de la prestación de servicio a los actuales clientes.**

Para abordar esta problemática, se propone la implementación de "La herramienta para la gestión de la postura centralizada de seguridad multinube", para los clientes de la empresa BPO, que permita el evaluar y mejorar continuamente el score de seguridad de la información de los recursos y la información gestionada por la empresa, independiente de quién sea el proveedor cloud. Se pretende consolidar la gestión de la información en un tablero de mando centralizado y dinámico, que facilite la buena y oportuna toma de decisiones, la implementación de controles, la remediación de vulnerabilidades y el mejorar la postura de seguridad a un nivel de confianza aceptable por el cliente, soportados en un único framework que tome las mejores prácticas de CIS Control V8, NIST e ISO 27001:2022.

Palabras clave**—**CSMP, Azure, AWS, Defender for Cloud, Security Hub, Framework CIS Control V8, NIST 800-53 y Estandar ISO 27001:2022, Inteligencia de Negocio BI, SIEM, Cuadro de Mando**.**

I. CONTEXTO

La empresa es una entidad de servicios integrales de ITO (Outsourcing de Tecnologías de la Información) y BPO (Outsourcing de Procesos de Negocio), que atiende a clientes del sector Gobierno con una alta demanda en disponibilidad y seguridad de información, sobre todo en los sistemas de atención al ciudadano. Estos clientes cuentan con cargas de trabajo desplegadas en servicios cloud en AWS y Azure. Con la rápida migración de sus servicios a la nube, se han generado varios desafíos en la gestión de riesgos y en la oportuna respuesta y remediación de vulnerabilidades. Como

ha crecido el número de clientes, con diferentes entornos cloud, se han incrementado los procesos y tareas de identificación, análisis, reporte, remediación y mejora de la postura de seguridad, lo que ha generado altas cargas de trabajo en la elaboración de matrices y planes de remediación, así como la ejecución de varias actividades manuales; el tener que ingresar a cada portal de cada cliente, de forma individual implica el desarrollo de los procesos demorados y poco eficientes, para luego ser socializados con los equipos de TI y Desarrollo.

Lo anterior, consume recursos valiosos, generando demoras en la identificación y mitigación de riesgos críticos; adicionalmente, se disminuye la capacidad del equipo para mantenerse al tanto de las amenazas emergentes. Para desarrollar las actividades de detección y remediación de vulnerabilidades, se necesita asignar un recurso humano dedicado aproximadamente 80 horas mensuales. Este empleado tiene un costo por hora significativo, lo que resulta en un costo operativo considerable para la organización cada mes. Estos recursos financieros podrían ser utilizados de manera más eficiente al asignar a este recurso tareas con un enfoque más especializado en la optimización de los servicios de seguridad ofrecidos.

La falta de visibilidad consolidada de la postura de seguridad de los diferentes clientes dificulta la identificación temprana de actividades maliciosas, vulnerabilidades o eventos de seguridad, requiriendo un esfuerzo adicional y manual para gestionar y analizar datos dispersos. Esta carga de trabajo elevada no solo afecta la capacidad de respuesta ante incidentes, sino que también limita la eficacia de la detección proactiva de posibles riesgos. Como resultado de lo anterior, se produjo un ataque de

denegación de servicio (DDoS) hace unos años, dejando uno de los portales principales de un cliente indisponible durante 45 minutos. Esto resultó en una multa significativa que refleja el costo directo asociado con la interrupción del servicio y la violación de la disponibilidad de los servicios esenciales del cliente.

El crecimiento y descentralización de la postura de seguridad ha creado desafíos en la gestión de riesgos en la nube, y la oportunidad de identificación, remediación y mejora. Actualmente, el tiempo de identificación, análisis y reporte está sobre las 3 semanas y el tiempo de remediación entre 2 a 3 meses, lo que genera un alto nivel de exposición.

La empresa requiere de una herramienta que facilite las funciones de identificación, protección, detección, respuesta y recuperación, que les permita cumplir con los requisitos de seguridad acordados con cada cliente y asegure el evidenciar el cumplimiento normativo o la adopción de las buenas prácticas de seguridad, de acuerdo con el entorno y las cargas de trabajo cloud.

Como parte fundamental de la herramienta, se requiere de un framework unificado que permita la evaluación de la postura de seguridad de forma transversal y estandarizada para todos los clientes. Esto facilitará la generación de indicadores, métricas, ANS y la toma adecuada de decisiones.

II. JUSTIFICACIÓN DEL PROBLEMA

En el siguiente diagrama de causa – efecto (Ishikawa), se presentan las posibles causas del problema de seguridad multinube en una empresa BPO:

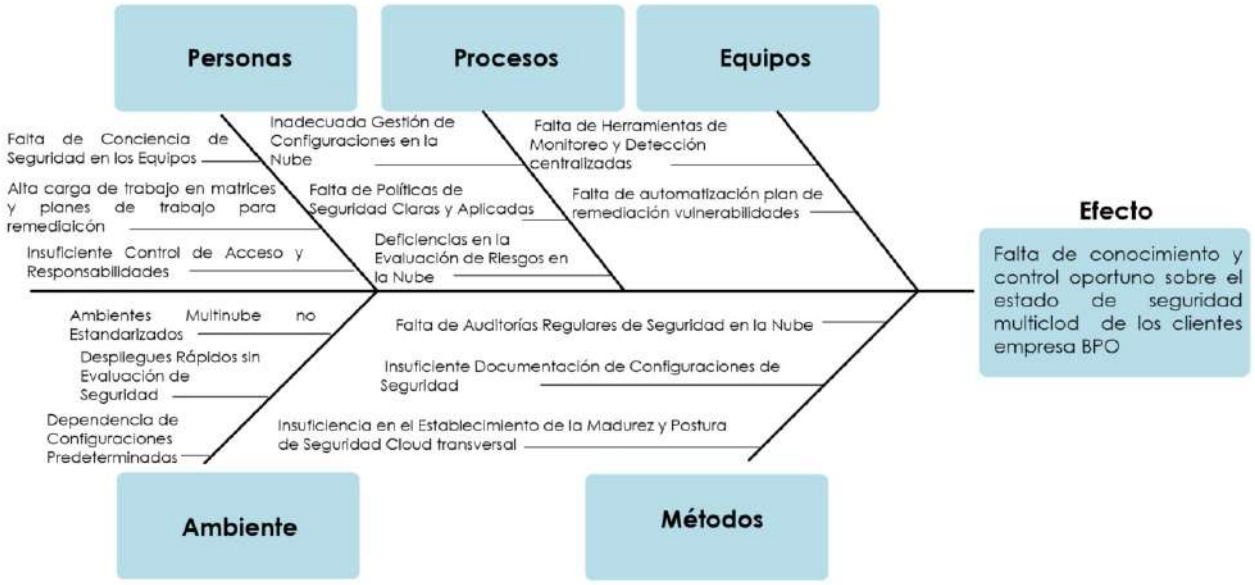


Imagen 1: diagrama (Ishikawa) Causas del problema

La identificación de las causas subyacentes revela las circunstancias y deficiencias que contribuyen al problema central de seguridad multinube en los clientes de la empresa BPO. Dentro de los principales se encuentran:

Falta de Conciencia en Seguridad: La falta de conocimiento y comprensión sobre las amenazas y las mejores prácticas de seguridad crea un desafío adicional, ya que la falta de madurez impide priorizar eficazmente los temas críticos que se necesitan abordar y concientizar en cada uno de los grupos de trabajo. Sin una comprensión sólida de la seguridad en la nube, resulta difícil discernir y destacar los temas clave que requieren atención urgente, dejando a los equipos potencialmente expuestos a riesgos y vulnerabilidades no identificados.

Alta Carga en la Gestión de remediación: la carga de trabajo elevada puede contribuir a la fatiga laboral y disminuir la capacidad del equipo para mantenerse al tanto de las

amenazas emergentes, agravando aún más la situación de seguridad en el entorno multinube. La simplificación y automatización de estos procesos se vuelve imperativa para aliviar la carga laboral, permitiendo una respuesta más ágil y efectiva a los desafíos de seguridad.

Insuficiencia en el Establecimiento de la Madurez y Postura de Seguridad Cloud: La insuficiencia en el establecimiento de un modelo de madurez y postura de seguridad cloud estándar y transversal, justifica la problemática al indicar la ausencia de un marco estructurado y de una gestión efectiva de la seguridad en los entornos multinube. Esta falta de claridad y aplicación propicia la existencia de brechas de seguridad no abordadas adecuadamente, aumentando el riesgo de ser fácilmente atacadas.

Falta de herramientas centralizadas: La carencia de una solución centralizada eficiente para monitorear y detectar amenazas en entornos multinube, impone una carga operativa significativa sobre los equipos encargados de la seguridad. Esta carga de trabajo elevada no solo afecta la capacidad de respuesta ante incidentes, sino que también limita la eficacia de la detección proactiva de posibles riesgos.

III. PROPUESTA DE LA SOLUCIÓN

Definir, diseñar y aplicar una herramienta para la gestión de la postura centralizada de seguridad multinube, para los clientes de la empresa BPO, que permita evaluar y mejorar continuamente el score de seguridad de la información de los recursos y la información gestionada por la empresa, independiente del proveedor cloud. Se busca consolidar la gestión de la información en un tablero de mando centralizado y dinámico, que facilite la buena toma de decisiones, la implementación de controles, la remediación de vulnerabilidades y mejorar la postura de seguridad a un nivel de confianza aceptable por cada cliente sobre un framework unificado para todos ellos.

IV. OBJETIVOS ESPECÍFICOS

- Seleccionar un marco de referencia que permita unificar una postura de seguridad cloud de forma transversal.
- Adaptar el modelo CSPM que permita identificar, priorizar, notificar y mitigar el riesgo en la infraestructura y las aplicaciones implementadas en entornos multinube.
- Consolidar de forma centralizada, actualizada y automática, los hallazgos de seguridad reportados por las herramientas de auditoría configurada en cada proveedor de servicios en la nube.
- Desarrollar flujos de trabajo que permitan determinar el path(ruta) para las remediaciones y la mejora del nivel de madurez (score) cloud.
- Centralizar la identificación de brechas de seguridad, de los recursos con mayor riesgo de explotación y de las configuraciones que requieran de una atención inmediata en todas las suscripciones cloud administradas por la empresa.
- Desplegar una plataforma centralizada para la gestión de seguridad de la información con tableros de control.
- Implementar mecanismos automáticos de aprobación y notificación de acciones urgentes, asegurando que estas sean informadas y autorizadas de manera eficiente.

V. DIAGRAMA DE ARQUITECTURA A ALTO NIVEL

La arquitectura de alto nivel propuesta está diseñada para centralizar la gestión de la postura de seguridad en entornos de nube de diferente proveedor, comprende diversos componentes que colaboran para evaluar y administrar la seguridad de los recursos en la nube.

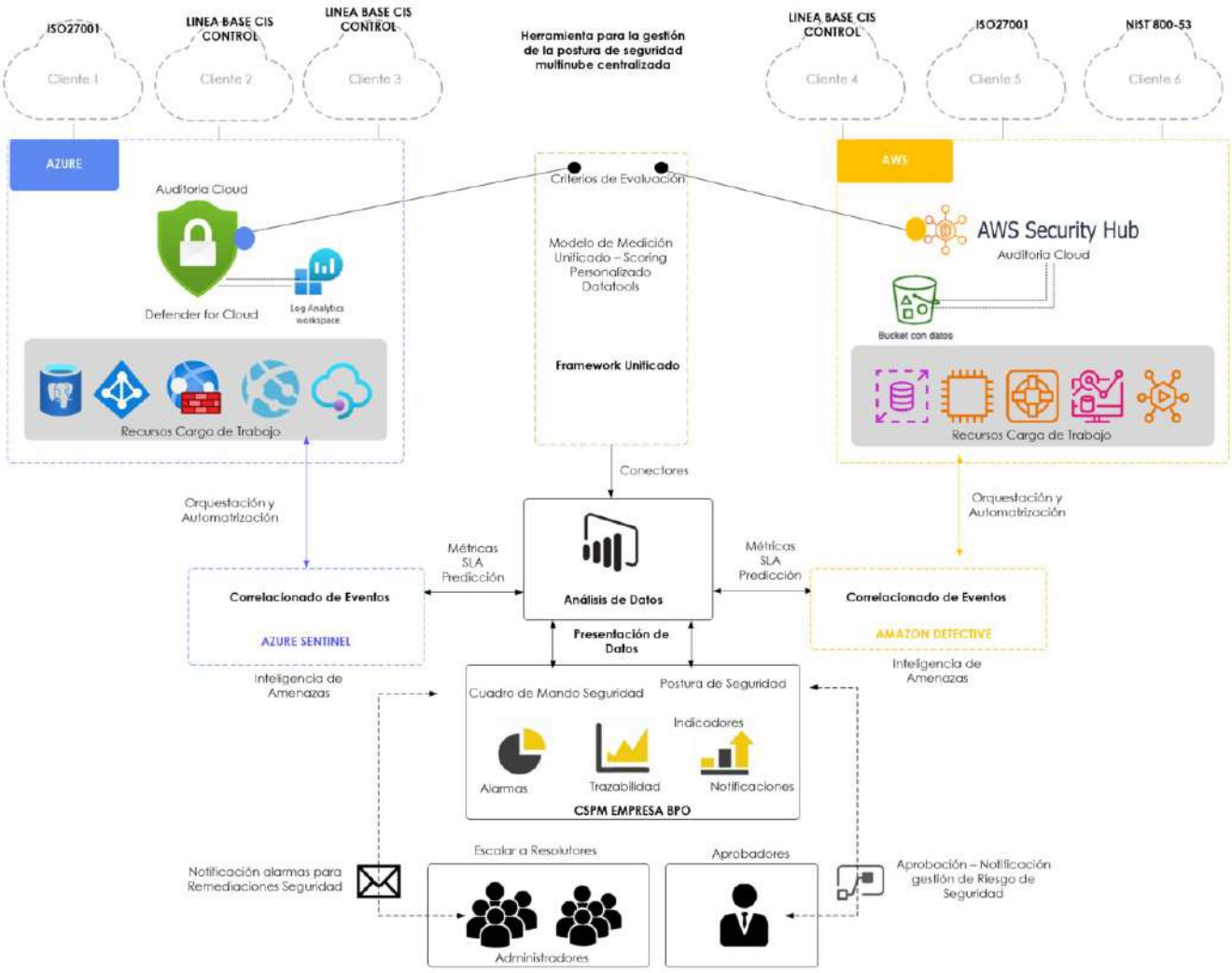


Imagen 2: Arquitectura de Alto Nivel

Dentro de los requerimientos se tienen:

Los Funcionales:

- Adaptar el Framework Unificado, con los resultados obtenidos de las herramientas Defender for Cloud (Azure) y Security Hub (AWS), buscando una homogeneización que permita una integración coherente de los datos y hallazgos proporcionados por ambas soluciones de seguridad.
- Reportar alertas y notificaciones para eventos de seguridad críticos.
- Generación de una visión consolidada de la postura de seguridad para Azure y AWS.
- Desarrollo de un dashboard visual que presente las brechas de seguridad por cliente.
- Capacidad para enviar notificaciones por correo electrónico ante eventos o brechas de seguridad
- Implementación de un flujo de trabajo que permita la autorización de remediaciones por líderes o directores.
- Funcionalidad que permite a los usuarios descargar reportes en formato PDF y CSV.
- Conservación de registros históricos para analizar tendencias de remediación y seguimiento de mejoras en el score a lo largo del tiempo.

Los No funcionales:

- Eficiencia en el procesamiento de grandes conjuntos de datos de seguridad para generar informes y alertas.

- Capacidad para manejar un crecimiento significativo en el número de recursos y entornos de nube gestionados.
- Adherencia a estándares y prácticas de seguridad robustas para proteger los datos y la integridad de la herramienta.
- Interfaz intuitiva y fácil de usar para simplificar la configuración, supervisión y análisis de la seguridad en la nube.

Los Técnicos:

- Conexión con las APIs de Azure y AWS para recopilar datos y aplicar cambios de seguridad.
- Implementación de un almacenamiento seguro para los datos de registros y configuraciones.
- Automatización de aprobaciones mediante flujos de trabajo.
- Integración con otras herramientas de seguridad como los correlacionadores de eventos y herramientas de monitoreo cloud.
- Utilizar protocolos seguros para la comunicación, asegurando la confidencialidad e integridad de los datos transmitidos.

VI. DESARROLLO ACOTADO AL ALCANCE

Por razones de tiempo, costos y recursos, el proyecto se enfocará en la implementación de un prototipo que se enfoca en los siguientes componentes:

Definición de Framework de seguridad Unificado:
La herramienta propuesta se centra en comparar tres marcos principales: ISO 27001:2022, NIST 800-53 y CIS Controls v8. Evaluará sus similitudes y diferencias en términos de seguridad de la información. Esta evaluación tiene como objetivo definir la postura de seguridad centralizada en la nube específica de la empresa para cada uno de los clientes cloud.

Activación de Defender For Cloud en Azure y Security hub en AWS para un cliente en cada nube: Esto permitirá el escaneo y reporte de las vulnerabilidades de seguridad de acuerdo a las cargas de trabajo desplegadas en cada suscripción.

Comparación del framework unificado con los resultados de las dos nubes. Esto permitirá evaluar el nivel de adherencia, cumplimiento y desviación de las dos suscripciones aws y Azure.

Configurar herramienta de análisis y presentación de Datos (Power BI) para conexión a las fuentes de datos de Defender for cloud y Security Hub.

Creación de Dashboard para presentar los resultados del score de seguridad de forma centralizada, presentar el Gap respecto al framework unificado.

VII. ARQUITECTURA ACOTADA AL ALCANCE

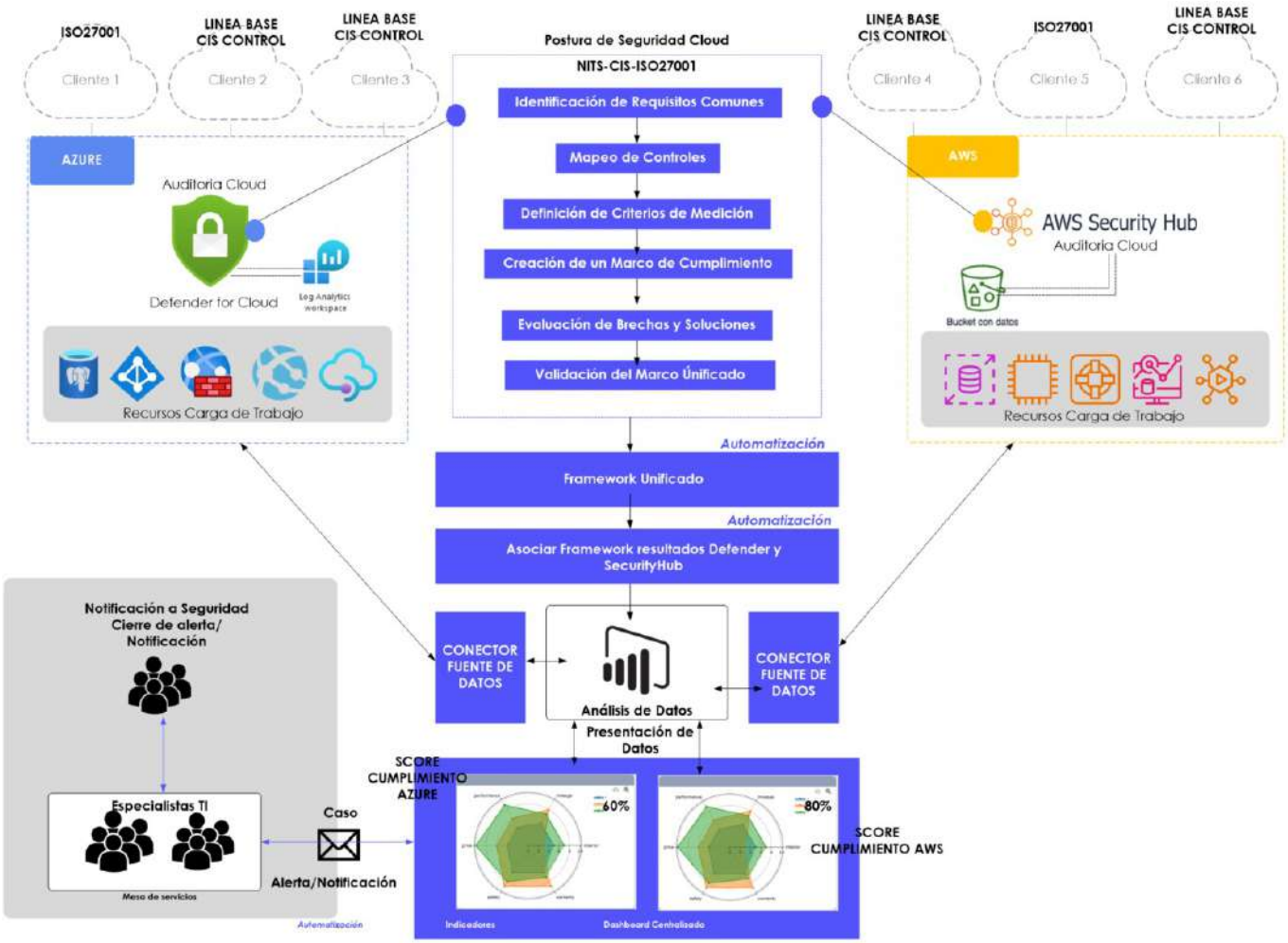


Imagen 3: Arquitectura Acotada al alcance

Conector de Nube: Este componente establece conexiones seguras con las fuentes de datos que almacenan la información de auditorías realizadas periódicamente por herramientas como Defender for Cloud y CloudTrail. Su función es recopilar de manera segura datos sobre el estado de seguridad de los recursos, asegurando conformidad con los marcos de trabajo y buenas prácticas definidas.

Framework Unificado: Proporciona una estructura unificada para estandarizar las posturas de seguridad en entornos Azure y AWS. Esto facilita la coherencia y la aplicación consistente de políticas de seguridad en ambas plataformas.

Fuentes de Datos: Recursos de almacenamiento dedicados a conservar los registros de las herramientas Defender for Cloud (para Azure) y CloudTrail (para AWS). Estos almacenes de datos contienen la información esencial para el análisis y seguimiento de la seguridad en la nube.

Procesamiento y Análisis de Datos: Se encarga de procesar y analizar los datos recopilados para generar métricas, estadísticas, historiales de vulnerabilidades, y controlar riesgos y severidades de los hallazgos. Esta fase es fundamental para comprender el panorama de seguridad y orientar las acciones correctivas.

Cuadro de Mando: Presenta de manera visual los datos relevantes, utilizando gráficos, radares y alarmas para representar brechas en la seguridad. Proporciona notificaciones y una visión general de la postura de seguridad, permitiendo una rápida identificación de áreas de mejora.

Notificaciones: Gestiona oportunamente los hallazgos notificando a los responsables pertinentes. Este componente facilita la interacción y colaboración eficiente en la toma de decisiones relacionadas con la seguridad.

VII. FRAMEWORK DE SEGURIDAD UNIFICADO

Para la evaluación de los 3 frameworks se empleó el siguiente procedimiento:

Paso	Acción	Descripción
1	Identificación de Requisitos Comunes	Analizar requisitos específicos de NIST 800-53, CIS Controls V8 e ISO 27001:2022 para la seguridad en la nube. Identificar áreas o controles comunes y similitudes.
2	Mapeo de Controles	Mapear controles específicos de cada estándar y asociarlos con sus equivalentes en los otros estándares.
3	Definición de Criterios de Medición	Establecer criterios de medición aplicables a los controles identificados. Definir métricas claras y objetivas para evaluar el cumplimiento de cada control.
4	Creación de un Marco de Cumplimiento	Desarrollar un marco de cumplimiento unificado que integre requisitos y controles clave de los tres estándares, abordando las particularidades de la nube.
5	Evaluación de Brechas y Soluciones	Realizar una evaluación de brechas comparando el estado actual con el marco unificado. Identificar áreas que requieren mejoras y desarrollar soluciones específicas.
6	Validación del marco unificado.	Mapear el marco unificado con los resultados de evaluación de las herramientas scoring de azure y AWS.
7	Minitoreo-Dashboard	Presentar resultados de cumplimiento scoring por cada cliente.

Tabla 1: Procedimiento de Evaluación

Para la evaluación se realizó el cruce de los 3 frameworks, NIST 800-53 con 20 familias de controles Moderado y Bajo, CIS control versión 8 con 18 controles e ISO 27001:2022 con 93 controles:

Cis Control cuenta con 153 Salvaguardas agrupadas en 18 controles con un enfoque de protección primaria y línea base de ciberdefensa.

La Iso 2701:2022 cubre 93 controles de los cuales 49 son homologables con el framework base CIS y 44 controles organizativos asociados a políticas, procesos y procedimientos documentados. Mas enfocada en establecer, implementa, mantiene y mejora continuamente un SGSI.

Para los controles NIST 800-53 de las 20 agrupaciones, 18 son homologables con controles CIS, aplicando a 219 controles. proporciona un marco global para la gestión de los riesgos de seguridad y privacidad la información.

ID CONTROL	CONTROL CIS V8	CONTROL CIS V8 DISPONIBLES	SUMA CONTROLES CIS	MAPEADOS ISO 27001:2022	NO MAPEADOS ISO 27001:2022	MAPEADOS NIST 800-53	NO MAPEADOS NIST 800-53
1	**Inventario y control de los activos de la empresa**	*1.1, 1.2, 1.3, 1.4, 1.5*	*5*	1.1 Con (A5.9,A8.8)	1.2, 1.3, 1.4, 1.5	1.1(CM8,CM(1),PM5) 1.2 (CM8(3)) 1.3(SI4) 1.4(CM8(3)) 1.5(SI(4)	*N/A*

2	**Inventario y control de activos de software**	*2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7*	*7*	*2.1(A5.9)* *2.5(A8.7,A8.19)* *2.6(A8.19)*	*2.2, 2.3, 2.4 y 2.7*	*2.1(CM-8)* *2.2(CM-7(1),MA-3 y SA-22)* *2.3(CM-7(2),CM-8(3),CM-10 y CM-11)* *2.4(CM-8(3))* *2.5(CM-7(5),CM-10)* *2.6(CM-7)* *2.7(CM-7(1),CM-7,SI-7 ySI-7(1))*	*N/A*
3	**Protección de datos**	*3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7,3.8,3,9,3.10,3.11, 3.12,3.13,3.14*	*14*	*3.1(A5.10,A5.9,A8.1)* *3.2(A5.9)* *3.3(A5.10,A5.15,A8.3,A8.4)* *3.4(A5.33)* *3.5(A5.10)* *3.6(A6.7,A8.1)* *3.7(A5.9,A5.12,A5.13,A5.33,A8.12)* *3.8(A5.14)* *3.9(A5.14)* *3.10(A5.14)* *3.11(A5.33)* *3.12 (A8.20,A8.22)* *3.13 (A5.14,A8.12,A8.15)* *3.14 (A8.15)*	*N/A*	*3.1(AU-11,CM-12 Y SI-12)* *3.2(CM-12,PM-5(1) Y RA-2)* *3.3(AC-3,AC-5,AC-6 Y MP-2)* *3.4(AU-11, SI-12)* *3.5(MP-6, SR-12)* *3.6(SC-28)* *3.7(RA-2)* *3.8(AC-4,CM-12)* *3.9(MP-5 Y MP-7)* *3.10(AC-17(2),IA-5,IA-5(1),SC-8 Y SC-8(1))* *3.11(IA-5(1),SC-28 Y SC-28(1))* *3.13 (CA-7,CM-12,CM-12(1) YSC-4)* *3.14(AC-6(9),AU-2,AU-12)*	*3.12*
4	**Configuración segura de los activos y el software de la empresa**	*4.1, 4.2, 4.3, 4.4, 4.5,4.6, 4.7,4.8,4,9,4.10,4.11, 4.12*	*12*	*4.1(A8.1 YA8.9)* *4.2(A8.9)* *4.3(A8.5 Y A8.9)* *4.5(A6.7 Y A8.1)* *4.7 (A8.2 Y A8.9)* *4.8 (A8.9)* *4.10(A8.5)* *4.11(A8.1, A8.10)* *4.12(A6.7, A8.1)*	*4.4, 4.6 Y 4.9*	*4.1(CM-1, CM-2,CM-6,CM-7,CM-7(1),CM-9,SA-3,SA-8,SA-10)* *4.2(AC-18,AC-18(1),AC-18(3),CM-2,CM-6,CM-7,CM-7(1),CM-9* *4.3(AC-2(5),AC-11,AC-11(1) y AC-12)* *4.4(CA-9)* *4.5(SC-7 ySC-7(5))* *4.6(MA-4)* *4.7(IA-5)* *4.8(CM-6 y CM-7)* *4.9(SC-20,SC-21 y SC-22)* *4.10(AC-7 y AC-19)* *4.11(AC-19, AC-20)* *4.12(AC-19(5) y SC-39)*	*N/A*
5	**Gestión de cuentas**	*5.1, 5.2, 5.3, 5.4, 5.5, 5.6*	*6*	*5.1(A5.16)* *5.2(A5.17)* *5.4(A5.15, A8.2)* *5.5(A5.15,A8.18)* *5.6 (A5.15)*	*5.3*	*5.1(AC-2)* *5.2(IA-5(1))* *5.3(AC-2(3))* *5.4(AC-6(2), AC-6(5))* *5.5(AC-2)* *5.6(AC-2(1))*	*N/A*
6	***Gestión del control de acceso***	*6.1, 6.2, 6.3, 6.4, 6.5,6.6, 6.7,6.8*	*8*	*6.1(A5.15,A5.16,A5.18)* *6.2(A5.16, A5.18, A6.5)* *6.3(A5.15)* *6.4(A6.7)* *6.5(A8.2)* *6.6(A8.5)* *6.7(A5.18)* *6.8(A5.3,A5.15,A8.2,A8.3)*	*N/A*	*6.1(IA-4,IA-5,AC-1,AC-2,AC-2(1))* *6.2(AC-1,AC-2,AC-2(1))* *6.3(IA-2(1),IA-2(2))* *6.4(AC-19,IA-2(1),IA-2(2))* *6.5(IA-2(1))* *6.6(CM-8,IA-8(2))* *6.7(AC-2(1),AC-3)* *6.8(AC-6,AC-6(1),AC-6(7),AU-9(4))*	*N/A*

7	**Gestión Contínua de Vulnerabilidades**	*7.1, 7.2, 7.3, 7.4, 7.5,7.6, 7.7*	*7*	*7.1(A8.8)* *7.2(A8.8)* *7.3(A8.8)* *7.4(A8.8)* *7.5(A8.8)* *7.6(A8.8)* *7.7(A8.8)*	*N/A*	*7.1(RA-5)* *7.2(RA-5)* *7.3(RA-5,SI-2,RA-5)* *7.4(RA-7,SI-2(2),RA-7,SI-2,SI-2(2))* *7.5(RA-5)* *7.6(RA-5)* *7.7(RA-5,RA-5(2),RA-7 y SI-2)*	*N/A*
8	**Gestión de registros de auditoría**	*8.1, 8.2, 8.3, 8.4,8.5,8.6, 8.7,8.8,8,9,8.10,8.11, 8.12*	*12*	*8.1(A8.15)* *8.2(A8.15,A8.20)* *8.3(A8.6)* *8.4(A8.17)* *8.5(A5.28,A8.15)* *8.8(A8.15)* *8.10(A5.28)* *8.11(A5.25)*	*8.6* *8.7* *8.9* *8.12*	*8.1(AU-1,AU-2)* *8.2(AU-2,AU-7,AU-12)* *8.3(AU-4)* *8.4(AU-8)* *8.5(AU-3,AU-3(1),AU-7,AU-12)* *8.6(AU-2)* *8.7(AU-2)* *8.8(AU-2)* *8,9(AU-6(3))* *8.10(AU-11)* *8.11(AU-6,AU-6(1),AU-7(1))* *8.12(AU-2)*	*N/A*
9	**Protección del correo electrónico y los navegadores web**	*9.1, 9.2, 9.3, 9.4,9.5,9.6, 9.7*	*7*	*9.1(A8.1)* *9.2(A8.23)* *9.3(A8.7,A8.23)* *9.7(A8.7)*	*9.4* *9.5* *9.6*	*9.1(CM-10,SC-18)* *9.2(SI-8)* *9.3(SC-7(3),SC-7(4))* *9.4(CM-10,CM-11,SC-18)* *9.5(SC-7)* *9.6(SI-3,SI-8)* *9.7(SI-3,SI-8)*	*N/A*
10	**Defensas contra malware**	*10.1,10.2,10.3,10.4,10.5,10.6,10.7*	*7*	*10.1(A8.1,A8.7)* *10.2(A8.7)* *10.4(A8.7)* *10.5(A8.7)* *10.6(A8.7)* *10.7(A8.1,A8.7)*	*10.3*	*10.1(SI-3)* *10.2(SI-3)* *10.3(MP-7)* *10.4(MP-7,SI-3)* *10.5(SI-16)* *10.6(SI-3)* *10.7(SI-4)*	*N/A*
11	**Recuperación de datos**	*11.1,11.2,11.3,11.4,11.5*	*5*	*11.1(A8.13)* *11.2(A8.13)* *11.3(A8.12,A8.13)* *11.4(A8.13)* *11.5(A8.13)*	*N/A*	*11.1(CP-2,CP-10)* *11.2(CP-9,CP-10)* *11.3(CP-9,CP-9(8),SC-28)* *11.4(CP-6,CP-6(1))* *11.5(CP-4,CP-9(1))*	*N/A*

12	**Gestión de infraestructuras de red**	*12.1,12.2,12.3,12.4,12.5,12.6,12.7,12.8*	*8*	*12.2(A8.22,A8.27)* *12.3(A8.20,A8.21)* *12.7(A6.7,A8.1,A8.1)* *12.8(A8.2,A8.22)*	*12.1* *12.4* *12.5* *12.6*	*12.1(CM-8(1))* *12.2(PL-8,PM-7,SA-8,CM-7,CP-6,CP-7,SC-7)* *12.3(CM-6,CM-7,SC-23)* *12.4(PL-8,PM-5)* *12.5(AC-2(1))* *12.6(AC-18,SC-23)* *12.7(AC-17,AC-17(1),AC-17(3))*	*12.8*
13	**Supervisión y defensa de redes**	*13.1,13.2,13.3,13.4,13.5,13.6,13.7,13.8, 13.9, 13.10, 13,11*	*11*	*13.1(A8.15)* *13.2(A8.16)* *13.3(A8.16)* *13.4(A8.16,A8.22)* *13.5(A6.7,A8.1,A8.3)* *13.6(A8.15,A8.16)* *13.7(A8.8)* *13.8(A8.8)* *13.9(A8.8)* *13.10(A8.8)*	*13.11*	*13.1(AU-6(1),AU-7,IR-4(1),SI-4(2),SI-4(5))* *13.3(SI-4,SI-4(4))* *13.4(CA-9,SC-7)* *13.5(CA-9,SC-7,AC-17,AC-17(1),SI-4, SC-7)* *13.6(SI-4,SI-4(4))* *13.8(SI-4,SI-4(4))* *13.9(CM-6,CM-7)* *13.10(SC-7(8))* *13.11(SI-4)*	*13.2* *13.7*
14	**Concienciación y formación en materia de seguridad**	*14.1,14.2,14.3,14.4,14.5,14.6,14.7,14.8,14.9*	*9*	*14.1(A6.3)* *14.2(A8.7)* *14.4(A5.10)* *14.5(A6.3)* *14.6(A6.3,A6.8)* *14.7(A6.3)* *14.8(A6.3)* *14.9(A6.3)*	*14.3*	*14.1(AT-1,AT-2,PM-13)* *14.2(AT-2(3),)* *14.3(AT-2)* *14.4(AT-2)* *14.5(AC-22)* *14.6(AT-2)* *14.7(AT-2)* *14.8(AT-2)* *14.9(AT-3)*	
15	**Gestión de proveedores de servicios**	15.1,15.2,15.3,15.4,15.5,15.6,15.7	*7*	15.1(A5.19) 15.2(A5.1,A5.10,A5.10,A5.19,A5.20,A5.23) 15.3(A5.19) 15.4(A5.14,A5.20,A5.21,A5.23) 15.5(A5.19,A5.22,A5.23) 15.6(A5.19,A5.20,A5.22,A5.21) 15.7(A5.19,A5.20)	*N/A*	15.1(PM-30(1)) 15.2(AC-21,SA-9,SA-9(2),PM-30,SR-1,) 15.3(AC-20,SR-6,) 15.4(AC-20(1),AC-20(2),PM-17,SR-5) 15.5(SA-4,SR-5,SR-6,) 15.6(AC-20(1),SI-4,SR-6)	*15.7*

16	**Seguridad del software de aplicación**	*16.1, 16.2, 16.3, 16.4,16.5,16.6, 16.7,16.8,16,9,16.10, 16.11,16.12, 16.13, 16.14*	*14*	*16.1(A5.8,A8.4,A8.25,A 8.28,)* *16.2(A8.8)* *16.3 (A8.8)* *16.4(A8.26,A8.30)* *16.5(A8.26,)* *16.6(A8.8)* *16.7(A8.8)* *16.8(A8.31)* *16,9 (A8.28)* *16.10 (A8.27)* *16.11(A8.25,A8.26)* *16.12 (A8.25,A8.28,A8.29)* *16.13(A8.8,A8.29)* *16.14(A8.29)*		*16.1(SA-3,SA-15)* *16.2(CA-5,RA-1,RA-5,RA-7)* *16.3(SI-2)* *16.4(CM-8)* *16.5(SR-11)* *16.6(RA-5)* *16.7(CM-6,CM-7)* *16,9(SA-8)* *16.10(PL-8,SA-8)* *16.11(SA-15)* *16.12(SA-11,SA-15)*	*16.8* *16.13* *16.14*
17	**Gestión de la respuesta a incidentes**	17.1, 17.2, 17.3, 17.4,17.5,17.6, 17.7,17.8,17.9	9	17.1(A5.24) 17.2(A5.5,A5.6,A5.20, A5.24) 17.3(A6.8) 17.4(A5.24,A5.26) 17.5(A5.2,A5.24) 17.6(A5.24) 17.7(A5.30) 17.8(A5.24,A5.27) 17.9(A5.24,A5.25)		17.1(IR-1,IR-7,IR-8) 17.2(IR-6,IR-6,IR-6(3)) 17.3(IR-5,IR-6,IR-6(1),IR-8) 17.4(IR-1,IR-6(1),IR-6,IR-6(1),IR-8) 17.5(IR-1,IR-8,CP-8) 17.6(IR-8) 17.7(IR-3) 17.8(8) 17.9(IR-6,IR-8)	
18	**Pruebas de penetración**	18.1, 18.2, 18.3, 18.4,18.5	5	18.1(A8.8) 18.2(A8.8) 18.3(A8.8) 18.4(A8.8) 18.5(A8.8)		NO CUBIERTO	*18.1* *18.2* *18.3* *18.4* *18.5*

Tabla 2: Comparación Controles NITS/CIS/ISO27001

La estrategia de comparación consiste en identificar todos los aspectos dentro de un Control e intentar establecer si ambos elementos afirman exactamente lo mismo. Se toma como base el Framework CISv8 teniendo en cuenta su practicidad, aplicabilidad y uso frecuente en entornos cloud.

Del proceso de cruce de los tres frameworks se identifica:

- Que se tiene 26 salvaguardas en CISv8 que no corresponden con la norma ISO/IEC 27001.2022, principalmente asociados a CIS 1, Inventario y control de los activos de la empresa, CIS2, Inventario y control de los activos de la empresa, CIS 4 Configuración segura de los activos y el software de la empresa, CIS 8 Registros de Auditoria y CIS 12, Gestión de infraestructuras de red.

- Que existen 33 controles de la norma ISO27001:2022 no mapeados en CIS Control v8, dentro de ellos se tienen los controles A5, A6, A7 y A8.

- Que hay 13 salvaguarda de CISv8 que no se han adaptado a la norma NIST SP 800-53, principalmente los relacionados con CIS 13 Supervisión y defensa de redes, CIS 16 Seguridad del software de aplicación y CIS 18 Pruebas de penetración.

- Que existen 203 controles de la línea de base NIST SP 800-53 MODERATE y BAJA que no están asignados a los controles CIS v8, principalmente los relacionados con AC, CA,CM, CP,IA,PM, PT y SR.

- Que CIS control cuenta con 55 Salvaguardas no técnicos asociados definición de políticas, procesos, procedimientos y programas en seguridad de la información.

- Que de acuerdo con las funciones NIST se identifican en CISv8 47 salvaguardas, para proteger 211 salvaguardas, para detectar 41 salvaguardas, para responder 33 salvaguarda y para recuperar 13 salvaguardas demostrando el mayor enfoque las actividades preventivas y defensa contra ataques cibernéticos.

Principales Diferencias entre frameworks:

ITEM	CIS v8	NIST	ISO
Descripción	Conjunto de acciones recomendadas para la ciberdefensa que proporcionan formas específicas y procesables de detener los ataques más generalizados y peligrosos de la actualidad.	Un marco reconocido que contiene controles de seguridad y privacidad para que los sistemas de información y las organizaciones protejan las operaciones y los activos de la organización con el objetivo de gestionar eficazmente los riesgos.	Norma reconocida internacionalmente que describe cómo gestionar la seguridad de la información en una organización.
Objetivos organizaciones	Proporcionar a las organizaciones un número más reducido y prioritario de controles. En lugar de implantar docenas de controles, este enfoque priorizado ayudará a las organizaciones a centrarse primero en lo que es importante para establecer una base de protección y ciberdefensa.	Se creó principalmente creado para ayudar agencias federales estadounidenses	Se puede implementado en cualquier tipo de organización, con o sin ánimo lucro, privada o estatal propiedad, pequeña o grande
Estructura	Contiene 18 controles agrupados en 3 grupos de higiene (G1,G2, G3 Madurez TI y administración)	La última versión del NIST 800-53, Revisión 5, contiene 1.189 controles individuales organizados en 20 familias de control.	La última versión ISO 27001:2022 costa de 93 controles agrupados en 4 frentes, Organizativos, Personas, Físicos y Tecnológicos
Enfoque de gestión de riesgos	Básico, centrado en áreas críticas	Amplia y detallada gestión de riesgos	Marco estructurado de gestión de riesgos
Complejidad	Baja, sencilla y práctica	Alta, muy detallada y extensa	Moderada, requiere documentación y pruebas
Certificación	Los controles CIS son ideales para las organizaciones que buscan controles de seguridad prácticos y aplicables sin necesidad de una certificación formal.	Es esencial para las agencias federales y contratistas de EE.UU. que necesitan cumplir con FISMA y otros requisitos federales.	La norma ISO 27001 es la más adecuada para las organizaciones que buscan una certificación formal para demostrar su compromiso con la gestión de la seguridad de la información.
Actualizaciones	Actualizaciones periódicas basadas en el panorama de amenazas.	Actualizaciones periódicas	Actualizadas periódicamente
Usabilidad en entornos Cloud	Alta, diseñada para ser práctica, uso frecuente en entornos cloud	Práctica Alta, muy detallada para entornos de nube	Moderada, puede adaptarse a la seguridad en la nube

Tabla 3: Diferencias Nist/CIS/ISO 27001

VIII. IMPLEMENTACIÓN DE LA HERRAMIENTA

Una vez definido el framework unificado se cruza con los resultados de defender con cloud para el caso de Azure de Security HUB para el caso de AWS:

En AWS, Security Hub reporta las vulnerabilidades asociando varios controles NIST. Para modelar el radar de brechas, si una vulnerabilidad se aplica a tres o más salvaguardas dentro de un mismo control, se sumará en ese control específico:

Security groups should not allow unrestricted access to ports with high risk	AC-4	AC-4(21)	CA-9(1)	CM-2	CM-2(2)	CM-7	SC-7	SC-7(11)	SC-7(16)	SC-7(21)
Hardware MFA should be enabled for the root user	AC-2(1)	AC-3(15)	IA-2(1)	IA-2(2)	IA-2(6)	IA-2(8)				
EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	AC-3	AC-3(15)	AC-3(7)	AC-6						
Security groups should only allow unrestricted incoming traffic for authorized ports	AC-4	AC-4(21)	SC-7	SC-7(11)	SC-7(16)	SC-7(21)	SC-7(4)	SC-7(5)		
Security groups should not allow ingress from 0.0.0.0/0 or ::/0 to port 22	AC-4	AC-4(21)	CM-7	SC-7	SC-7(11)	SC-7(16)	SC-7(21)	SC-7(4)	SC-7(5)	
S3 general purpose buckets should block public access	AC-21	AC-3	AC-3(7)	AC-4	AC-4(21)	AC-6	SC-7	SC-7(11)	SC-7(16)	SC-7(20)
EC2 instances should not have a public IPv4 address	AC-21	AC-3	AC-3(7)	AC-4	AC-4(21)	AC-6	SC-7	SC-7(11)	SC-7(16)	SC-7(20)
VPC default security groups should not allow inbound or outbound traffic	AC-4	AC-4(21)	SC-7	SC-7(11)	SC-7(16)	SC-7(21)	SC-7(4)	SC-7(5)		
EC2 launch templates should not assign public IPs to network interfaces	AC-21	AC-3	AC-3(7)	AC-4	AC-4(21)	AC-6	SC-7	SC-7(11)	SC-7(16)	SC-7(20)

Tabla 4: Vulnerabilidades AWS – Security HUB

En Azure, Microsoft Defender for Cloud realiza una agrupación personalizada de controles (Ejemplo: NS Network Security, IM Identity Management), basada en las mejores prácticas de NIST. Esta agrupación es homologable con los controles CIS v8. Para cruzar esta agrupación con el marco personalizado propuesto, se establece una correspondencia entre la nomenclatura utilizada por Azure y la agrupación de salvaguardas coincidentes como lo muestra la siguiente tabla:

NOMENCLATURA	AGRUPACIÓN
NS.	Network Security
IM.	Identity Management
PA.	Privileged Access
DP.	Data Protection
AM.	Asset Management
LT.	Logging and Threat Detection
IR.	Incident Response

Tabla 5: Agrupación Vulnerabilidades *Azure – Defender for cloud*

Una vez realizado el cruce de hallazgos de las nubes con el framework unificado, se revisan las brechas y se actualizan los dashboards. Estos se ajustan según los cambios, remediaciones y nuevos recursos desplegados en las cargas de trabajo en ambas nubes.

Para lograr ello, es necesario realizar una adecuada conexión entre PowerBI y la fuente de datos:

Configuración AWS:
Para sincronizar Power BI con la fuente de datos AWS, se utilizan los siguientes componentes:

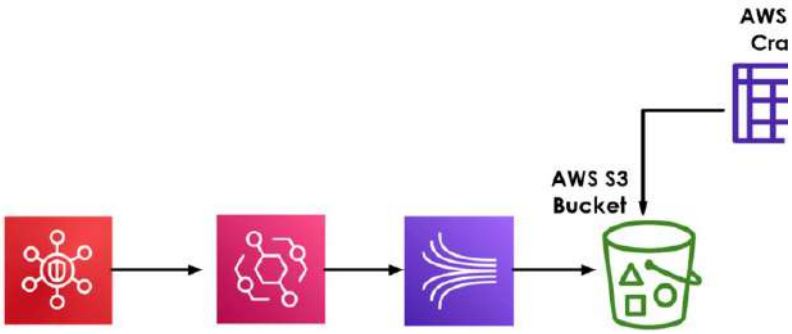
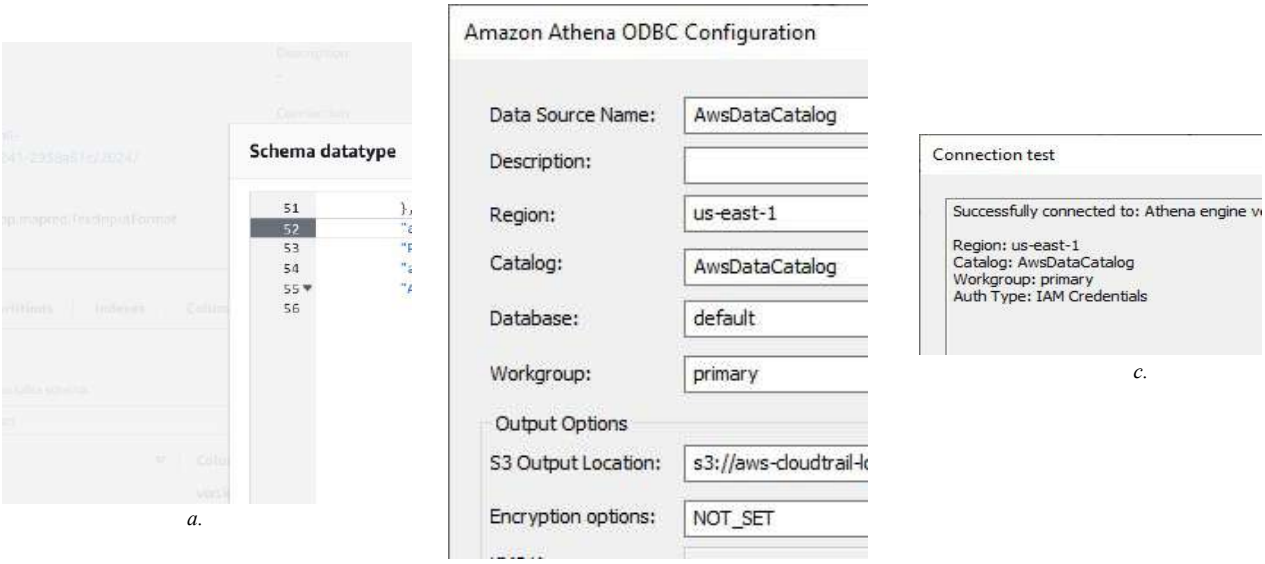


Imagen 4: Conector y Recursos Cloud Azure - AWS

Se activa AWS Security Hub para realizar la evaluación de seguridad. Luego, los eventos se enrutan a través de EventBridge y se entregan a Kinesis Firehose para permitir la adquisición, transformación y entrega de secuencias de datos en tiempo real, presentandolos en archivos JSON. Estos archivos se guardan en un bucket S3, permitiendo que recursos como AWS Glue y AWS Data Catalog integren y estructuren los datos. Posteriormente, mediante Athena, se crea el conector ODBC para la conexión, análisis y presentación de datos en Power BI.



a. *b.* *c.*

Imagen 5: Conexión Power BI – AWS: a. Imagen Kinesis, b. Conexión Athena, c. Conexión PBI.

Configuración Azure:
Para sincronizar Power BI con la fuente de datos de Azure, se utilizan los siguientes componentes:

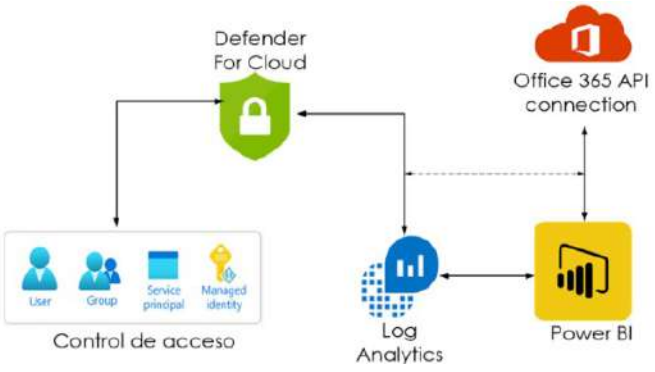


Imagen 6: Conexión Power BI - AZURE.

Se activa Azure Defender for Cloud en la suscripción seleccionada y se verifica la disponibilidad de los datos de evaluación de seguridad para su exportación a Power BI. Es fundamental contar con permisos administrativos en la suscripción de Azure, dado que Azure Defender for Cloud guarda estos datos en un Log Analytics Workspace. Una vez que los datos se hayan exportado correctamente a Log Analytics, se podrá conectar Power BI mediante la URL: https://<myworkspace-name>.ods.opinsights.azure.com. Después de esto, se modelan y crean visualizaciones que muestren los hallazgos de vulnerabilidades para cada recurso y se presentar los datos.

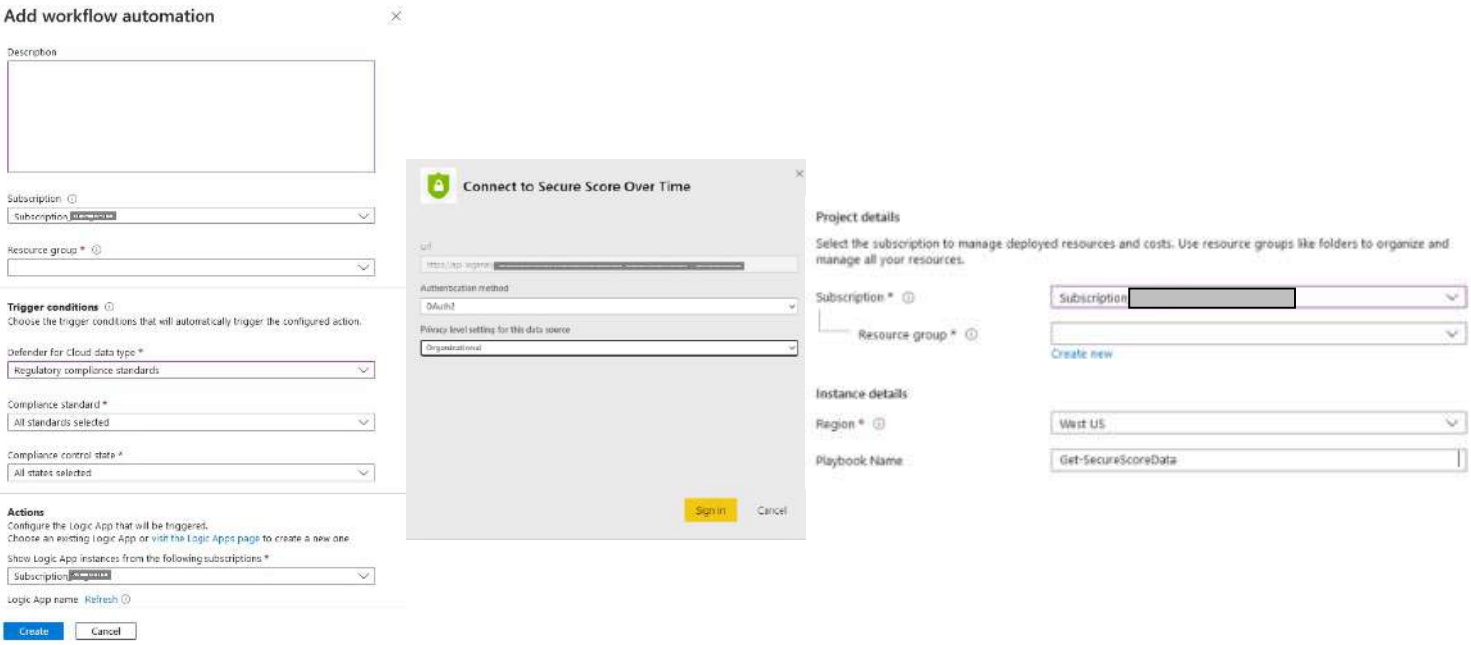


Imagen 7: Conexión Power BI – Azure Componente Log Analytics y Conexión API

Presentación de datos:
Radares en dashboard unificado para los dos clientes:

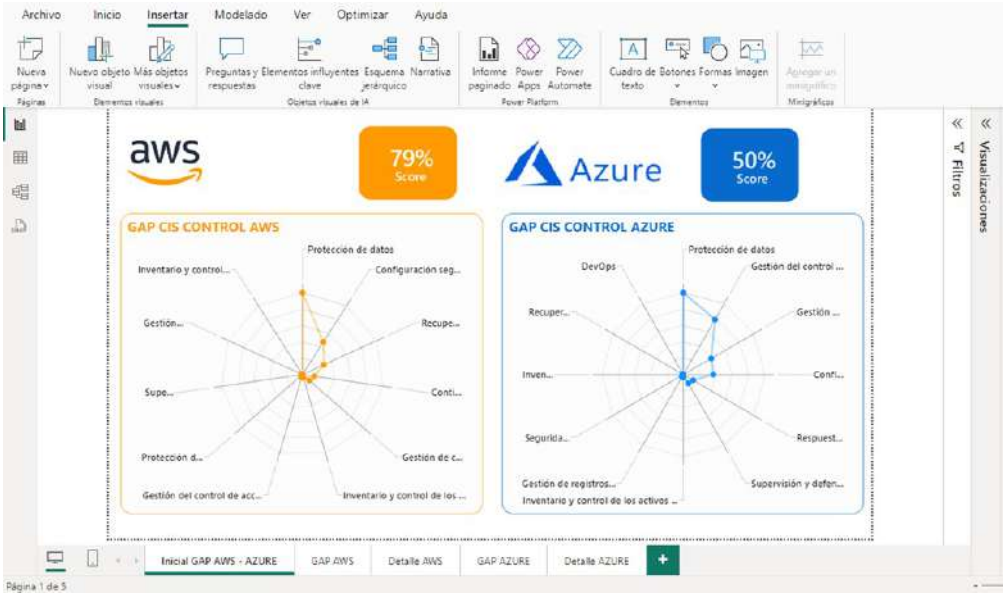


Imagen 8: *Radares con las brechas*

Detalle resultados AWS, se presenta score de seguridad Criticidad, cantidad de hallazgos y recomendación de remediación:

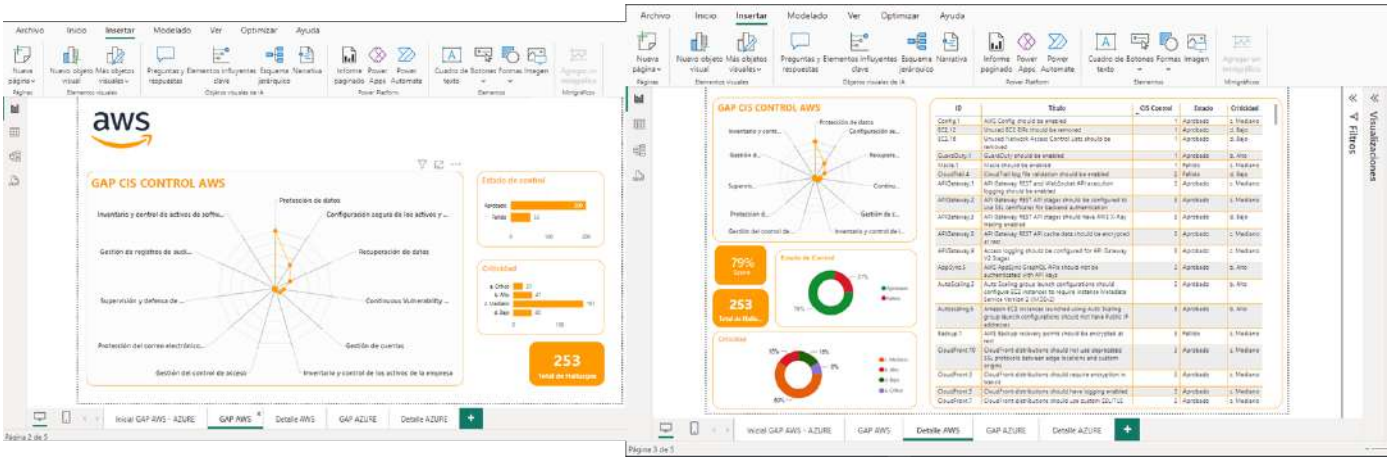


Imagen 9: *Detalle hallazgos AWS*

El score de seguridad se calcula tomando como 100% la cobertura de los hallazgos en cada control en estado Aprobado**.**

Detalle resultados AZURE, se presenta score de seguridad Criticidad, cantidad de hallazgos y recomendación de remediación:

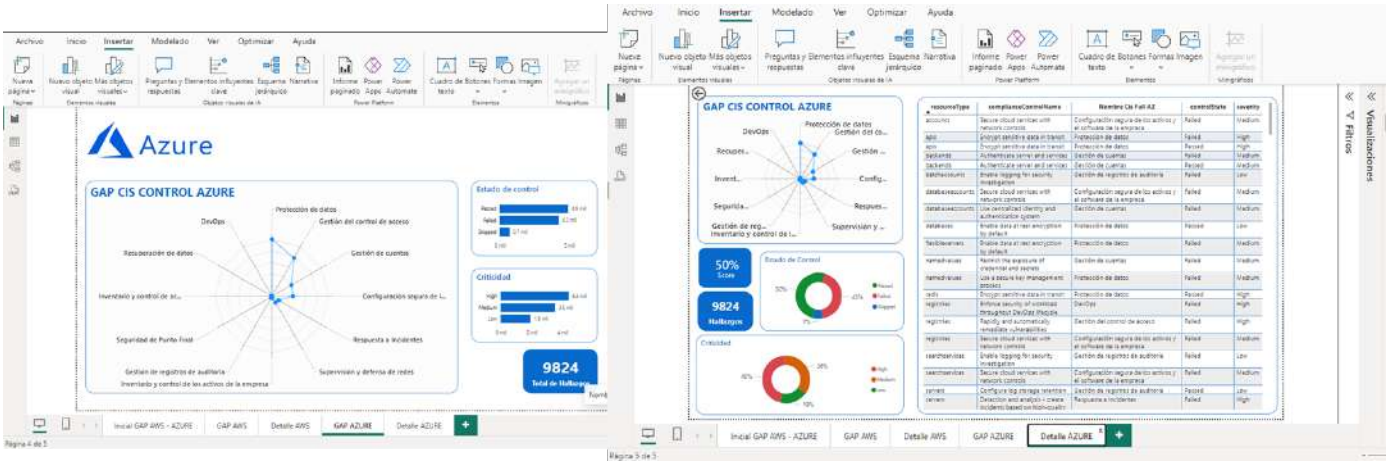


Imagen 10: Detalle hallazgos AWS

El score de seguridad se calcula tomando como 100% la cobertura de los hallazgos en cada control en estado "Passed"**.**

IX. RESULTADOS Y ANÁLISIS

- Para los hallazgos de Vulnerabilidades de Azure, los ítems de cis control 3,4,5 y 6 son los de mayor peso, representando:

CONTROL	% Hallazgos Azure
3	34,2%
4	12,6%
5	13,5%
6	26,6%

Tabla 6: Porcentaje adherencia controles Azure

- Para los hallazgos de Vulnerabilidades de AWS, los ítems de cis control 3,4,11 y 7 son los de mayor peso representando:

Control	% hallazgos AWS
3	46,60%
4	22,10%
11	13,40%
7	6,70%

Tabla 7: Porcentaje adherencia controles AWS

- El estado de 690 Hallazgos de Azure que corresponden al 7% de la totalidad fueron no testeados, generando un nuevo estado (Skipped) diferente satisfactorios y fallidos como los agrupa AWS. Para las acciones posteriores en una segunda fase, será necesario validar o identificar la forma de retestearlos.

- El framework unificado es ideal para los clientes de la empresa BPO, que buscan controles de seguridad prácticos y aplicables sin necesidad de una certificación formal.

- El framework unificado proporciona a empresa un número más reducido y prioritario de controles, permitiendo priorizar de mejor forma los hallazgos.

X. RECOMENDACIONES

Para asegurar la continuidad del proyecto de implementación, es esencial centrarse en varios componentes clave que abordan el licenciamiento y los costos asociados, dentro de ellos se tiene:

El licenciamiento de Power BI es crucial para garantizar que todos los usuarios tengan acceso a las capacidades analíticas avanzadas necesarias para evaluar la postura de seguridad. Se recomienda adquirir licencias adecuadas para todos los usuarios involucrados en el análisis y la toma de decisiones. Además, es beneficioso optar por la versión Pro o Premium de Power BI, que ofrece capacidades mejoradas para la colaboración, almacenamiento de datos y actualizaciones automáticas de informes, lo cual es fundamental para mantener la información de seguridad actualizada y accesible.

Los correlacionadores de eventos ayudan a identificar patrones y anomalías en el tráfico de red y eventos de seguridad, lo que permite una detección más rápida y precisa de amenazas potenciales. Se recomienda integrar herramientas como Azure Sentinel y Amazon Detective, que ofrecen capacidades robustas de SIEM (Security Information and Event Management) y SOAR (Security Orchestration, Automation, and Response). Esto no solo mejora la capacidad de respuesta a incidentes, sino que también proporciona un contexto más rico para la evaluación de la postura de seguridad.

Autorizar y controlar los costos asociados al tráfico de red, ingesta de logs, analítica y retención de información, esto es fundamental para garantizar la eficacia y continuidad del proyecto. Los recursos deben configurarse para ser escalables y adaptables a variaciones en el volumen de datos y la carga de trabajo, asegurando que la infraestructura de seguridad de la organización pueda responder de manera efectiva a cualquier amenaza o incidente.

Incluir servicio en el modelo económico por cada cliente. Para monetizar el proyecto, se propone la creación de un nuevo paquete de servicios para gestionar la postura de seguridad que sea incluido por cada cliente en las próximas renovaciones de contrato e incluido en el portafolio de servicios integrales de TI.

XI. REFERENCIAS

[1] ISO/IEC 27001:2013
Http://siso.org/contents/data/standard
Consultado: 03/03/2024 a 15/05/2024
[2] CIS Control v8, https://www.cisecurity.org/controls
Consultado: 03/03/2024 a 15/05/2024
[3] NIST 800-53
https://www.stigviewer.com/controls/800-53
Consultado: : 03/03/2024 a 15/05/2024
[4] Integración PowerBI,

https://learn.microsoft.com/es-es/power-pages/admin/set-up-power-bi-integration
Consultado: 03/03/2024 a 15/05/2024