Diseño e implementación del SGSI y diseño del DRP para una entidad pública del estado colombiano.

Christian Manuel Márquez González c.marquezg@uniandes.edu.co
Julián Andrés Páez ja.paez2@uniandes.edu.co
Manuel Alfonso Mora ma.moram1@uniandes.edu.co

Departamento de Ingeniería de Sistemas y Computación Universidad de los Andes

***Resumen*—Este artículo describe la manera adecuada de realizar el diseño y la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) y el DRP (Disaster Recovery Plan) en una entidad del Estado Colombiano, teniendo como base la norma ISO/IEC 27001 e ISO/IEC 22301, alineado a la metodología OCTAVE Allegro.**

En la actualidad, la entidad carece de un marco formal y sistemático para la gestión de la seguridad de la información a nivel organizacional. Si bien se han implementado medidas de seguridad de forma aislada, se observa la ausencia de un gobierno de la seguridad de la información robusto y debidamente alineado con los objetivos estratégicos, las metas operacionales y la visión institucional. Esta carencia de una estructura integral de seguridad de la información expone a la organización a vulnerabilidades significativas, tales como ataques cibernéticos, pérdida, alteración o filtración de información crítica, así como a potenciales disrupciones de sus procesos esenciales.

***Abstract*-- This article describes the proper approach for designing and implementing an ISMS (Information Security Management System) and a DRP (Disaster Recovery Plan) within a Colombian government entity, based on the ISO/IEC 27001 and ISO/IEC 22301 standards, and aligned with the OCTAVE Allegro methodology.**

Currently, the entity lacks a formal and systematic framework for managing information security at the organizational level. Although some isolated security measures have been implemented, there is a clear absence of a robust information security governance structure properly aligned with strategic objectives, operational goals, and institutional vision. This lack of a comprehensive information security structure exposes the organization to significant vulnerabilities, such as cyberattacks, loss, alteration, or leakage of critical information, as well as potential disruptions to its essential processes.

I. Contexto

La organización ha implementado diversas iniciativas de seguridad de la información de manera independiente en distintas áreas, con el objetivo de salvaguardar sus activos críticos y procesos esenciales. No obstante, se identifican debilidades en el marco de gobierno de la seguridad de la información integral actual que armonice estos esfuerzos de forma sistemática y asegure su alineación estratégica con los objetivos organizacionales.[1] Adicionalmente, la gestión de la seguridad basada en la aplicación de controles aislados se ve complementada por la carencia de un plan de recuperación ante desastres formalmente establecido, así como la indefinición de los requerimientos específicos que dicho plan debería contemplar para adecuarse a la realidad operativa de la organización.

La existencia de un gobierno débilmente estructurado de la seguridad de la información expone a la organización a un incremento en la vulnerabilidad frente a amenazas contemporáneas como ataques cibernéticos, pérdida o exfiltración de información, sabotaje y otras modalidades de riesgo inherentes a los sistemas modernos. Esta situación conlleva el incumplimiento de estándares internacionales reconocidos, como la norma ISO 27001, y la normativa nacional vigente, específicamente el Modelo de Seguridad y Privacidad de la Información (MSPI)[2] de Colombia. En consecuencia, resulta imperativo no solo optimizar la gestión de la seguridad de la información a través de la implementación de un marco de gobierno robusto, sino también fomentar una transformación en la cultura de gestión general. Este cambio permitirá abordar los desafíos actuales y establecer un proceso de mejora continua que facilite la adaptación a las nuevas amenazas emergentes, impulsadas por avances tecnológicos como la inteligencia artificial y la computación cuántica. [3]

II. Justificación del problema

Actualmente, la organización no tiene forma de gestionar adecuadamente la seguridad de la información dentro de la entidad; aun con medidas aisladas, el gobierno actual de la seguridad de la información no está alineado a los objetivos, metas y visión de esta. La entidad se encuentra expuesta a ataques cibernéticos, pérdida, alteración y filtración de información, junto con afectaciones a los procesos **críticos**.

Los principales problemas del actual gobierno de la seguridad de la información son:

- Los activos críticos de la organización no están definidos y, por tanto, las medidas de protección sobre los mismos no garantizan el adecuado manejo de riesgos y amenazas.
- La organización no tiene una política que garantice el correcto manejo y transferencia de conocimientos, en especial por la falta de una documentación estructurada.
- Las políticas de seguridad son informales y no están sistematizadas.
- La organización desconoce si cumple con las regulaciones nacionales e internacionales.
- La organización requiere un estándar para poder relacionarse con sus pares, clientes y proveedores en cuanto a su aproximación al manejo de la seguridad

[1] Tim Freestone. (September 2, 2022). A Guide to Information Security Governance. Kiteworks. https://www.kiteworks.com/secure-file-transfer/security-governance/

[2] MINTIC. ¿Qué es el MSPI?. MINTIC. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

[3] Cystel. (10 de junio de 2024). Cybersecurity Insights: The Impact of AI and Quantum Computing on Hacker Tactics and Defence Mechanisms. Quantum & Cybersecurity Series. https://www.linkedin.com/pulse/cybersecurity-insights-impact-ai-quantum-computing-hacker-tactics-ezwoe/

informática y su gestión.

- La organización no garantiza que los procesos se encuentren debidamente asegurados a partir de su acoplamiento con otras organizaciones.
- La organización no tiene acciones definidas para recuperarse ante un evento que pueda afectar sus procesos y accesos a información crítica y no tiene definido un tiempo de recuperación ante estos.

III. Propuesta de solución

La entidad pública del estado colombiano enfrenta el desafío de fortalecer su postura de seguridad ante la ausencia de un gobierno de la seguridad de la información, para lo cual es necesario diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) formal y diseñar un Plan de Recuperación ante Desastres (DRP). Para abordar esta brecha, se propone una estrategia estructurada bajo el estándar ISO 27001, complementada con la metodología OCTAVE Allegro para realizar la evaluación de riesgos y priorizarlos basados en el impacto sobre el negocio.

IV. Objetivos específicos

- Desarrollar y documentar las políticas de seguridad.
- Analizar las herramientas de seguridad y los controles usados actualmente, junto con la implementación de nuevos controles y herramientas.
- Diseñar y probar el Plan de Recuperación ante Desastres.
- Brindar a la organización capacitaciones sobre el uso de las tecnologías de seguridad de la información que actualmente poseen, buenas prácticas y sobre las tecnologías propuestas para mejorar la seguridad actual.

V. Alcance

Se detalla el alcance del proyecto de ciberseguridad; el proyecto se desarrollará en un plazo de doce meses, con objetivos específicos y entregables definidos para cada fase, con una duración de cuatro meses por fase.

Fase 1 – Meses 1 a 4

- Realizar una auditoría de seguridad integral y una evaluación de riesgos exhaustiva de los sistemas de información, basándose en ISO 27001[4], para identificar vulnerabilidades, evaluar el nivel de riesgo y proponer recomendaciones para mitigar las amenazas potenciales.
- Desarrollar y documentar un sistema de políticas de seguridad que cumpla con la normativa ISO 27001 y mejores prácticas de la industria, con el fin de proteger la información de la entidad y garantizar la confidencialidad, integridad y disponibilidad de los datos.
- Diseñar un Plan de Recuperación ante Desastres (PRD) integral que garantice la continuidad operativa de los sistemas críticos de la empresa en caso de interrupción, minimizando el tiempo de inactividad y la pérdida de datos.

Fase 2 – Meses 5 a 8

- Analizar las herramientas de seguridad y sus controles, con el objetivo de optimizar su implementación y configuración para una máxima eficacia.
- Implementar controles y herramientas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.
- Implementar un Plan de Recuperación ante Desastres (PRD) integral que garantice la continuidad operativa de los sistemas críticos de la empresa en caso de interrupción, minimizando el tiempo de inactividad y la pérdida de datos.

Fase 3 – Meses 9 a 12

- Verificar el Plan de Recuperación ante Desastres (PRD) integral que garantice la continuidad operativa de los sistemas críticos de la empresa en caso de interrupción, minimizando el tiempo de inactividad y la pérdida de datos.
- Realizar un programa integral de entrenamiento y pruebas del sistema, abarcando todos los componentes y funcionalidades, para asegurar su correcto desempeño y la preparación del personal para su uso eficiente.

VI. Metodologías Seleccionadas

Considerando los objetivos estratégicos de la organización, la problemática central identificada y la aspiración institucional de obtener la certificación bajo la norma ISO 27001 como mecanismo fundamental para evidenciar el cumplimiento de estándares internacionales de seguridad de la información, se ha determinado adoptar dicho estándar como base estructurante para el plan de trabajo de implementación. A partir de este marco referencial, se procedió a la selección de estándares complementarios con el propósito de desarrollar un gobierno de la seguridad de la información integral y adaptado a los requerimientos específicos de protección del capital intelectual de la organización.

En la selección de la metodología para el levantamiento de información y el análisis de riesgos, se llevó a cabo una evaluación comparativa de diversas metodologías disponibles, tomando como criterios fundamentales las siguientes características:

TABLA I
CUADRO COMPARATIVO DE METODOLOGÍAS

Metodologías			
Aspecto	OCTAVE Allegro	NIST SP 800-30	ISO/IEC 27005
Enfoque	Integral, abarcando aspectos operativos, técnicos y organizacionales.	Principalmente técnico, con enfoque en sistemas y tecnología.	Enfocado en la gestión de riesgos para la seguridad de la información.
Identificación de activos	Define explícitamente 4 tipos: personas, edificios, tecnologías e información.	Identifica activos principalmente tecnológicos y de información.	Se centra en activos relacionados con la información.
Participación	Involucra equipos multidisciplinarios y altos directivos.	Mayormente enfocado en equipos	Involucra a la organización, pero en el

[4] https://www.iso.org/standard/27001

		técnicos y expertos en ciberseguridad.	marco del SGSI.
Priorización de riesgos	Utiliza una matriz de riesgos basada en impacto y probabilidad, con enfoque cualitativo.	Cuantifica riesgos técnicos para facilitar decisiones en entornos TI.	Evalúa riesgos en función de la criticidad de la información y controles existentes.
Integración organizacional	Destaca la importancia de integrar riesgos relacionados con activos físicos y humanos.	Puede requerir adaptaciones para incluir aspectos no técnicos.	Se integra con políticas y procesos del SGSI, centrado en información.

La misión de la organización es la investigación y desarrollo de tecnología, en especial software. Para lograr que ellos tengan capacidad de identificar y priorizar los activos de la organización, se decidió trabajar con equipos multidisciplinarios conformados por integrantes activos de la organización y con partícipes de sus procesos. De esta forma tenemos seguridad de abarcar los activos físicos y humanos que son un factor importante para la organización, adicional al foco que es el material intelectual.

La metodología de análisis y gestión de riesgos OCTAVE (Operational Critical, Threat, Asset and Vulnerability Evaluation) se orienta principalmente a los aspectos de riesgo operativos y prácticas de seguridad, esto buscando que las organizaciones puedan tomar decisiones en el momento adecuado para proteger la información con base en los riesgos que se puedan presentar por falta de confidencialidad, integridad y/o disponibilidad de la información.

La metodología OCTAVE Allegro se compone de cuatro fases, y cada una de ellas con sus respectivos procesos:

1. Fase 1: Establecer factores determinantes
    a. Establecer los criterios de medición de riesgos.

2. Fase 2: Perfilar los activos
    a. Desarrollar un perfil de activos de información.
    b. Identificar los contenedores de activos de información.

3. Fase 3: Identificar las amenazas
    a. Identificar las áreas de preocupación.
    b. Identificar los escenarios de amenazas.

4. Fase 4: Identificar y mitigar los riesgos.
    a. Identificar los riesgos.
    b. Analizar los riesgos.
    c. Seleccionar el enfoque de mitigación.

La implementación del SGSI iniciaría con la definición del alcance y contexto organizacional, priorizando sistemas críticos como proyectos de investigación aeroespacial, redes de comunicación estratégica y bases de datos confidenciales. Este proceso requiere el compromiso explícito de la alta dirección para garantizar la asignación de recursos y la integración de la seguridad en la cultura organizacional. Posteriormente, se realizará una evaluación de riesgos híbrida: bajo ISO 27001, se identificarán activos, amenazas y vulnerabilidades mediante matrices de riesgo, mientras que para infraestructura crítica (ej. sistemas de defensa cibernética o datos clasificados), se aplicará OCTAVE Allegro. Esta metodología facilitará talleres colaborativos con equipos técnicos y operativos para mapear escenarios de amenazas de alto impacto, como ciberataques dirigidos o interrupciones energéticas prolongadas, y definir planes de mitigación alineados con controles del Anexo A de ISO 27001, como la gestión de vulnerabilidades (A.12.6) o la continuidad del negocio (A.17.1).

El desarrollo del DRP se basará en un Business Impact Analysis (BIA) para establecer objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO). Esto incluirá estrategias como copias de seguridad cifradas de manera que se genere una nube local cumpliendo con el marco de seguridad nacional (Decreto 1078 de 2015), redundancia geográfica de servidores críticos y simulacros periódicos de escenarios de desastre (ej.: ransomware o fallas eléctricas). Adicionalmente, OCTAVE Allegro aportará un enfoque cualitativo para priorizar riesgos en sistemas sensibles, vinculando amenazas identificadas (ej.: robo de propiedad intelectual) con controles técnicos como la segmentación de redes (VLANs avanzadas) o la implementación de soluciones de detección de intrusos (IDS/IPS).

Para garantizar la mejora continua, el SGSI integrará auditorías internas anuales, métricas de desempeño (ej. tiempo de respuesta a incidentes) y revisiones luego de un incidente. La certificación ISO 27001 podría alcanzarse en un plazo de 12 a 18 meses, mientras que el DRP debería lograr tiempos de recuperación inferiores a 4 horas para sistemas prioritarios. La sinergia entre ISO 27001 y OCTAVE Allegro fortalecería no solo la resiliencia técnica, sino también la concientización de los patrocinadores del proyecto en la gestión proactiva de riesgos.

Como parte de las actividades se plantean:

- Crear la documentación propia del SGSI para garantizar la correcta transferencia de conocimientos y manejo de la información generada por el proyecto, tanto al finalizar el mismo como dentro del SGSI, basados en los entregables de la metodología OCTAVE Allegro.
- Diseñar las políticas de seguridad de la información basadas en el análisis de riesgos, análisis de vulnerabilidades, estando alineadas con las políticas de seguridad de la información actuales.
- Garantizar la seguridad de la propiedad intelectual, datos y procesos de la institución considerando la importancia nacional que representa y las amenazas potenciales.
- El DRP diseñado debe cumplir con los niveles de servicio adecuados, teniendo en cuenta los requerimientos de la institución, considerando el RTO y el RPO.
- Otros requerimientos que puedan ser necesarios y que sean planteados por los consultores y jefe de área.
- La implementación del SGSI debe ceñirse a la norma ISO 27001 para facilitar la sincronización con otras organizaciones que siguen el mismo estándar, adicionalmente con el actual gobierno de seguridad de la información.
- Aplicar las recomendaciones de las diferentes normas seleccionadas para la implementación del SGSI y DRP dentro del contexto particular de la organización.
- Usar tecnologías que garanticen la seguridad de la propiedad intelectual, datos y procesos de la

institución, considerando la importancia nacional que representa y las amenazas potenciales.
- La institución debe avalar las tecnologías utilizadas en el proyecto, desde el punto de vista de la seguridad propia del medio, y contar con madurez de software y soportes adecuados desde la perspectiva de la ciberseguridad.

VII. Plan de trabajo

Teniendo en cuenta los objetivos que tiene la organización con el proyecto, su rol en investigación, desarrollo e innovación, además del marco legal y lineamientos a los que debe acogerse, hemos seleccionado el siguiente compendio de normas y metodologías para cubrir las necesidades específicas del caso. Siempre con el objetivo de brindar la mayor seguridad de la información y la gestión de esta.

a. Análisis de riesgos: Se hará uso de la metodología OCTAVE Allegro. Esta decisión se toma teniendo en cuenta el enfoque en los activos críticos de la organización y los riesgos asociados a los mismos. La metodología nos facilitará enfocarnos en los activos con más valor para la misión de la organización y realizar un análisis completo de estos, considerando el conocimiento de los integrantes de la organización.
b. Análisis de vulnerabilidades: Se escoge la metodología STRIDE para el análisis y decisión de mitigación de las vulnerabilidades presentes en la organización, permitiendo clasificar de forma clara y sistemática las amenazas según seis categorías fundamentales (Suplantación, Repudio, Divulgación de información, Denegación de servicio, Elevación de privilegios y Manipulación de datos), lo cual facilita una cobertura integral de los posibles vectores de ataque.
c. Diseño del DRP: Para realizar el diseño del DRP nos basaremos en la norma ISO 22301, en la cual se detallan las consideraciones necesarias para esta labor.
d. Gobierno: Nos alinearemos con la norma ISO 27001 para estructurar las políticas y auditorías necesarias para complementar las que actualmente lleva a cabo la organización.
e. Cumplimiento: El desarrollo del proyecto debe enmarcarse en las normas y leyes de la legislación nacional, organismos y el MINTIC y la institución a la que pertenece la organización.

VIII. Ejecución del plan de trabajo

El primer paso del plan de trabajo establecido es la aplicación de la metodología OCTAVE Allegro para realizar el análisis de riesgos: comenzando por la preparación para la aplicación de la metodología, seguido por la implementación de los pasos de la metodología OCTAVE Allegro. A partir de los resultados de la metodología de análisis de riesgo, se establecerá un plan de trabajo basado en el “plan de acción”, para lograr mejoras rápidas y significativas de la seguridad de la información en la organización. Finalmente, se dejará un diseño de las medidas de recuperación ante desastres según la información de la organización y sus necesidades, junto con toda la documentación generada anteriormente.

1. Estos son los pasos de preparación que se tomaron para implementar la metodología OCTAVE Allegro[5]:

   a. Asegurar el apoyo de la gerencia.
      i. Obtener la aceptación de la alta gerencia para asegurar que se asignen los recursos y el compromiso necesarios al proceso OCTAVE Allegro.
      ii. Definir claramente el alcance y los objetivos de la evaluación para alinearlos con las metas de la organización.

   b. Formar un equipo de análisis
      i. Reunir un equipo multidisciplinario con representantes de TI, operaciones y unidades de negocio para proporcionar diversas perspectivas.
      ii. Garantizar que los miembros del equipo tengan una buena comprensión de las operaciones, los activos y las prácticas de seguridad de la organización.

   c. Definir criterios de medición de riesgos.
      i. Establecer criterios claros para evaluar la probabilidad y el impacto de los riesgos potenciales.
      ii. Determinar la tolerancia al riesgo de la organización para guiar la toma de decisiones durante el proceso de evaluación.

   d. Identificar activos críticos.
      i. Catalogar los activos de información críticos de la organización, incluyendo datos, sistemas y procesos.
      ii. Priorizar los activos en función de su importancia para la misión y las operaciones de la organización.

   e. Recopilar información.
      i. Recopilar información relevante sobre la infraestructura de TI, los controles de seguridad y las amenazas potenciales de la organización.
      ii. Realizar entrevistas, encuestas y revisiones de documentos para obtener información de diversas partes interesadas.

   f. Desarrollar perfiles de amenazas.
      i. Identificar las amenazas potenciales que podrían afectar los activos críticos de la organización.
      ii. Considerar las amenazas internas y externas, así como las amenazas intencionales y accidentales.

   g. Prepararse para la evaluación.
      i. Desarrollar un plan detallado para la evaluación OCTAVE Allegro, incluyendo cronogramas, roles y responsabilidades.
      ii. Hay que asegurar que todos los miembros del equipo estén capacitados en la metodología OCTAVE Allegro y comprendan sus roles en el proceso.

[5] Cyrill Brunschwiler. (April 9, 2013). Lean Risk Assessment based on OCTAVE Allegro. https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/

2. Aplicación de la metodología OCTAVE Allegro

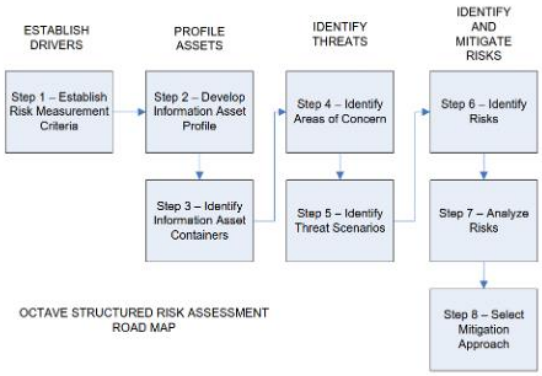

Fig. 1 Pasos de OCTAVE Allegro[6]

Fase 1: Establecer factores determinantes

- Paso 1 - Establecer los criterios de medición de riesgos: En este paso, se definen los criterios cualitativos que se utilizarán para evaluar el impacto de los riesgos potenciales en la misión y los objetivos de la organización. Este paso asegura que la evaluación de riesgos esté alineada con lo que la organización valora más.

TABLA II
CUADRO COMPARATIVO DE METODOLOGÍAS

Ejemplo	Explicación
Impacto en los plazos de investigación	Un ciberataque puede retrasar la entrega de un proyecto que posea una fecha de entrega específica. Impactando a otros proyectos dependientes de este y los objetivos de la organización en general.
Posible pérdida de ventaja competitiva	Los retrasos o la exfiltración de información de los proyectos pueden traducirse en una desventaja para la organización y su parte operativa.
Reputación científica de la organización	Toda exfiltración de información generaría la pérdida de confianza en la organización por parte de sus pares y de la dirección de la organización en su capacidad de proteger la propiedad intelectual que se está creando.
Pérdidas financieras debido a la investigación comprometida	Una exfiltración de un proyecto puede resultar en un producto que no puede ser utilizado o que puede ser copiado por una organización rival para su uso. Lo cual representa una pérdida de la inversión realizada y de la ventaja operativa esperada.
Las multas o sanciones legales relacionadas con violaciones de datos	La organización puede verse sancionada por la pérdida de información sensible que se pierda, lo cual afecta la parte operativa de la organización y pone en riesgo su funcionamiento.
El impacto en la productividad de los investigadores	Una interrupción causada por un atacante sobre los activos críticos de la organización (como por ejemplo un ransomware) puede causar demoras en la recuperación del funcionamiento normal de la organización, su función de investigación y entrega de productos a la parte operativa.

La selección de criterios de medición de riesgos relevantes y específicos es crucial para que la organización priorice los riesgos con precisión. Los criterios deben reflejar los aspectos únicos del entorno de investigación, como el impacto a largo plazo de la pérdida de propiedad intelectual o las consideraciones éticas de la seguridad de los datos en los estudios científicos.

Los criterios de riesgo genéricos podrían no capturar completamente los matices del riesgo en investigación, desarrollo e innovación. Por ejemplo, el criterio de "reputación" debe considerarse en el contexto de la integridad y credibilidad científicas dentro de la comunidad investigadora, lo que puede tener efectos duraderos.

Fase 2: Perfilar los activos

- Paso 2 - Desarrollar un perfil de activos de información: En esta etapa, se identifican y documentan los activos de información críticos dentro de la organización. Esto incluye describir el activo, su propietario, sus requisitos de seguridad (confidencialidad, integridad, disponibilidad), su valor para la organización y cualquier característica única. Este paso constituye el núcleo del enfoque centrado en los activos. Algunos ejemplos de activos de información son los datos de investigación (brutos y procesados), los resultados experimentales, los documentos de propiedad intelectual (patentes, secretos comerciales), el software y los algoritmos propietarios, las metodologías de investigación, las plataformas de investigación colaborativa y el conocimiento de los investigadores (conocimiento tácito). Es vital identificar tanto los activos tangibles (por ejemplo, archivos de datos, software) como los intangibles (por ejemplo, la experiencia de los investigadores, los descubrimientos no patentados). Estos últimos a menudo tienen un valor estratégico significativo y requieren diferentes estrategias de protección.

  Mientras que las evaluaciones de riesgos de TI tradicionales podrían centrarse en sistemas y datos, en investigación y desarrollo, el conocimiento y las ideas de los investigadores también son activos críticos. La pérdida de un investigador clave o la puesta en peligro de su experiencia pueden tener consecuencias significativas.
- Paso 3 - Identificar los Contenedores de Activos de Información: Este paso implica determinar dónde se almacenan, transportan o procesan estos activos de información críticos. Los contenedores pueden ser técnicos (servidores, bases de datos, almacenamiento en la nube), físicos (laboratorios, cuadernos, documentos) o incluso personas (computadoras portátiles de los investigadores, dispositivos móviles y su conocimiento). Comprender dónde residen los activos ayuda a identificar posibles vulnerabilidades. Algunos ejemplos de contenedores son la documentación, los sistemas de gestión de información, los servidores de investigación, imágenes basadas en Docker, las plataformas de colaboración basadas en la nube, los cuadernos de laboratorio físicos, las

[6] Cyrill Brunschwiler. (April 9, 2013). Lean Risk Assessment based on OCTAVE Allegro. https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/

computadoras personales y los dispositivos móviles de los investigadores utilizados para el trabajo, e incluso las comunicaciones verbales en las reuniones de investigación. Reconocer la diversa gama de contenedores en un entorno de investigación y desarrollo, incluidos los dispositivos personales y los documentos físicos, es crucial para una evaluación de riesgos exhaustiva.

Los controles de seguridad deben adaptarse a cada tipo de contenedor. La investigación y desarrollo a menudo implica una mezcla de sistemas de TI formales y prácticas informales de manejo de datos. Pasar por alto contenedores como dispositivos personales o notas de laboratorio físicas puede generar importantes puntos ciegos en la evaluación de riesgos.

Fase 3: Identificar las amenazas

- Paso 4 - **Identificar las áreas de preocupación:** En esta fase, se realiza una lluvia de ideas y se documentan las posibles condiciones o situaciones que podrían afectar negativamente a los activos de información identificados. Estas son áreas generales de vulnerabilidad o posibles amenazas. Este paso fomenta una perspectiva amplia sobre los riesgos potenciales. Algunos ejemplos de áreas de preocupación en I+D (inteligencia y desarrollo) incluyen las amenazas internas (intencionales o no intencionales), los ciberataques externos dirigidos a datos de investigación, las fugas de datos accidentales, la pérdida o el robo de materiales de investigación físicos, las fallas de equipos que provocan la pérdida de datos, los desastres naturales que afectan las instalaciones de investigación y los ataques de ingeniería social dirigidos a los investigadores.
- Paso 5 - Identificar los escenarios de amenazas: A continuación, se desarrollan escenarios específicos que detallan cómo las áreas de preocupación podrían dañar potencialmente los activos de información. Esto implica describir al agente de la amenaza, su motivación, la vulnerabilidad explotada y la posible consecuencia. Este paso hace que las amenazas sean más concretas y accionables. Algunos ejemplos de escenarios de amenazas son: un investigador descontento copia datos de investigación sensibles en una unidad USB y abandona la organización (Amenaza Interna); un atacante externo explota una vulnerabilidad en un servidor de investigación para robar propiedad intelectual (ciberataque externo); un investigador envía accidentalmente por correo electrónico un informe de investigación confidencial a un externo (fuga de datos accidental).

Fase 4: Identificar y mitigar los riesgos.

- Paso 6 - **Identificar los riesgos:** En este paso, se determinan los riesgos potenciales considerando la probabilidad de que ocurran los escenarios de amenazas y el impacto que tendrían en la organización en función de los criterios de medición de riesgos establecidos. Este paso conecta las amenazas con el impacto organizacional.
- Paso 7 - **Analizar los riesgos:** Los riesgos identificados se evalúan y priorizan en función de su impacto y probabilidad potencial. Esto a menudo implica la asignación de niveles de riesgo (por ejemplo, alto, medio, bajo). La priorización ayuda a la organización a centrar sus esfuerzos de mitigación en los riesgos más significativos.
- Paso 8 - Seleccionar el enfoque de mitigación: Se eligen estrategias apropiadas para abordar los riesgos priorizados. Las opciones incluyen: aceptar el riesgo (decidir no tomar medidas si el impacto o la probabilidad son bajos); reducir el riesgo (implementar controles de seguridad (técnicos, administrativos, físicos) para disminuir la probabilidad o el impacto); evitar el riesgo (cesar la actividad que conduce al riesgo); transferir el riesgo (trasladar el riesgo a un tercero, por ejemplo, a través de un seguro). Las estrategias de mitigación podrían incluir controles de acceso más estrictos a los datos de investigación, capacitación en concientización sobre seguridad a los investigadores, cifrado de datos sensibles, implementación de herramientas de prevención de pérdida de datos (DLP) y establecer protocolos claros para intercambiar datos y colaborar.

3. Implementación de la metodología

   La implementación empezó con una reunión inicial con integrantes de la entidad para socializarlo, alinear expectativas con la organización e iniciar la preparación de OCTAVE. En la primera y segunda reunión se obtuvieron los siguientes resultados:

   1. Se socializó el plan de trabajo anteriormente especificado, cada metodología y por qué se escogieron. Se obtuvo aprobación por parte de los representantes de la organización para hacer uso de dichas metodologías.
   2. Por parte de los representantes se expresó la necesidad de incluir la normatividad colombiana dentro del plan de trabajo.
   3. Se trabajaron los siguientes pasos de la preparación para la aplicación de la metodología OCTAVE:
      a. Asegurar el apoyo de la gerencia.
         i. Obtener la aceptación de la alta gerencia para asegurar que se asignen los recursos y el compromiso necesarios al proceso OCTAVE: Se obtuvo el compromiso para la realización de los talleres, acceso a información necesaria, personal requerido para cada taller y ejecución de acciones necesarias en la fase de implementación.
         ii. Definir claramente el alcance y los objetivos de la evaluación para alinearlos con las metas de la organización: Se definió que se usará un enfoque en los activos críticos de la entidad, en especial la propiedad intelectual, considerando la naturaleza de los proyectos manejados por la institución.
      b. Formar un equipo de análisis
         i. Reunir un equipo multidisciplinario con representantes de TI, operaciones y unidades de negocio para proporcionar diversas perspectivas. El equipo multidisciplinario base por parte de la organización estará conformado por:

TABLA III
LISTADO DE EQUIPO

Gerente del proyecto	Entidad
Desarrollador	Entidad
Ingeniero TI	Entidad

Adicionalmente, cualquier integrante que sea requerido para la realización de los talleres será agendado sin ninguna limitación.

ii. Garantizar que los miembros del equipo tengan una buena comprensión de las operaciones, los activos y las prácticas de seguridad de la organización: Los participantes del equipo de parte de la entidad tienen conocimientos de todos los proyectos dentro de la organización.

c. Definir criterios de medición de riesgos.
   i. Establecer criterios claros para evaluar la probabilidad y el impacto de los riesgos potenciales. La principal preocupación es la protección de la propiedad intelectual de sus proyectos, que tienen como objetivo final pasar a producción. Por tanto, cualquier exfiltración de información, acceso no autorizado o daño de la integridad representa un impacto crítico.
   ii. Determinar la tolerancia al riesgo de la organización para guiar la toma de decisiones durante el proceso de evaluación. La organización no está dispuesta a tolerar ningún riesgo con respecto a la indisponibilidad, integridad y confidencialidad de su propiedad intelectual, teniendo como base el impacto que esto puede tener, especialmente cuando hablamos de activos que hayan sido promovidos a producción. Por otra parte, en cuanto a disponibilidad y confianza del servicio que prestan, la organización está dispuesta a asumir riesgos que representen la interrupción de sus procesos por hasta una semana.

Luego de esta reunión inicial, se procedió a agendar los talleres para el desarrollo de la metodología OCTAVE Allegro. Siendo el siguiente paso el paso dos, Desarrollar un perfil de activos de información, ya que en la primera reunión se desarrolló el primer paso, Establecer los criterios de medición de riesgos. A partir de la tercera reunión se inició la creación del listado de activos críticos. En el taller se creó el listado de activos críticos en la infraestructura de red y servidores utilizados y las instalaciones físicas de la organización. Solicitamos la documentación relacionada y se procedió a socializar la información dentro de la reunión, con el objetivo de clarificar cualquier duda y garantizar un entendimiento claro del estado actual de la infraestructura de red y servicios dentro de la organización. A partir de este taller fue evidente la necesidad de realizar un taller aparte para enfocarnos exclusivamente en el proceso de software DevSecOps, no solamente por la necesidad de tener el tiempo necesario para abarcar todo el proceso, sino también para contar con el personal encargado de esa área, que tiene una perspectiva diferente y más profunda de los procesos.

Con base en los activos críticos que hasta ese momento se habían listado y para poder avanzar con la metodología, se adelantó el análisis de los riesgos. Es importante recalcar que el análisis de riesgos de la perspectiva de software se realizaría dentro de la misma reunión donde se creara el listado de activos críticos.

Posterior al análisis de riesgos, se procede a llevar a cabo una cuarta reunión, donde en principio se le realizan preguntas puntuales al equipo con el fin de aclarar cómo ejecutan cada control y saber qué necesidades o expectativas de mejora tienen frente a cada uno de ellos. En consecuencia, se obtienen las bases necesarias para poder determinar cuáles serían las oportunidades de mejora y los planes de acción para desarrollar, acorde con las necesidades de la organización.

La siguiente reunión se enfocó en el proceso de desarrollo de software dentro de la organización. En especial al ciclo de vida del software y a las prácticas de DevSecOps actualmente en funcionamiento. Para esta reunión se solicitó participación de un representante del área encargada del DevSecOps. A partir de ambas reuniones obtuvimos el listado completo de los activos críticos y los detalles necesarios para los siguientes pasos de la metodología. En la misma reunión se trataron los riesgos asociados a los activos críticos recién listados. Se encontró que los mayores riesgos son:

1. Exfiltración del código fuente: Debido a lo valioso y sensible para la organización de este activo, cualquier La exfiltración puede representar un impacto grave para la organización.
2. Integridad: Cualquier daño al código o adición de código malicioso también generaría un impacto alto en la organización.

En caso de materializarse estos riesgos, se generarían desde atrasos en el despliegue o culminación de un proyecto hasta afectar las operaciones, al representar un riesgo para la parte operativa de la misma.
Para la organización, la seguridad final de sus desarrollos es importante; por tal razón, el análisis SAST que actualmente se encuentra implementado es un excelente primer paso, pero no es suficiente. El análisis DAST le dará a la organización otra perspectiva de sus desarrollos, además de tener la ventaja de tener diferentes fabricantes en diferentes etapas del ciclo de vida del software.

Con estos talleres se completaron los primeros siete pasos de la metodología OCTAVE Allegro. Ya teniendo la información recabada de la organización, se realizó el análisis de mitigación teniendo en cuenta las restricciones en recursos y tiempo.

IX. Plan de acción

A partir del análisis realizado por medio de la metodología OCTAVE Allegro, se creó una lista de acciones que buscan mejorar la gestión de riesgos en el ámbito de la seguridad de la información y la ciberseguridad. Para esto se identificaron tres puntos claves de acción que se presentan a continuación.

1. La implementación de escaneos DAST en el ciclo de vida de la aplicación, dentro del enfoque de trabajo DevSecOps de la aplicación. Se sugirió el uso de herramientas open-source que tienen un menor impacto en el presupuesto de la organización. Al final del proceso de selección se optó por el uso de Nikto y OWASP ZAP debido al soporte que poseen y al nivel de documentación disponible.

   a. Prueba de concepto con Nikto.

   La imagen seleccionada para esta prueba es: Nikto-Docker

Repositorio: https://github.com/ellerbrock/nikto-docker

Descarga de la imagen a Docker:

docker pull frapsoft/nikto

Ejecución de un escaneo a demanda:
docker run frapsoft/nikto -host https://seofolio.co

b. Prueba de concepto con OWASP ZAP.

La imagen seleccionada para esta prueba es: zaproxy/zap-stable

Repositorio:
https://github.com/zaproxy/zaproxy/tree/main

Descarga de la imagen a Docker:

docker pull zaproxy/zap-stable

Ejecución de un escaneo a demanda:
docker run -v ${PWD}:/zap/wrk/:rw --network="host" zaproxy/zap-stable zap-baseline.py -t https://seofolio.co -r scan-report.html

Este comando de escaneo está adaptado para ser ejecutado solamente en Power Shell.

Estas opciones son viables para ser adaptadas, probadas e implementadas dentro del proceso DevSecOps de la organización. Esta prueba de concepto se limitó a la ejecución sobre Docker, apuntando a un sitio web sobre el cual contamos con permisos para realizar escaneos de prueba.

Ambas ejecuciones retornan información valiosa sobre vulnerabilidades, configuraciones indebidas y otras recomendaciones que pueden ser útiles para mejorar la seguridad del sitio.

Estas pruebas de concepto están desarrolladas en Docker; por tanto, la organización tiene la tarea de realizar los ajustes necesarios para que puedan ser incluidas de forma exitosa dentro de los pipelines actuales del proceso de despliegue. Además, se hizo explicita la necesidad de validar la seguridad de los contenedores generados a partir del repositorio público.

2. A través de las funcionalidades integradas en el software de firewall actualmente en uso, se llevó a cabo una evaluación de seguridad automática proporcionada por el fabricante. El resultado evidenció múltiples áreas con potencial de mejora. Sin embargo, el análisis no especificaba detalladamente dichas deficiencias, por lo que se procedió a realizar un examen exhaustivo de la configuración y las funcionalidades del firewall. Con esto se determinan las siguientes acciones para aumentar el SCORE de seguridad.
    a. Cambio del orden de las reglas, dejando toda clase de bloqueos específicos al inicio de la matriz de reglas junto con la regla de denegación total al final.
    b. Generación de reglas por medio de usuarios que se encuentren ya sea por Active Directory o por Wildcars asociadas a cuentas específicas.
    c. Compra de la licencia de IPS de modo que sea posible crear perfiles de seguridad dentro del dispositivo de seguridad perimetral.

3. Análisis y descubrimiento de vulnerabilidades mediante el uso de la metodología STRIDE (desarrollada por Microsoft) con el fin de que esta sea aplicable no solo a la topología de red, sino también a las aplicaciones que se desarrollen a nivel de software. En esta se verifican principalmente:
    a. Spoofing.
    b. Tampering.
    c. Repudiation.
    d. Information Disclosure.
    e. Denial of Service.
    f. Elevation of Privilege.

4. Se realiza la síntesis de todas las amenazas centralizadas por tipo de ataque y categoría, usando la matriz de MITRE para lograr conformar el árbol de amenazas junto con las actividades de mitigación de estas.

5. Mediante el uso de la creación del BIA se determinan las criticidades junto con el impacto que este pueda generar en la organización; así, con base en la norma ISO 22301, se desarrolla el plan de contingencia y el plan de continuidad. A partir del levantamiento de información a través de OCTAVE Allegro, se descubrió que las necesidades de la entidad no ameritaban un DRP que garantizara alta disponibilidad. Esto, sumado a los recursos de otras entidades englobadas dentro de la organización que engloba a la entidad, es posible crear un servidor alterno que proteja la propiedad intelectual de la entidad y sea una contingencia valiosa para continuar con las operaciones sin incurrir en grandes costos adicionales.

6. Se mitiga la posibilidad de exfiltración de información mediante carencia de herramientas a nivel de host, la cual se considera crucial para la organización. De este modo se plantea una comunicación mediante una infraestructura de tipo “bastión”, la cual, complementada con reglas de seguridad a nivel de firewall, impide la exfiltración de información de código fuente, así como integridad y confidencialidad de la propiedad intelectual. Esto es particularmente interesante para este caso, porque se hace uso de los recursos existentes en la organización debido a la limitación de recursos, pero aun así logrando el nivel de seguridad deseado.

7. Debido al manejo de costos de la entidad, se realiza una propuesta para realizar un modelo saludable de costos del proyecto, el cual le permite a la entidad tener una visión general de los consumos y costos tanto fijos como variables en los despliegues actuales y futuros. Se plantea a la organización una nueva forma de realizar el manejo de la seguridad de la información dentro de la organización, incluyendo un presupuesto centralizado para garantizar la correcta gestión en el tiempo.

8. Se realiza una correlación con tecnología de vanguardia. La inteligencia artificial es una herramienta que la entidad ha estado interesada en implementar, sin embargo, esta al ser una entidad pública, requiere de ciertas reglas en materia de seguridad de la información para garantizar la integridad, confidencialidad y disponibilidad de la información, sin dejar de lado los riesgos a nivel de seguridad nacional. De modo que se realizan políticas de seguridad de la información enfocadas en el uso de inteligencia artificial, LLM y su respectivo entrenamiento, así como el uso de machine learning para proyectos futuros, todo basado en el marco de la normativa nacional del ministerio de tecnologías de comunicaciones MINTIC en el decreto 1078 del 2015.

9. Una de las problemáticas adicionales fue en cómo es posible que este proyecto sea autosustentable en el tiempo; la entidad pública está ceñida a los lineamientos del ministerio de Ciencias en Colombia, por ende, los recursos van a ser catalogados como investigación y desarrollo. De este modo se plantean el siguiente supuesto para este proyecto:
    a. Cómo determinar una fórmula aplicable a la gestión de proyectos donde se determine un presupuesto para cada uno y se tenga un margen seguro de redirección de recursos para financiar otros proyectos sin afectar los proyectos activos.

   Para poder responder a este supuesto se tuvo que revisar los siguientes criterios para determinar los costos saludables para la manutención del proyecto:

- Establecer las mismas equivalencias de medición (Ej: si se está midiendo en GB y en MB poner ambas medidas en GB).
- Establecer el consumo promedio asignado por proyecto.
- Establecer el consumo promedio actual por proyecto.
- Establecer el número de nodos por proyecto.
- Establecer el presupuesto asignado por proyecto e identificar si es correspondiente al proyecto total o a la fase.
- Convertir el tiempo (inicio/fin) del proyecto a meses. (se asume que cada mes tiene 30 días)
- Establecer el número de proyectos paralelos.
- Establecer costos de licenciamiento.
- Establecer costos de capital humano.

Se asume que cada día laboral tiene 8 horas.

Fórmulas de referencia en la gestión de costos y presupuestos en la gestión de proyectos:

- **Variación de costo (CV):** CV = EV - AC. Mide el rendimiento de costos del proyecto.
- **Variación del cronograma (SV):** SV = EV - PV. Mide el rendimiento del cronograma del proyecto.
- **Índice de rendimiento de costos (CPI):** CPI = EV / AC. Mide la eficiencia en el uso del presupuesto.
- **Índice de rendimiento del cronograma (SPI):** SPI = EV / PV. Mide el rendimiento del cronograma en relación con el tiempo planificado.
- **Estimación al finalizar (EAC):** EAC = BAC / CPI. Estimación del costo total del proyecto en función de su desempeño actual.
- **Estimación hasta la conclusión (ETC):** ETC = BAC - EV. Costo estimado para completar el trabajo restante.

Formulación:

La fórmula ahora debe considerar tres componentes clave:

1. **Presupuesto inicial del proyecto (PIP):** Cubre todos los costos directos del proyecto.
2. **Margen de Contingencia (MC):** Un porcentaje sobre el PIP destinado a cubrir riesgos o financiar otros proyectos.
3. **Fondo de redistribución (FR):** Un monto fijo o porcentaje que se puede redireccionar a otros proyectos.

En este caso, el planteamiento va dirigido a proyectos que aún no tienen presupuesto asignado y que deben permitir distribuir recursos a otros proyectos sin afectar el costo del proyecto por ejecutar.

Por lo que:

P.I.P = (CH * TH) + (CA * TR) + CL

Dónde

- CH representa el costo del capital humano.
- TH representa el total de horas estimadas por perfil.
- CA representa el costo por unidad de recurso (CPU, RAM, HDD).
- TR representa el total de recursos asignados (CPU, RAM, HDD).
- CL representa el costo proporcional de licenciamiento.

Para definir el margen de contingencia, se deberá multiplicar el PIP por el porcentaje de contingencia (puede variar entre el 10% y el 20% del PIP).

MC= PIP * % de contingencia.

Para definir el fondo de redistribución se deberá multiplicar el PIP por el porcentaje de redistribución (en este caso se sugirió 5%).

FR= PIP * % de contingencia.

Por lo que la fórmula para definir el presupuesto total asignado (PTA) es:

PTA= PTP+ MC+ FR

10. En el marco del desarrollo del proyecto, se abordó de manera estratégica la forma de cómo se debería realizar la implementación de soluciones basadas en **inteligencia artificial (IA)** bajo un enfoque **completamente local**, con el objetivo de fortalecer la soberanía tecnológica, garantizar la confidencialidad de la información y apoyar directamente las capacidades de **seguridad nacional**. Esta implementación se fundamentó normativamente en el **Decreto 1078 de 2015**, el cual establece directrices claras para el uso de tecnologías de la información por parte de entidades estatales, haciendo énfasis en que estas son responsables por el tratamiento, protección y seguridad de la información, aun cuando se adopten entornos tecnológicos avanzados. Tomando como punto de partida este marco legal, se estructuró una **justificación técnica y normativa** que dio sustento a la decisión de evitar cualquier tipo de dependencia de servicios externos, especialmente aquellos que operan bajo modelos de nube pública o procesamiento fuera del país, lo cual podría poner en riesgo la integridad de los datos clasificados o estratégicos.
    En este sentido, se optó por el uso de **modelos de inteligencia artificial open source**, como **LLama2, Mistral, Falcon y DEEPSEEK, los cuales cumplen con estos requerimientos para esta futura implementación.**

11. **Se crea una tabla en la cual se categorizan las políticas de seguridad de la información, como se evidencia en la siguiente tabla:**

TABLA IV
INDICADORES POR SEGURIDAD

Categoría	Nombre	Nº de políticas
P1	Gestión de accesos	10
P2	Protección de infraestructura	10
P3	Protección de la información y backups	5
P4	Seguridad en el ciclo de desarrollo (DevSecOps)	6
P5	Ciclo de desarrollo DevSecOps	13
P6	Desarrollo de código	33
P7	Gestión de incidentes y continuidad	11
P8	Cumplimiento legal y normativo	8
P9	Formación y concienciación	5
P10	Seguridad en el uso de inteligencia artificial	26

X. Indicadores

Como las pruebas se realizaron como POC (prueba de concepto) se dejan establecidos los indicadores para poder realizar la respectiva medición de los controles y el plan actual en materia de seguridad de la información. Se proyecta que estos sean aplicados en fase 2 a nivel de SGSI y en fase 3 a nivel de DRP. A continuación, se listan los indicadores por categoría que se dejan planteados para su futura evaluación.

TABLA V
INDICADORES POR SEGURIDAD

Indicador	Descripción	Fórmula
Nivel de implementación de controles críticos	Mide el porcentaje de controles definidos en la PoC que fueron implementados en el entorno operativo.	(# controles implementados / # controles planeados) × 100
Índice de incidentes de seguridad	Número de incidentes detectados vs. mitigados luego de PoC.	(# incidentes mitigados / # incidentes totales detectados) × 100
Tiempo promedio de detección (MTTD)	Tiempo medio que toma detectar un incidente desde su ocurrencia.	Σ tiempo detección / # incidentes
Tiempo promedio de respuesta (MTTR)	Tiempo medio para resolver incidentes desde su detección.	Σ tiempo resolución / # incidentes

TABLA VI
INDICADORES POR CAPACITACIÓN

Indicador	Descripción	Fórmula
Cobertura de capacitación en SGSI	Proporción del personal clave que recibió formación.	(# capacitados / # personal objetivo) × 100
Evaluación de conocimientos adquiridos	Puntaje promedio en evaluaciones tras capacitaciones.	Σ puntajes / # evaluados

TABLA VII
INDICADORES POR GESTIÓN DE INCIDENTES

Indicador	Descripción	Fórmula
Número de hallazgos recurrentes	¿Cuántos problemas de seguridad se repiten tras PoC?	# de hallazgos repetidos
Cumplimiento de recomendaciones de auditoría interna	Medida de adopción de las recomendaciones post-PoC.	(# acciones implementadas / # recomendaciones) × 100

TABLA VIII
INDICADORES POR CONTINUIDAD

Indicador	Descripción	Fórmula
Ejecución de pruebas del plan de contingencia	Pruebas ejecutadas vs. planificadas (GitLab en sitio alterno).	(# pruebas realizadas / # pruebas planificadas) × 100
Cumplimiento del RTO/RPO estimado	Verifica si se logró el RTO ≤ 5 días y RPO ≤ 24 h.	Tiempo real de recuperación vs. objetivo

XI. Conclusión

El desarrollo de este proyecto se estructuró en tres fases progresivas, alineadas con estándares internacionales de seguridad de la información y continuidad del negocio, específicamente ISO/IEC 27001, ISO/IEC 22301 y prácticas metodológicas de OCTAVE Allegro. La ejecución permitió avanzar significativamente en la maduración del modelo de ciberseguridad institucional en una entidad estatal colombiana, la cual inicialmente carecía de una estructura formal para la protección de activos de información críticos.

Aunque este proyecto se divide en 3 fases, durante la primera de ellas se dejan planteadas pruebas de concepto y documentación que servirán como bases en el avance en varias áreas en materia de seguridad de la información, gestión de incidentes, así como tener un componente para la organización.

Durante la ejecución del proyecto se incorporaron componentes innovadores que permiten mejorar la gobernanza, la sostenibilidad financiera y la adaptabilidad tecnológica del SGSI:

- **Modelo de costos saludables para proyectos tecnológicos:** Se desarrolló una fórmula de costos que contempla no solo gastos de adquisición y licenciamiento, sino también variables asociadas a depreciación, escalabilidad, soporte y riesgo residual. Este modelo permite priorizar inversiones según su impacto estratégico, mitigando sobredimensionamientos o subinversiones comunes en entornos públicos.
- **Planeación prospectiva para requisitos de inteligencia artificial (IA):** Se incluyó un marco base para la futura integración de sistemas de IA en funciones críticas del SGSI, como análisis predictivo de amenazas, automatización de auditorías y gestión dinámica de accesos. Esto permitirá en fases posteriores evaluar soluciones de machine learning y detección de anomalías, elevando el nivel de madurez del sistema de seguridad.
- Así mismo, se define una fórmula para el cálculo de unos costos aproximados y cómo estos pueden ser sostenibles en el tiempo, esto con el fin de que la implementación del SGSI para que cada uno de los proyectos trabajados tenga en sí su propio mantenimiento.

Una de las grandes limitantes de este proyecto se basó en que la implantación sobre sistemas no se puede realizar durante este tiempo debido a procesos organizacionales y tiempo en la ejecución de los debidos planes, sin embargo, mediante el uso de las pruebas de concepto, se avanzó en la presentación de las ventajas para la entidad de contar con su respectiva implementación en fase 2 junto con su proyecto de migración de tecnología.

REFERENCIAS

[1] Tim Freestone. (September 2, 2022). A Guide to Information Security Governance. Kiteworks. https://www.kiteworks.com/secure-file-transfer/security-governance/

[2] MINTIC. ¿Qué es el MSPI?. MINTIC. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

[3] Cystel. (10 de junio de 2024). Cybersecurity Insights: The Impact of AI and Quantum Computing on Hacker Tactics and Defence Mechanisms. Quantum & Cybersecurity Series. https://www.linkedin.com/pulse/cybersecurity-insights-impact-ai-quantum-computing-hacker-tactics-ezwoe/

[4] https://www.iso.org/standard/27001

[5] Cyrill Brunschwiler. (April 9, 2013). Lean Risk Assessment based on OCTAVE Allegro. https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/

[6] Cyrill Brunschwiler. (April 9, 2013). Lean Risk Assessment based on OCTAVE Allegro. https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/