FORTALECIMIENTO DE LA SEGURIDAD DEL SOC: DIAGNÓSTICO Y PLAN DE ACCIÓN

Luis Carlos Guerrero Contreras
Universidad de los Andes
Bogotá, Colombia
l.guerreroc@uniandes.edu.co

Javier Merchan
Universidad de los Andes
Bogotá, Colombia
j.merchang@uniandes.edu.co

***Abstract*— ACME SAS, consultora en ciberseguridad, enfrenta desafíos para alinear su nuevo Centro de Operaciones de Seguridad (SOC) con estándares internacionales. Este trabajo propone un plan de acción basado en la mejora de la ISO 27035 con la NIST 800-61 con un enfoque práctico para la gestión de incidentes. Mediante un análisis comparativo y un cuestionario asociado al modelo CMMI, se evaluó el estado actual del SOC, priorizando acciones críticas según su impacto estratégico y madurez operativa. El plan de mejora, con un plazo de seis meses, busca cerrar brechas, optimizar tiempos de respuesta, y fortalecer la resiliencia del SOC frente a amenazas cibernéticas. Estas mejoras no solo alinean las operaciones con mejores prácticas internacionales, sino que también mitigan riesgos financieros, protegen la continuidad del negocio y fortalecen la confianza de los clientes, posicionando a la empresa como un socio confiable en ciberseguridad.**

Keywords—SOC, NIST, ISO, Plan Mejora

I. INTRODUCCIÓN

ACME SAS es una consultora especializada en seguridad de la información y continuidad del negocio, que ofrece servicios de Centros de Operaciones de Seguridad (SOC) para apoyar a organizaciones en la mitigación de riesgos tecnológicos. La empresa proporciona monitoreo de activos, auditorías y consultoría de cumplimiento para asegurar la adherencia a normativas. Ha colaborado en proyectos clave como la implementación de sistemas de seguridad en el Poder Judicial y el desarrollo de sistemas de continuidad de negocio para el Ministerio de Hacienda y Crédito Público, enfocándose en soluciones personalizadas para proteger activos críticos frente a amenazas cibernéticas.

II. DEFINICIÓN PROBLEMA

ACME SAS, en su nuevo Centro de Operaciones de Seguridad (SOC), enfrenta desafíos para alinear sus operaciones con los estándares de la industria de ciberseguridad. La ausencia de procesos y procedimientos establecidos limita la capacidad del SOC para gestionar eficazmente los incidentes, lo que aumenta los tiempos de respuesta, retrasa la resolución de incidentes y eleva los riesgos de seguridad para la empresa y sus clientes. Alinear sus prácticas con marcos reconocidos como la ISO 27035 y la NIST 800-61 permitirá mejorar la detección, análisis y respuesta a incidentes, fortaleciendo la madurez y resiliencia en ciberseguridad.

III. JUSTIFICACIÓN DEL PROBLEMA

El problema identificado es la falta de alineación del SOC de ACME SAS con estándares de referencia y el impacto que esto ocasiona en la prestación del servicio a sus clientes, esto se justifica a través de varios aspectos claves que se explican a continuación:

A. Impacto en la continuidad del negocio

La falta de gestión adecuada de los incidentes de seguridad puede causar interrupciones en los servicios, pérdida de ingresos y daño reputacional, afectando la continuidad del negocio. Según IDC [1], el costo promedio de una hora de inactividad no planificada oscila entre $250,000 y $500,000 USD, destacando la importancia de una respuesta efectiva para mitigar riesgos operativos y financieros.

B. Fortalecimiento en la confianza

La entrega de informes asertivos y la respuesta efectiva a amenazas cibernéticas desde el SOC refuerzan la confianza interna y externa en la organización. Esto demuestra el compromiso con la protección de activos y la mitigación de riesgos, fortaleciendo relaciones comerciales. Según PwC [2], el 85% de los CEO consideran crucial que las empresas sean vistas como responsables de la seguridad cibernética de sus clientes, destacando la importancia de una gestión sólida y transparente.

C. Mejora continua en la respuesta a incidentes

Las organizaciones con capacidades maduras de respuesta a incidentes logran reducir costos y acelerar la recuperación. Según IBM [3], contar con un equipo de respuesta puede disminuir el costo promedio de una filtración de datos en $1.5M USD. Al implementar las guías de la ISO 27035 y NIST 800-61,

ACME SAS puede fortalecer su respuesta a incidentes, minimizando el impacto y las pérdidas financieras para la empresa y sus clientes.

D. Eficiencia Operativa

Los estudios [4] han demostrado que las organizaciones que utilizan herramientas integradas de gestión de incidentes experimentan una mayor eficiencia operativa y ganancias de productividad. Una investigación realizada por Forrester Consulting [5] encontró que las empresas que utilizan este tipo de herramientas reportaron un aumento del 25 % en la eficiencia y una reducción del 20 % en los tiempos de respuesta a incidentes. Al implementar una herramienta unificada de gestión de incidentes alineada con los estándares ISO 27035 y NIST SP 800-61, ACME SAS puede optimizar sus operaciones SOC, optimizar la utilización de recursos y ofrecer tiempos de respuesta a incidentes más rápidos, mejorando la eficiencia operativa general y la satisfacción del cliente.

E. Mitigación de riesgos

El costo promedio de una filtración de datos alcanza los 4,24 millones de dólares a nivel mundial [6]. Al alinearse con los estándares ISO 27035 y NIST 800-61, ACME SAS puede mitigar eficazmente los riesgos de ciberseguridad, reduciendo la probabilidad de ataques exitosos y minimizando su impacto. Estas medidas proactivas ayudan a prevenir pérdidas financieras, daños reputacionales y costosas filtraciones de datos.

F. Ventaja competitiva usando frames referenciales

En el entorno actual, la ciberseguridad es clave para elegir proveedores, con un 70% de empresas considerándola crucial según Deloitte [7]. Al cumplir con las normas ISO 27035 y NIST 800-61, ACME SAS puede diferenciarse, generar confianza y obtener una ventaja competitiva, atrayendo más clientes y posicionándose como un socio confiable en ciberseguridad

IV. Propuesta de solución

A. Dominios ISO 27035

La gestión de incidentes de seguridad de la información es un pilar fundamental para garantizar la continuidad operativa y la resiliencia en las organizaciones modernas. En este contexto, la ISO 27035 se posiciona como un estándar internacional clave, ofreciendo un marco estructurado para abordar todas las etapas de un incidente, desde su planificación y detección hasta la recuperación y mejora continua. En el caso de ACME, este estándar ha sido implementado como base para SOC, destacando su enfoque sistemático y preventivo. A continuación, una breve descripción de los dominios [8].

- El primer dominio de la ISO 27035, Planificación y Preparación, establece la base para una gestión efectiva de incidentes de seguridad. Incluye la creación de políticas, procedimientos, y la formación de equipos especializados como el CSIRT, asegurando que la organización esté preparada para identificar, responder y gestionar incidentes de manera estructurada y eficiente. Este enfoque promueve la prevención y reduce el impacto de los incidentes en el negocio.
- El segundo dominio de la ISO 27035, Detección e Informe, se enfoca en la identificación temprana de incidentes y la comunicación oportuna a las partes relevantes. Incluye el establecimiento de herramientas, procedimientos y canales de reporte para garantizar que los eventos de seguridad sean detectados rápidamente y reportados de manera efectiva, facilitando una respuesta coordinada y minimizando el impacto en la organización.
- El tercer dominio de la ISO 27035, Evaluación y Decisión, aborda el análisis de los incidentes para determinar su alcance, impacto y la respuesta adecuada. Este dominio se centra en clasificar, priorizar y tomar decisiones informadas basadas en la naturaleza del incidente, asegurando una gestión eficiente y minimizando riesgos para la organización.
- El cuarto dominio de la ISO 27035, Respuesta, se enfoca en la contención, erradicación y recuperación frente a incidentes de seguridad. Este dominio asegura que las acciones sean rápidas y efectivas para limitar el impacto, eliminar amenazas y restaurar las operaciones normales, minimizando el daño a la organización y garantizando la continuidad del negocio
- El quinto dominio de la ISO 27035, Lecciones Aprendidas, se centra en analizar los incidentes gestionados para identificar áreas de mejora. Incluye la documentación de experiencias, la revisión de procedimientos y la implementación de ajustes para fortalecer la preparación y la respuesta futura, promoviendo la mejora continua y la resiliencia organizacional.

B. Mejora de la ISO 27035 basado en la NIST 800-61

La gestión de incidentes de seguridad de la información, estructurada en cinco dominios según la ISO 27035, constituye una base sólida para garantizar una respuesta efectiva y coordinada ante las amenazas emergentes. No obstante, la incorporación de las mejores prácticas del NIST 800-61 [9] aporta mejoras sustanciales a cada uno de estos dominios, proporcionando un enfoque más pragmático y detallado que complementa la visión estructural de la ISO. A continuación, describimos brevemente las mejoras por dominio.

- La fase de planificación y preparación en la gestión de incidentes, abordada por la ISO 27035 y la NIST 800-61, establece una base esencial para equipos de respuesta eficaces. Mientras que la ISO proporciona una estructura inicial para políticas y creación de CSIRTs, la NIST complementa con enfoques pragmáticos, como guías para medir efectividad, gestión de relaciones con terceros, coordinación regional y escenarios específicos de manejo de incidentes. Este enfoque integrado refuerza aspectos críticos como la moral del equipo, la relación

con otras áreas, y la preparación para incidentes complejos.

- El dominio de detección y reporte, clave para una gestión efectiva de incidentes, combina la estructura de la ISO 27035 con el enfoque práctico de la NIST 800-61. Ambos estándares enfatizan la detección temprana y el reporte oportuno, mientras que la NIST aporta herramientas como Jump Kits, evaluaciones de riesgo y SIEMs para mejorar la precisión y velocidad en la identificación de incidentes. Esto fortalece la capacidad del SOC para priorizar respuestas y minimizar impactos en la organización.
- El dominio de evaluación y decisión se centra en la gestión de incidentes, combina el enfoque estructurado de la ISO 27035 con la orientación práctica de la NIST 800-61. Este enfoque permite una clasificación precisa, priorización basada en impacto y una respuesta informada, utilizando herramientas como perfilamiento de equipos, correlación de eventos y análisis de logs. La integración de estos elementos fortalece la capacidad del SOC para minimizar impactos y garantizar la resiliencia organizacional.
- El dominio de contención, erradicación y recuperación integra la estructura de la ISO 27035 con el enfoque práctico de la NIST 800-61, priorizando estrategias específicas para cada tipo de incidente, como el uso de sandbox y la recolección forense de evidencia. Ambas normativas enfatizan restaurar operaciones con copias seguras, documentar cada acción y realizar pruebas periódicas para garantizar una respuesta efectiva y fortalecer la resiliencia organizacional.
- El dominio de lecciones aprendidas y mejora continua combina el análisis post-incidente de la ISO 27035 con las recomendaciones prácticas de la NIST 800-61, como la recopilación de datos clave y la realización de sesiones de retroalimentación. Este enfoque permite identificar áreas de mejora, ajustar políticas y procedimientos, y fortalecer la capacidad del SOC para prevenir y responder eficazmente a futuros incidentes.
- Adicionalmente la NIST provee unas guías, tablas, checklist que permiten mejorar la ISO. A continuación, una tabla con los artefactos usados de la NIST.

TABLE I. ARTEFACTOS NIST.

Artefactos	
Dominio	***Artefacto***
1	Elementos básicos de datos. (Lista con los campos básicos para manejar una incidencia).
1	Escenarios. (Lista con diferentes ejemplos de ciberataques o eventos para validar como es la respuesta a incidentes en cada uno)
1	Manejo de crisis.
2	Comunicación e instalaciones del gestor de incidentes.
2	Hardware y software del gestor de incidentes.
2	Recursos de análisis de incidencias.
3	Estatus Incidente.
3	Categorías de impacto funcional (capacidad de la organización para prestar un servicio a un usuario).
3	Categorías de impacto de la información (perdida o alteración de información sensible o confidencial).
3	Categorías de esfuerzo de recuperabilidad (si es o no posible recuperarse del ataque o evento).
4	Estrategia de contención.
4	Guías, para detectar el host atacante.
5	Tabla de control de manejo de incidentes (checklist).

C. Metodología para la mejora de la ISO 27035

La metodología presentada busca optimizar la gestión de incidentes en un SOC combinando las fortalezas de la ISO 27035 y la NIST 800-61. A través de un análisis comparativo, se identificaron oportunidades de mejora al integrar la estructura robusta de la ISO con el enfoque práctico y operativo de la NIST. Esto permitió establecer prácticas claras para preparación, respuesta y evaluación de incidentes. Se desarrolló un cuestionario para evaluar el estado actual del SOC, complementado con herramientas visuales como gráficos de araña que facilitan identificar brechas y priorizar mejoras, fortaleciendo la resiliencia y eficiencia del SOC frente a incidentes de seguridad.

D. Cuestionario

Con el objetivo de evaluar de manera integral el estado actual del Centro de Operaciones de Seguridad (SOC), se diseñó un cuestionario compuesto por 67 preguntas, elaborado a partir de una comparación detallada entre los estándares ISO 27035 y NIST 800-61. Este enfoque combinó la estructura metodológica de la ISO con el enfoque práctico y detallado del NIST, aprovechando los artefactos proporcionados por este último, como tablas, guías y checklists, para enriquecer el análisis y garantizar una cobertura exhaustiva de los aspectos clave de la gestión de incidentes.

El cuestionario resultante permite, a través de un proceso de socialización con los responsables del SOC, identificar con precisión el estado actual de sus capacidades y prácticas en gestión de incidentes. Este diagnóstico no solo proporciona un panorama claro de las fortalezas y debilidades del SOC, sino que también sirve como base para planificar un plan de mejora estructurado. Dicho plan se enfocará en cerrar las brechas identificadas, alineando al SOC con las mejores prácticas internacionales y fortaleciendo su capacidad de respuesta frente a amenazas en constante evolución.

TABLE II. CUESTIONARIO

Cuestionario	
Dominio	***Pregunta***
1	¿La política cuenta con misión, alcance y estructura del equipo?
1	¿Se cuenta con un método para medir la efectividad de dicha política?
1	¿Se establece un escalamiento con terceros dentro de la política o procedimientos?
2	¿Se ha revisado y aplicado el SCAP como guía para endurecer los hosts?
2	¿La empresa considera la incorporación de un Jump Kit como parte de su plan de respuesta a incidentes?
3	¿Con qué frecuencia se realizan revisiones de integridad mediante checksum en los archivos de equipos críticos monitoreados por el SOC?
3	¿Qué criterios se utilizan en el SOC para priorizar las incidencias detectadas y cómo se alinean con las recomendaciones de la NIST (Impacto en funcionalidad, impacto en la información, recuperabilidad)?
3	¿Cómo se lleva a cabo la correlación de eventos de diversas fuentes en el SOC y qué herramientas se utilizan para ello?
4	¿Se utiliza un entorno sandbox para analizar archivos sospechosos antes de proceder con la erradicación? ¿Cómo se integra este proceso en la respuesta general del SOC?
4	¿Cómo se asegura la correcta recolección de evidencia durante la respuesta a un incidente? ¿Se documentan aspectos como identificación, responsables, tiempo y ubicación?
4	¿Qué mecanismos se implementan para garantizar la validez de la evidencia a efectos legales?
5	¿Se realizan auditorías o evaluaciones externas para validar la efectividad de las acciones de mejora continua y lecciones aprendidas?
5	¿Qué herramientas o recursos adicionales se necesitan para detectar, analizar y mitigar incidentes futuros?
5	¿Qué procesos existen para documentar las acciones tomadas durante el manejo de incidentes y evaluar su efectividad?

E. Metodología para el análisis

Para evaluar el estado actual del SOC y realizar un análisis detallado, basados en el cuestionario anterior, cada pregunta específica fue cuantificada mediante los niveles de madurez del modelo CMMI para determinar la posición actual del SOC en términos de desarrollo y capacidades. Adicionalmente, para cada pregunta derivada del cuestionario, se consultó al cliente sobre la relevancia de cada aspecto para su negocio, evaluando su prioridad estratégica. La priorización de acciones se realizó utilizando la fórmula siguiente, donde "a" representa el nivel de madurez y "b" la relevancia para el negocio. Este enfoque permitió identificar las áreas de mayor impacto estratégico, garantizando que las mejoras propuestas estén alineadas con las necesidades del negocio, optimizando la eficacia del SOC y fortaleciendo su capacidad de respuesta ante incidentes de seguridad.

$$(6\text{-}a) * (2*b) = \text{Prioridad} \quad (1)$$

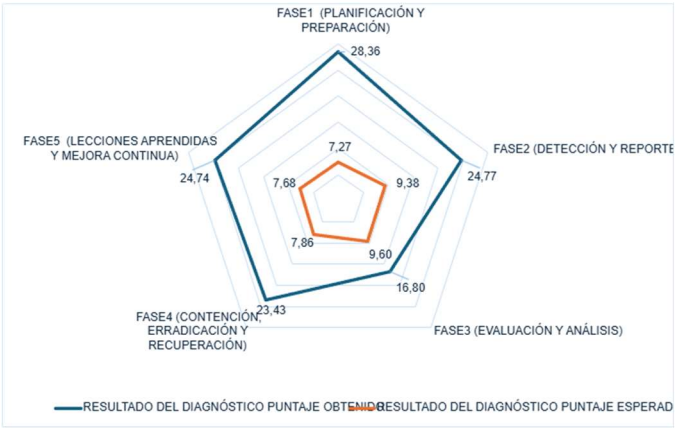
F. Herrramienta de análisis (Arañas)

Para garantizar la mejora continua del SOC, se desarrolló una herramienta diseñada para analizar su estado actual y priorizar las acciones necesarias para fortalecer sus capacidades. Esta herramienta permite evaluar cada actividad en función de dos factores clave: el nivel de madurez de seguridad basado en el modelo CMMI y la priorización estratégica definida por la organización. Este enfoque garantiza que los esfuerzos de mejora se enfoquen en las áreas de mayor impacto para el negocio.

La herramienta no solo identifica debilidades clave del SOC, sino que también facilita la priorización de actividades con alta importancia empresarial y baja madurez, permitiendo un análisis claro y orientado a la acción. Este proceso es esencial para formular un plan de mejora estructurado y alineado con las necesidades y objetivos estratégicos de la organización. Además, al integrar esta evaluación con el diagnóstico detallado de capacidades, se logra una visión integral que respalda la toma de decisiones y asegura la eficacia en la implementación de mejoras.

A continuación, se presenta la gráfica del diagnóstico:

FIGURA I: DIAGNÓSTICO ACTUAL



La gráfica de araña presentada utiliza dos colores para contrastar las prioridades por dominio del SOC. El color azul representa el puntaje obtenido tras aplicar la herramienta de evaluación, mientras que el color naranja muestra el estado esperado si el SOC alcanzara un nivel de madurez 5 según el modelo CMMI. Es importante destacar que esta gráfica no representa directamente el estado actual del SOC, sino que refleja las prioridades de acción: cuanto más alto es el puntaje en un dominio, mayor es la urgencia de implementar un plan de mejora en esa área. Por ejemplo, al promediar el valor de prioridad para las preguntas de la FASE 1 se obtuvo un puntaje global de 28,36, teniendo en cuenta que el puntaje objetivo es 7,27 (calificación CMMI en 5 para todas las preguntas) y que el peor puntaje posible a obtener es 43,63 (calificación CMMI en 0 para todas las preguntas) se puede establecer que actualmente la compañía va por la mitad aproximadamente del nivel de madurez deseado. La siguiente tabla muestra las valoraciones obtenidas para esta FASE 1 con el objetivo de entender cómo se llegan a los datos presentados anteriormente.

TABLE III. PUNTAJES FASE 1

Tabla puntajes obtenidos FASE 1			
Pregunta	***Calificación CMMI (A)***	***Priorización (B)***	***Prioridad (6-A*2*B)***
P1	**5**	**3**	**6**
P2	**5**	**3**	**6**
P3	**0**	**5**	**60**
P4	**5**	**2**	**4**
P5	**0**	**4**	**48**
P6	**2**	**5**	**40**
P7	**0**	**3**	**36**
P8	**3**	**3**	**18**
P9	**0**	**2**	**24**
P10	**3**	**5**	**30**
P11	**2**	**5**	**40**

Este contraste permite identificar claramente las brechas entre las prioridades actuales y el ideal de madurez, facilitando un análisis estratégico de los dominios que requieren atención inmediata. Con base en estos resultados, se puede estructurar un plan de mejora enfocado en fortalecer las capacidades críticas del SOC, alineándose con las necesidades de la organización y su visión estratégica de seguridad.

G. Plan Mejora

El plan de mejora del SOC se diseñó con un plazo de implementación de seis meses, garantizando un enfoque estratégico y medible para cerrar brechas en la gestión de incidentes de seguridad. Basándonos en la priorización obtenida mediante la metodología previamente descrita, identificamos los puntos críticos que requieren atención inmediata. Esta priorización permitió enfocar los esfuerzos en aquellas áreas que, además de tener mayor relevancia para el negocio, presentan niveles de madurez más bajos. El análisis destacó las acciones clave necesarias para abordar las deficiencias identificadas, asegurando que los recursos y el tiempo se inviertan de manera eficiente. Para transformar los resultados de la priorización obtenidos mediante el gráfico de arañas en un plan de mejora secuencial, se asignaron acciones concretas basadas en el análisis de brechas entre el estado actual y el estado objetivo. Cada pregunta del cuestionario incluye una acción implícita por desarrollar, la cual fue clasificada según su criticidad e impacto en el negocio. Esto permitió estructurar un plan de mejora compuesto por iniciativas secuenciales, priorizando aquellas de mayor relevancia para la organización, por ejemplo, la primera actividad definida en el plan: *Establecer un indicador al menos para medir la eficacia de la política*, era la acción asociada a la pregunta No 3 de la Fase 1: *¿Se cuenta con un método para medir la efectividad de dicha política?* Que como se puede observar en la TABLE III tiene una calificación CMMI de 0 y una priorización 5 convirtiéndola en la actividad más crítica y de mayor valor para la organización. Este enfoque asegura una implementación progresiva y alineada con los objetivos estratégicos del SOC. De esta manera, el plan no solo busca cerrar brechas específicas, sino también fortalecer la resiliencia del SOC y alinearlo con las mejores prácticas en la gestión de incidentes de seguridad.

TABLE IV. PLAN MEJORA

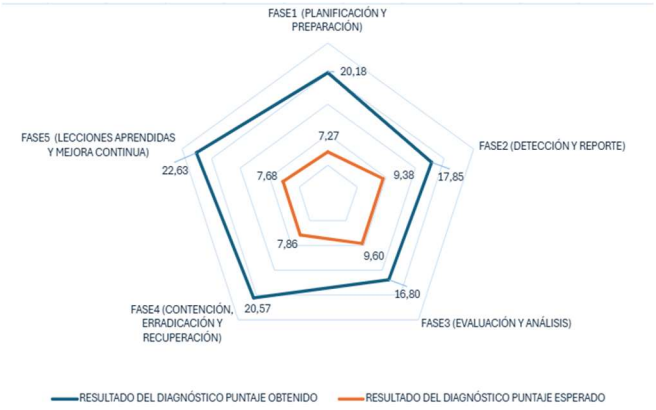
Tabla plan mejora		
Actividad	***Días***	***Valor***
Establecer un indicador al menos para medir la eficacia de la política	1	$800.000,00
Revisar la implementación del SCAP y aplicar las pautas de seguridad necesarias.	15	$12.000.000,00
Definir el escalamiento con terceros	1	$800.000,00
Incorporar un Jump Kit.	2	
Implementar un entorno de sandboxing	15	$12.000.000,00
Programar auditorías o evaluaciones externas anuales	8	$6.400.000,00
Centralizar la gestión de crisis ante incidentes de seguridad	2	$1.600.000,00
Definir el procedimiento de gestión de incidentes en que momento debe escalarse a una estructura de seguridad	1	$800.000,00
Evaluar herramientas adicionales para el SOC.	3	$2.400.000,00
Estandarizar el proceso de documentación	2	$1.600.000,00
Definir los criterios de costos, disponibilidad, motiviación y experiencia para la estructura del equipo	2	$1.600.000,00
Desarrollar una política de retención de evidencias	2	$1.600.000,00
Establecer un calendario de revisiones	1	$800.000,00
Implementar un proceso de auditoría periódica para asegurar el cumplimiento con todos los requisitos legales y regulatorios.	1	$800.000,00
Realizar una auditoría para verificar que todos los hosts, servidores y aplicaciones críticos estén protegidos	5	$4.000.000,00
Establecer una frecuencia adecuada para las revisiones de checksum en archivos críticos	1	$800.000,00
Establecer un metodo detallado de recolección de evidencia	3	$2.400.000,00
Implementar mecanismos que cumplan con estándares legales y de la cadena de custodia para asegurar la validez de la evidencia	2	$1.600.000,00
Identificar patrones comunes en incidentes previos	8	$6.400.000,00
Definir indicadores clave de alerta temprana y configurarlos en herramientas de monitoreo	8	$6.400.000,00
Centralizar los flujos de trabajo según los escenarios de incidente	1	$800.000,00
Realizar una auditoría completa de las herramientas y recursos en uso.	15	$12.000.000,00
Evaluar las configuraciones de red en el perímetro del SOC.	5	$4.000.000,00
Definir y documentar criterios claros de priorización de incidentes que se alineen con el impacto en funcionalidad, información y recuperabilidad	5	$4.000.000,00

Tabla plan mejora		
Actividad	***Días***	***Valor***
Actualizar la política o procedimiento de gestión de incidentes	1	$800.000,00
Evaluar las soluciones antimalware en uso.	5	$4.000.000,00
Documentar y automatizar, si es posible, el procedimiento para identificar todos los hosts afectados.	1	$800.000,00
Crear un metodo de recuperación	3	$2.400.000,00
Identificar y documentar las necesidades de información para diferentes tipos de incidentes	1	$800.000,00
Establecer un metodo de intercambio de información con otras organizaciones.	20	$16.000.000,00
Definir métricas específicas para evaluar controles de seguridad y configurar sistemas de monitoreo que generen estos datos.	3	$2.400.000,00

V. CONCLUSIONES Y TRABAJO FUTURO

- Se observa que enriquecer la norma ISO 27035 con las proposiciones de la NIST 800-61 proporciona un diagnóstico más detallado abarcando desde actividades de gestión hasta la implementación de controles específicos, esto conlleva a proponer la posibilidad de incluir otros marcos adicionales. La herramienta propuesta permite adaptar esto de manera sencilla ya que solo deben agregarse las preguntas que se consideren pertinentes.
- El aspecto más complicado del análisis fue la recolección de evidencias debido a las restricciones de tiempo y confidencialidad específicas de la compañía. Se plantea para ejercicios futuros establecer un sistema o herramienta adicional que permita facilitar a la compañía sobre la que se realiza el diagnóstico el cargue de dichas evidencias, no solo cargar archivos (pdf, jpg, mp4, etc) sino que estos estén relacionados con las diferentes preguntas que se formularon en el cuestionario.
- Ya que las actividades del plan de mejora responden a la priorización planteada por la compañía, se espera que su implementación reduzca rápidamente las brechas identificadas, la siguiente araña muestra la reducción de brechas que se tendría con la ejecución de únicamente las primeras 6 actividades definidas en el plan (estas son las que se consideran tienen mayor impacto en el cierre de brechas). Se puede observar cómo FASE 1 pasa de un puntaje de 28,36 a 20,18 y FASE 2 pasa de 24,77 a 17,85 teniendo una reducción del más del 20% en las brechas identificadas para estas fases.

FIGURA II: DIAGNÓSTICO LUEGO DE EJECUTAR LAS ACCIONES MAS IMPORTANTES DEL PLAN DE MEJORA



REFERENCIAS

[1] PowerData. Los costes de la gestión de datos, demasiado altos para las pymes. 2022. [En línea]. Disponible en: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/392699/los-costes-de-la-gesti-n-de-datos-demasiado-altos-para-las-pymes.

[2] PwC. Encuesta de confianza PwC 2023. [En línea]. Disponible en: https://www.pwc.com/co/es/pwc-insights/encuesta-confianza-2023.html.

[3] IBM, "Incident Response Services," IBM, 2023. [En línea]. Disponible en: https://www.ibm.com/mx-es/services/incident-response.

[4] J. Smith, R. Johnson, y A. Patel, "AIOps Solutions for Incident Management: Technical Guidelines and A Comprehensive Literature Review," arXiv preprint, vol. 2404.01363, 2024. [En línea]. Disponible en: https://arxiv.org/abs/2404.01363.

[5] Crowdstrike. Una visión integral: Nuevos estudios revelan los beneficios asociados a una detección y una respueta completamente gestionadas. 2021. [En línea]. Disponible en: https://www.crowdstrike.com/wp-content/uploads/2021/05/crowdstrike-forrester-tei-blog-es.pdf.

[6] IBM, "Cost of a Data Breach Report 2021," IBM Security, 2021. [En línea]. Disponible en: https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.

[7] Deloitte, "Deloitte's 2023 Global Future of Cyber Survey," Deloitte, 2023. [En línea]. Disponible en: https://www.deloitte.com/global/en/about/press-room/deloittes-2023-global-future-of-cyber-survey.html.

[8] International Organization for Standardization (ISO), "ISO/IEC 27035-1:2016 - Information technology - Security techniques - Information security incident management," 2016. [En línea]. Disponible en: https://www.iso.org/standard/60803.html.

[9] National Institute of Standards and Technology (NIST), "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Revision 2, 2012. [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.