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

Diana María Andica Bueno d.andica@uniandes.edu.co
Yoimer Andres Seña Cespedes y.sena@uniandes.edu.co
Jonnathan Navarro Roa j.navarror2@uniandes.edu.co

Departamento de Ingeniería de Sistemas y Computación Universidad de los Andes

***Resumen*— Este artículo presenta el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y de un Plan de Recuperación ante Desastres (DRP) en una entidad pública del Estado colombiano dedicada a actividades de Investigación, Desarrollo e Innovación Tecnológica (I+D+I). En la Fase I se realizó un diagnóstico de riesgos y brechas, se definieron los lineamientos iniciales para el SGSI y el DRP, y se estableció una priorización preliminar para la implementación de controles técnicos y organizacionales.**

El presente proyecto corresponde a la Fase II, en la cual se validaron los controles de seguridad mediante una matriz de seguimiento, se fortaleció la documentación del DRP con escenarios y estrategias de recuperación, se diseñó e implementó una emulación de los componentes críticos para evaluar escenarios de ciberseguridad, y se diseñaron y se midieron indicadores de madurez en seguridad de la información y DRP.

En conclusión, la ejecución de la Fase II del proyecto logró elevar la madurez en ciberseguridad, aportar insumos técnicos para decisiones estratégicas, crear una base metodológica y técnica para un SGSI y DRP sostenibles, establecer un entorno seguro de pruebas y definir un plan realista para la continuación del proyecto por los próximos años.

***Abstract*-- This article presents the design and implementation of an Information Security Management System (ISMS) and Disaster Recovery Plan (DRP) in a Colombian public entity dedicated to research, development and innovation (I+D+I). In Phase I, a risk and gap assessment was conducted, initial guidelines for ISMS and DRP were drafted, and a preliminary prioritization for the implementation of technical and organizational controls was established.**

This project focuses on Phase II, in which security controls were validated through a follow-up matrix, documentation DRP was improved by adding scenarios and recovery strategies, an emulation of critical components was designed and developed to assess cybersecurity scenarios and maturity metrics were designed and calculated to evaluate the current state of the ISMS and DRP.

To summarize, phase II managed to increase cybersecurity maturity, provide technical inputs for strategic decision-making, established a methodological and technical framework for sustainable ISMS and DRP, build a safe testing environment, and define a realistic plan to continue the project in the coming years.

I. Contexto

La Entidad pública del estado colombiano bajo alcance es un centro de Investigación, Desarrollo Tecnológico e Innovación (I+D+I) que posee un rol como unidad tecnológica especializada, lo que exige una gestión de seguridad de la información sólida y articulada.

En la Fase I de diagnóstico, Páez, Márquez y Mora identificaron que dicha Entidad cuenta con iniciativas de seguridad aisladas, surgidas de manera independiente y sin un gobierno integral que las articule con los objetivos institucionales [1]. También se evidenció la ausencia de un Plan de Recuperación ante Desastres (DRP) con requerimientos definidos y ajustados a la realidad operativa de la Entidad. Estas condiciones aumentan la exposición a amenazas —como exfiltración o pérdida de información y sabotaje—, dificultan el cumplimiento de marcos como ISO/IEC 27001 y el Modelo de Seguridad y Privacidad de la Información (MSPI), y refuerzan la necesidad de pasar de controles dispersos a un enfoque de gobierno formalizado y de mejora continua.

Como resultado, la Fase I entregó una matriz de análisis de brechas (GAP) que muestra los aspectos pendientes, el nivel de madurez actual y los controles necesarios sobre la infraestructura de la Entidad, junto con un plan básico de continuidad y contingencia que sirve como insumo para avanzar en las siguientes etapas del proyecto, con una propuesta de innovación que contempla la formulación de costos e implementación de tecnologías basada en Inteligencia Artificial (IA).

Actualmente, se trabajó en la Fase II del proyecto, en la cual se entrega una matriz de seguimiento que organiza los controles propuestos en la Fase I y los identificados durante la revisión de la Matriz GAP. Asimismo, se fortalece la documentación del DRP, incluyendo: análisis de impacto a las aplicaciones, roles y responsabilidades, plan de comunicación, escenarios, secuencia de recuperación, métricas, pruebas y un documento completo del DRP. A partir de esta documentación, se selecciona un escenario del DRP para ser evaluado en un entorno emulado, desarrollado como un Producto Mínimo Viable (MVP), que replica los componentes críticos de la infraestructura tecnológica. Este entorno permite, además, probar controles críticos, validar cambios, simular ataques y apoyar la capacitación del personal. Durante esta fase también se realiza la medición de indicadores del SGSI y del DRP, y se presenta la cuantificación del proyecto.

En resumen, la Fase II busca validar los controles de seguridad y el diseño del DRP mediante una matriz de seguimiento y una prueba de concepto en el entorno de emulación, generando insumos técnicos para su implementación futura.

II. Definición del problema

La ausencia de un SGSI y un DRP convierte a las entidades en un objetivo vulnerable frente a amenazas cibernéticas, con consecuencias significativas como la filtración de información sensible, la materialización de riesgos, la afectación a procesos de negocio críticos y la ocurrencia de incidentes de seguridad, que pueden derivar en una recuperación tardía de servicios críticos, afectación reputacional, pérdidas económicas, entre otros impactos. En síntesis, la falta de una estrategia integral, holística, formalizada e implementada expone a las entidades a un amplio espectro de riesgos técnicos, operacionales y estratégicos, ubicándolas en una posición reactiva frente a

amenazas tanto internas como externas, y comprometiendo su capacidad de resiliencia.

Este proyecto es la continuación de la Fase I, donde se realizó un diagnóstico de riesgos y brechas, se definieron lineamientos para el SGSI y el DRP, y se estableció una priorización inicial de despliegue de controles técnicos y organizacionales; sin embargo, la no implementación de un SGSI y un DRP representa una brecha que expone la infraestructura tecnológica y las operaciones de la Entidad a riesgos de ciberseguridad, tales como la interrupción de servicios esenciales del core de negocio y el compromiso de sus capacidades, amenazando directamente la continuidad de su misión institucional.

En este contexto, la problemática central radica en que la Organización continúa expuesta a riesgos de ciberseguridad previamente identificados, sin evidencias operativas que demuestren la eficacia en la implementación de controles priorizados, la consistencia de roles y procedimientos ante incidentes de ciberseguridad y tampoco la capacidad técnica de resiliencia, continuidad operativa y recuperación. La integración práctica de elementos como pruebas dinámicas de seguridad de aplicaciones (DAST) en integración y entrega continua (CI/CD), así como medidas de segmentación, hardening y control de accesos, permanece sin validación en condiciones controladas o reales.

Esta situación genera incertidumbre técnica y operativa respecto a la capacidad de la Entidad para preservar la confidencialidad, integridad y disponibilidad de sus activos críticos, así como para asegurar la continuidad de su misión frente a escenarios de amenazas plausibles. Tal incertidumbre dificulta la toma de decisiones informadas, y prolonga la exposición a impactos operacionales y reputacionales, mientras no se cuente con una verificación mínima y documentada de controles efectivos implementados.

III. Justificación del problema

Colombia enfrenta un panorama de amenazas cibernéticas sostenidas y en constante evolución, caracterizado por altos volúmenes de intentos de intrusión y campañas de Ransomware que desafían la capacidad del sector público para prevenir, detectar y recuperar sus servicios.

Durante el primer semestre de 2023, el país registró 5.000 millones de intentos de ciberataques [2]; a escala anual, distintos reportes estiman que en 2023 se alcanzaron 12.000 millones de intentos [3]. Asimismo, la actividad delictiva medida por denuncias ante autoridades nacionales dimensiona la magnitud del problema: de acuerdo con el Centro Cibernético Policial, se reportaron 59.033 denuncias por delitos informáticos en ese mismo año; la situación sigue agravándose, durante el 2024, Colombia se posicionó como el cuarto país con mayor número de ciberataques en América Latina, con más de 36.000 millones de ofensas registradas, lo que representa un incremento del 29% con respecto al año anterior [4]. Los vectores y la frecuencia de ataques cibernéticos evidencian una exposición significativa de las entidades frente a actores maliciosos con motivaciones criminales y/o estratégicas.

Estos hechos subrayan que la amenaza es persistente y que su materialización impacta directamente la disponibilidad, integridad y confidencialidad de entidades de misión crítica.

Si bien las medidas tradicionales como seguridad perimetral, firewalls, segmentación por VLANs, políticas de acceso y hardening siguen siendo necesarias, resultan insuficientes, puesto que, aunque mitigan riesgos en el borde de la red, no cubren capacidades integrales de ciberseguridad como gobierno, procesos, personas, gestión del riesgo, detección, respuesta y recuperación. En este contexto, el enfoque de seguridad basado en Zero Trust plantea que no debe conferirse confianza implícita por la ubicación en la red, ni por la propiedad de un activo, por el contrario, exige autenticación y autorización continuas, aplicación de políticas dinámicas y uso de información contextual para decisiones de acceso centradas en recursos, identidades y datos. En este sentido, la norma ISO/IEC 27001 y su Anexo A proporcionan un marco para integrar este enfoque mediante controles de gestión de accesos, seguridad de redes, monitoreo y registro de eventos, así como respuesta y recuperación ante incidentes, garantizando la confidencialidad, integridad y disponibilidad de la información bajo un modelo de mejora continua. [5]

La evidencia internacional respalda la importancia de contar con programas maduros (SGSI + BCP/DRP) y con capacidades de automatización en la respuesta a incidentes de Seguridad. El informe “IBM Cost of a Data Breach 2024” señala que el costo promedio global de una brecha alcanzó USD 4,88 millones, y que las organizaciones con orquestación y automatización de seguridad logran reducir tanto el ciclo de vida como el impacto económico de los incidentes en comparación con aquellas que carecen de dichas capacidades [6]. Para un entorno de I+D+I, donde la misión depende en buena medida de la confidencialidad, integridad y disponibilidad de la información, así como de la continuidad de servicios TIC, estas capacidades no son agregadas sino fundamentales.

Frente al panorama de amenazas cibernéticas a nivel nacional, la implementación de un SGSI conforme a ISO/IEC 27001 complementado con el enfoque Zero Trust y de un DRP sustentado en ISO 22301, constituye una iniciativa estratégica para fortalecer la resiliencia, asegurar la continuidad y proteger la misión de la Entidad frente a adversarios en rápida y constante evolución.

IV. Propuesta de solución

Con base en lo identificado en el diagnóstico, la Entidad cuenta con iniciativas de seguridad dispersas que han sido desplegadas de manera aislada y se evidencia la ausencia de una estrategia y un gobierno integral de seguridad de la información que alinee y orqueste todos estos esfuerzos, asimismo, se constató la ausencia de un DRP con requerimientos claros y ajustados a la realidad operativa de la Entidad.

Como respuesta a lo anterior, se plantea una estrategia de despliegue por etapas, estructurada bajo un horizonte de tres años. Durante el primer año, el enfoque se centrará en el diseño detallado, la validación de lineamientos, la creación de artefactos base y la ejecución de pruebas piloto que permitan ajustar el alcance real de las implementaciones. En los años siguientes, se proyecta avanzar hacia la implementación progresiva de los controles, la evaluación de su efectividad mediante auditorías internas, la integración de mejoras derivadas de las lecciones aprendidas y la consolidación de un ciclo permanente de mejora continua.

Objetivo general Fase II

- Contribuir al cumplimiento del objetivo general del proyecto mediante la validación y análisis de los controles de seguridad definidos en la Fase I, a través de una matriz de seguimiento que permita monitorear su ejecución y efectividad a futuro, facilitando su mejora

continua. Asimismo, apoyar la validación del diseño del DRP mediante una prueba de concepto (PoC) ejecutada en una emulación de los sistemas críticos, con el fin de simular un escenario del DRP, generar evidencias documentadas, establecer criterios de aceptación y definir un plan de despliegue para su implementación.

Objetivos específicos Fase II

- Diseñar una matriz de seguimiento para validar la implementación de controles definidos en la Fase I del Proyecto, que permita monitorear su ejecución, efectividad y mejora continua.
- Actualizar la Declaración de Aplicabilidad (SoA) derivada de la Fase I y estructurar un plan de despliegue por etapas para su implementación en siguientes Fases.
- Actualizar y fortalecer la documentación del DRP, incluyendo escenarios disruptivos, estrategias de recuperación actuales y propuestas, secuencia de recuperación, Matriz de Análisis de Impacto a las Aplicaciones (AIA), roles y responsabilidades, plan de comunicaciones, métricas y prueba unitaria del plan de comunicaciones.
- Diseñar e implementar una emulación de las aplicaciones críticas identificadas, que sirva como herramienta de validación y prueba dentro del DRP.
- Validar a través de la emulación, la ejecución de un escenario del Plan de Recuperación ante Desastres.
- Crear un procedimiento de gestión de incidentes de seguridad alineado con el DRP.
- Realizar el seguimiento y la medición del avance y nivel de madurez de indicadores de los indicadores del SGSI y del DRP.
- Desarrollar una metodología para la implementación, operación y evaluación de la emulación con un enfoque específico en el fortalecimiento de la ciberseguridad y la gestión de riesgos.
- Elaborar y presentar recomendaciones de ciberseguridad derivadas del análisis de las migraciones efectuadas en herramientas tecnológicas relevantes para el negocio, con el fin de fortalecer su protección y operación.
- Reestructurar el plan de despliegue para las siguientes fases del proyecto.

V. Alcance y plan de trabajo

En el documento inicial de la fase I, se planteó desarrollar el proyecto en un plazo de doce meses, distribuidos en 3 fases a lo largo de tres semestres académicos. No obstante, implementar de forma integral un SGSI y un DRP exige un nivel de madurez organizacional que no se logra de un momento a otro. Estos procesos requieren ciclos iterativos de mejora, ajustes culturales, adopción gradual de controles técnicos y un monitoreo constante de su efectividad. Todo esto, junto con las limitaciones identificadas durante el desarrollo del proyecto, demuestra la inviabilidad de completarlo en el lapso de tiempo propuesto. [7] Ante esta situación, en la fase II se optó por una estrategia de despliegue por etapas con un horizonte de tres años. El primer año se enfocará en el diseño detallado, la validación de lineamientos, la creación de artefactos base y pruebas piloto que permitan ajustar el alcance real. Ya en los años siguientes, se avanzará hacia la implementación progresiva de los controles, su evaluación mediante auditorías internas y la integración de mejoras a partir de las lecciones aprendidas.

Antes de iniciar con la Fase II, el equipo revisó y analizó toda la documentación generada en la Fase I; esto implicó leer los entregables en detalle, entender los lineamientos establecidos y estudiar las actividades que el equipo anterior había propuesto para las siguientes etapas, también se llevó a cabo una sesión de empalme con el grupo de la Fase I para aclarar dudas, transferir conocimiento y entender el estado real del proyecto junto con los retos pendientes, esta sesión fue clave para garantizar la continuidad entre ambas fases.

VI. Ejecución del plan de trabajo

La ejecución del plan de trabajo permitió transformar las actividades del proyecto en aportaciones concretas y reutilizables para la implementación eficaz de un SGSI y un DRP en organizaciones con niveles de madurez inicial, los resultados obtenidos representan buenas prácticas aplicables, orientadas a facilitar la toma de decisiones, agilizar la implementación y elevar la coherencia del sistema de gestión.

A continuación, se sintetizan las contribuciones más relevantes.

1. Metodología unificada para seguimiento de controles.
   Estructuración de una matriz integrada de seguimiento, que consolida controles y contramedidas del plan de acción, plan de mitigación y SoA; su aporte principal es un modelo de trazabilidad que permite relacionar cada control con su evidencia, responsables, dependencias y estado de avance, facilitando la toma de decisiones, trazabilidad y el escalamiento.

2. Fortalecimiento de lineamientos DRP.
   Proceso integral de optimización de la documentación asociada al DRP, integrando y evolucionando en un único documento los insumos de contingencia, continuidad y el análisis de impacto al negocio (BIA), esta consolidación que fue soportada en sesiones con las áreas de negocio permitió alinear criterios, precisar información clave y asegurar coherencia operativa. El resultado es un DRP unificado, alineado al negocio y orientado a la acción, que incorpora escenarios de desastre, estrategias de recuperación, árbol de llamadas, secuencia operativa, roles y equipos responsables, así como un modelo operativo definido por fases; representa una actividad que aporta un marco documental robusto y fácilmente gestionable, que fortalece la preparación organizacional y facilita la adopción, mantenimiento y activación del DRP en situaciones críticas.

3. Modelo de gestión de incidentes de ciberseguridad.
   Definición del ciclo de vida para la gestión de incidentes de ciberseguridad, proporcionando a la Organización un modelo práctico y estandarizado para la preparación, identificación, análisis, gestión y cierre. Este componente incluyó la elaboración de un plan de respuesta a incidentes y la definición de una matriz de gestión (RACI) que establece roles, responsabilidades y puntos de coordinación con áreas internas y externas.
   A través de este componente, se consolida un modelo operativo claro y aplicable, que establece cómo actuar ante un incidente, quién participa en cada etapa y cómo se articula la comunicación entre todos los involucrados; este

marco fortalece la capacidad de respuesta organizacional, agiliza la toma de decisiones y facilita una gestión coordinada y eficaz de los incidentes de ciberseguridad.

4. Modelo de indicadores de seguimiento y madurez.
Diseño de un conjunto estructurado de indicadores que permite medir el avance del SGSI y del DRP de manera objetiva, consistente y alineada con el nivel de madurez actual de la Organización en esta Fase II del proyecto. Estos indicadores integran variables de seguimiento, desempeño y adopción operativa, que ofrece una visión clara del progreso y facilita la toma de decisiones, es un marco de medición práctico y accionable, que habilita la gestión continua del SGSI, promueve la mejora progresiva y establece bases cuantitativas para evaluar la evolución del sistema, tal como se muestra en la Tabla I.

TABLA I
INDICADORES – FASE II

No	NOMBRE	DESCRIPCIÓN	FÓRMULA
1	DISPONIBILIDAD DE INTERNET	Proveer servicios ininterrumpidos de la red pública de datos para los componentes críticos	Tiempo medio entre fallas (TMF)/Tiempo Medio entre fallas (TMF) + Tiempo máximo de Recuperación (TMR)
2	DISPONIBILIDAD DE PLATAFORMA CRÍTICA	Proveer servicios ininterrumpido de la infraestructura tecnológica que apoya la misión de la Organización	Tiempo medio entre fallas (TMF) / Tiempo Medio entre fallas (TMF) + Tiempo máximo de Recuperación (TMR)
3	NIVEL DE CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Seguimiento a la Preservación y Administración de la confidencialidad, integridad y disponibilidad de la información	Políticas cumplidas / Políticas existentes * 100
4	EXACTITUD MVP EMULACIÓN	Determina qué tan bien emula o replica la emulación el comportamiento del componente real.	1 - ((valor real - valor emulación) / valor real)
5	SISTEMAS CRÍTICOS IDENTIFICADOS Y PRIORIZADOS EN DRP	Evalúa cuántos sistemas tecnológicos críticos han sido identificados y priorizados	# sistemas críticos identificados / # sistemas críticos reales
6	RESPALDOS CONFIGURADOS	Evalúa la disponibilidad y preparación del entorno alterno de respaldo	# sistemas críticos respaldados / # total sistemas críticos
7	PRUEBA DE ESCRITORIO DE ESCENARIOS DRP	Mide la prueba de escenarios alineados con el plan de recuperación	# Pruebas de escritorio de escenarios realizadas / # Total escenarios definidos
8	INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Gestión adecuada de los incidentes de seguridad de la información presentados en la entidad	# incidentes mitigados / # incidentes detectados

5. Lineamientos de seguridad para herramientas tecnológicas críticas.
Definición de guías de seguridad y hardening para tres componentes esenciales de la operación tecnológica: el servidor intermedio Bastion Host, la plataforma de virtualización y la puerta de enlace de acceso remoto; este trabajo incluyó la definición de una línea base de seguridad, recomendaciones priorizadas y criterios de protección alineados con las necesidades operativas.
La principal contribución es la entrega de un marco técnico práctico y aplicable, que fortalece la postura de ciberseguridad, reduce la superficie de exposición y proporciona directrices claras para la protección de herramientas clave del entorno tecnológico, facilitando su adopción, operación y mantenimiento continuo.

6. Metodología integral para la selección de herramientas de seguridad.
Marco holístico y estandarizado que guía la evaluación, la comparación y la selección de herramientas de seguridad, alineando las decisiones tecnológicas con las necesidades del negocio y las condiciones operativas; establece un proceso estructurado que abarca la definición de requisitos, criterios de evaluación, análisis de alternativas y valoración técnica, hasta llegar a una toma de decisiones fundamentada y transparente. Este componente aporta un modelo replicable y de alto valor práctico, que facilita decisiones tecnológicas coherentes, reduce la subjetividad en los procesos de adquisición y proporciona una base metodológica sólida para futuras implementaciones de soluciones de ciberseguridad.

VII. Requerimientos

Requerimientos funcionales

- Estructurar un plan de despliegue por etapas, incluyendo la definición de hitos, responsables y plazos para la implementación de los controles.
- Mantener actualizado el Roadmap del proyecto frente a cambios derivados de nuevos riesgos, ajustes tecnológicos o modificaciones en la infraestructura.
- Diseñar y ejecutar una prueba de concepto (POC) para validar la viabilidad técnica, operativa y procedimental del DRP, utilizando un entorno controlado basado en la emulación de la infraestructura crítica.
- Alinear el proceso de gestión integral de incidentes de ciberseguridad con las estrategias de recuperación y continuidad operativa.
- Incorporar requerimientos adicionales que puedan ser necesarios, y que sean planteados y consensuados por las partes involucradas.

Requerimientos no funcionales

- Promover la alineación de la implementación del SGSI con estándares internacionales contemplados en la Fase I como ISO/IEC 27001 y el modelo MSPI, facilitando la interoperabilidad y la integración con otras organizaciones que adopten marcos equivalentes.

- Adaptar las recomendaciones normativas seleccionadas para la implementación del SGSI y DRP dentro del contexto particular de la Organización.
- Proteger todas las evidencias, documentos y artefactos generados durante el proyecto, mediante cifrado en tránsito y en reposo conforme a buenas prácticas.
- Mantener trazabilidad completa de las actividades ejecutadas, haciendo uso de registros auditables que documenten cambios, usuarios involucrados y fechas asociadas.
- La implementación del SGSI y DRP debe ser flexible y escalable, permitiendo la incorporación de nuevos controles, riesgos o fases del proyecto sin afectar la estabilidad del sistema o la continuidad del proyecto.
- Implementar un repositorio seguro para el almacenamiento centralizado de documentos, evidencias, el SoA y demás artefactos del proyecto, con controles de acceso adecuados.
- Configurar entornos de prueba aislados (ya sea mediante máquinas virtuales o laboratorios dedicados) que permitan ejecutar la PoC del DRP sin comprometer la infraestructura productiva.

Requerimientos técnicos

- Utilizar tecnologías que garanticen la protección de la propiedad intelectual, datos y procesos de la institución, considerando la relevancia misional de la Organización y las amenazas potenciales.
- Verificar que las tecnologías utilizadas durante el proyecto cuenten con aval institucional, tanto a nivel de seguridad como de madurez tecnológica, soporte y alineación con buenas prácticas y compatibilidad con la infraestructura existente.

VIII. Propuesta de innovación

La propuesta de innovación consiste en diseñar e implementar la emulación de componentes críticos de la infraestructura tecnológica, entendida como la capacidad en replicar, dentro de un entorno controlado y seguro, el funcionamiento de los sistemas, servicios y elementos esenciales que soportan las operaciones misionales. Esta emulación permite reproducir la arquitectura, el comportamiento operativo y las interdependencias de la infraestructura física y lógica, sin afectar el ambiente productivo.

El objetivo principal es probar, validar y anticipar cómo responderían los componentes institucionales frente a escenarios realistas de riesgo, fallas operativas o incidentes de ciberseguridad. Al disponer de un entorno virtual que reproduce los servicios críticos y sus mecanismos de protección, es posible evaluar el impacto de diferentes amenazas, identificar vulnerabilidades, verificar estrategias de continuidad y recuperación y optimizar los tiempos de respuesta.

Esta aproximación aporta un valor significativo en materia de ciberseguridad, resiliencia y continuidad operativa, permitiendo:

- Analizar el comportamiento del sistema frente a fallas de hardware, interrupción de conectividad, saturación de servicios o configuraciones erróneas.
- Validar plan de continuidad y DRP sin comprometer la operación real.
- Simular procesos de crecimiento, incorporación de nuevas dependencias o actualizaciones de infraestructura, evitando riesgos sobre los activos productivos.
- Identificar brechas, dependencias frágiles y configuraciones débiles mediante experimentación controlada.
- Ejecutar ataques controlados (penetration testing), evaluar amenazas emergentes y estudiar escenarios de intrusión en un ambiente aislado.
- Detectar vulnerabilidades futuras que aún no han sido explotadas en el entorno real, anticipándose a tendencias de amenazas y nuevas técnicas de ataque.
- Evaluar el impacto y la eficacia de controles de ciberseguridad sin comprometer activos productivos.
- Probar configuraciones de endurecimiento en componentes de la infraestructura tecnológica.
- Facilitar ejercicios de red team, blue team, simulacros de ataque y prácticas de respuesta a incidentes.
- Ajustar reglas de correlación, validar umbrales, reducir falsos positivos y comprobar flujos de ingestión de logs.
- Ejecutar playbooks reales, midiendo tiempos de reacción, desempeño de roles y efectividad técnica de las acciones realizadas.

En el marco de la Fase II del proyecto, se acordó con el equipo de la Entidad diseñar e implementar un MVP que permita emular los componentes críticos priorizados de la infraestructura tecnológica, sirviendo como punto de partida para pruebas, validaciones y futuras iteraciones del entorno de emulación.

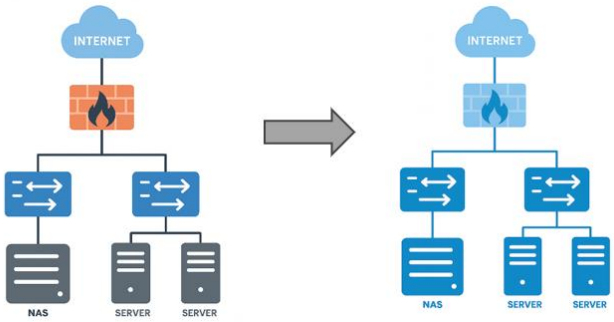

Fig. 1 Infraestructura tecnológica a emular

A continuación se presenta detalle de la propuesta de innovación, donde se abordan tres componentes: el diseño de la emulación, que establece la arquitectura, funcionalidad y componentes técnicos necesarios; la implementación de la emulación, donde se mencionan los mecanismos y servicios que permiten su funcionamiento; y la gestión de cambios que define el proceso para asegurar la trazabilidad y control ante cualquier modificación.

a. Diseño de la emulación

El diseño de la emulación constituye el núcleo teórico de la propuesta de innovación, ya que define la arquitectura, los componentes y las capacidades necesarias para replicar el comportamiento de la infraestructura priorizada en un entorno

controlado. Dentro de la emulación, se encuentran dos proyectos:

digital-infrastructure: Aprovisionamiento automatizado de infraestructura permitiendo desplegar entornos consistentes, reproducibles y seguros, entre sus componentes se incluye:

- Docker [8] como base de containerización.
- GNS3 [9] y Containerlab [10] para emulación de redes y dispositivos.
- code-server para desarrollo y gestión remota.
- Infraestructura PKI para certificados y cifrado.
- Nginx [11] con HTTPS para asegurar las comunicaciones.

digital-dashboard: Destinado a ofrecer la interfaz web de supervisión y gestión, permitiendo a los usuarios interactuar con la emulación de forma centralizada. Sus funcionalidades comprenden:

- Monitoreo de métricas críticas (CPU, memoria, disco, red).
- Canvas interactivo para visualización de topologías mediante Cytoscape.js. [12]
- Gestión de laboratorios usando herramientas oficiales como gns3web y code-server. [13]
- API REST para integración y automatización de operaciones.
- Mecanismos de autenticación para control seguro de accesos.

Tareas

Se especifican a continuación las tareas del sistema, orientadas a garantizar el funcionamiento de la emulación:

TABLA II
TAREAS DEL SISTEMA

N°	Tarea	Proyecto	Actor
T1	Aprovisionar infraestructura desde cero	Infrastructure	CI/CD Pipeline
T2	Monitorear métricas del sistema	Dashboard	Operador
T3	Visualizar topología de red activa	Dashboard	Operador/Desarrollador
T4	Crear/editar topologías YAML	Infrastructure (code-server)	Desarrollador
T5	Desplegar nueva versión del dashboard	Dashboard	CI/CD Pipeline
T6	Consultar estado de labs GNS3/Containerlab	Dashboard API	Sistema externo
T7	Realizar backup antes de deploy	Dashboard	CI/CD Pipeline

Usuarios y roles

Como parte fundamental de la propuesta de innovación, la definición de usuarios y roles dentro de la plataforma de emulación permite establecer límites de acceso, garantizar la trazabilidad de las acciones y minimizar riesgos operativos derivados de configuraciones inadecuadas o accesos no autorizados. La asignación diferenciada asegura que cada actor interactúe únicamente con los componentes necesarios para su función, protegiendo la integridad del entorno emulado y fortaleciendo los mecanismos de gobierno del sistema.

A continuación, se describen los roles propuestos y sus principales capacidades dentro de la plataforma:

TABLA III
USUARIOS Y ROLES

Rol	Permisos	Acceso a
Administrador de Sistemas	Completo (infraestructura + dashboard)	• Servidor vía SSH • GitLab CI/CD • Todos los servicios
Operador de Red	Solo acceso al dashboard	• Dashboard web (autenticado) • Visualización de métricas y topologías
Desarrollador/Ingeniero	Lectura en dashboard + escritura en code-server	• Dashboard web • code-server para editar topologías en Containerlab • GNS3 Web
Sistema Externo (API)	Solo endpoints API específicos	• API REST del dashboard • Topology Agent API

A continuación, se muestra la topología de red unificada, diseñada para emular la infraestructura crítica y para realizar las pruebas del DRP, donde:

- El lado izquierdo contiene servicios y aplicaciones que representan el entorno principal.
- El lado derecho representa la infraestructura alterna o de respaldo.
- La conexión entre ambos permite simular la recuperación ante desastres y evaluar la resiliencia del sistema.

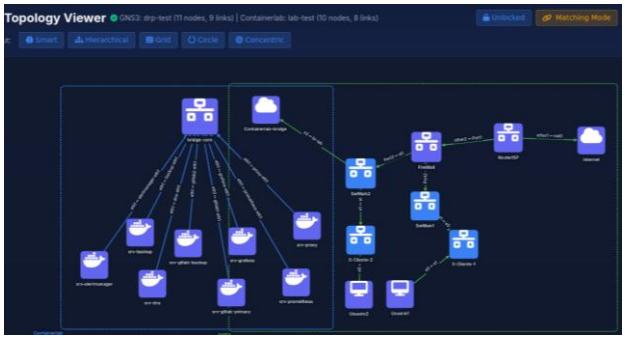

Fig. 2 Topología unificada (Topology viewer) en Dashboard.

Componentes

La arquitectura de la plataforma de emulación está compuesta por varios elementos que interactúan de manera coordinada para permitir la creación, gestión y monitoreo de laboratorios en un entorno controlado.

Uno de los elementos centrales es el Topology Agent, el cual actúa como un puente crítico entre el Dashboard (que opera dentro de un contenedor) y los servicios de virtualización nativos que residen en el host como GNS3 y Containerlab, su función es facilitar un acceso seguro a las APIs y a las interfaces de línea de comandos (CLI) de estos servicios, evitando exponer directamente el host o permitir accesos no controlados desde el container aislado.

TABLA IV
COMPONENTES

Compo-nente	Tecnolo-gía	Puerto	Ejecución	Función	Proyecto
Nginx	Nginx 1.18+	443, 8001	Host (nativo)	Reverse proxy HTTPS	Infrastruc-ture
PKI	OpenSS L	-	Host (nativo)	CA privada + Certificad os SSL	Infrastruc-ture
Dashbo-ard	Flask 3.0	8080	Docker container	UI web + API REST	Dashboard
Topolo-gy Agent	Flask (micro)	5001	Host (systemd)	Enlace: Dashboar d <-> GNS3/Co ntainerlab	Dashboard
GNS3 Server	Python	3080	Host (nativo)	Emulació n de dispositiv os de red	Infrastruc-ture
Contai-nerlab	Go	-	Host (nativo)	Simulació n con containers	Infrastruc-ture
Code-server	TypeScri pt	8443	Host (nativo)	VS Code Web	Infrastruc-ture
Docker Engine	Go	-	Host (nativo)	Runtime (Dashboar d + containers de red)	Infrastruc-ture

La interfaz de Containerlab es una herramienta usada para crear, visualizar y administrar topologías de red basadas en contenedores. La siguiente imagen muestra múltiples servicios interconectados, lo que permite ver al usuario: topología completa con nodos y conexiones, estado de cada contenedor, flujo de red entre servicios y estado en tiempo real, como logs, arranque y ejecución.

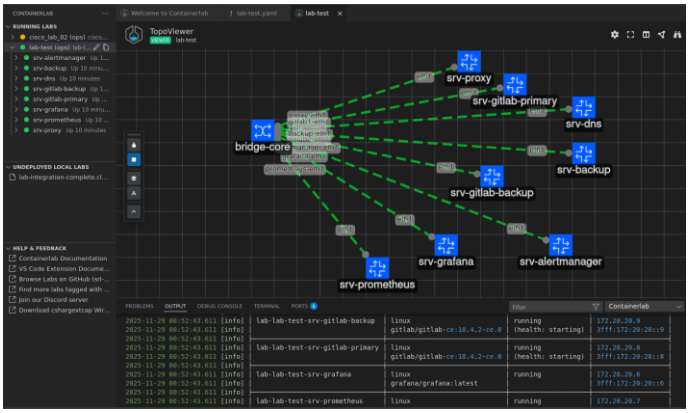

Fig. 3 Administrador de Topología de contenedores.

A continuación, se muestra la topología de red con los componentes críticos emulada en GNS3, que es una herramienta que permite diseñar, probar y validar arquitecturas de red completas. La topología está representada de manera jerárquica representando el flujo natural desde Internet – proveedor – firewall – red interna.

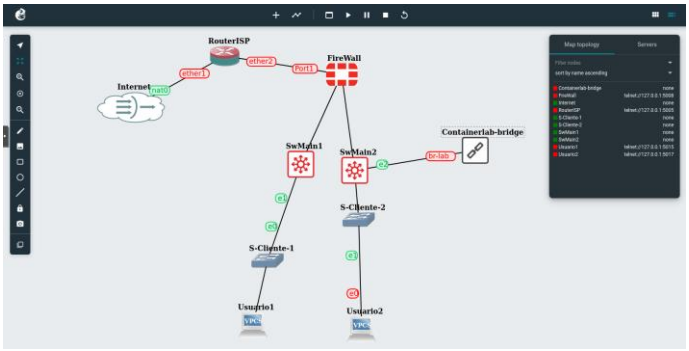

Fig. 4 Administrador de Topología en GNS3.

Arquitectura

La arquitectura de la plataforma se organiza en 5 capas principales:

- Capa de usuario: Incluye los componentes mediante los cuales los usuarios interactúan con el sistema:
  - ✓ Navegador Web (Dashboard UI): Permite visualizar el estado de la emulación, métricas, topologías y modelos.
  - ✓ Herramientas (SSH, code-server, GNS3 Web): Facilitan la conexión a servidores, la edición de archivos, la ejecución de scripts y la administración de configuraciones necesarias para los laboratorios.
- Capa de seguridad: Mecanismos que garantizan la protección del tráfico y la integridad de la plataforma:
  - ✓ Reverse Proxy HTTPS: Gestiona certificados PKI (con CA privada), aplica TLS para el cifrado del tráfico y enruta todas las solicitudes hacia la capa de aplicación.
  - ✓ Security Headers: Se aplican cabeceras como: HSTS, X-Frame-Options, X-Content-Type-Options y CSP, los cuales protegen contra ataques de downgrade, inyección, man-in-the-middle y clickjacking
- Capa de aplicación: Agrupa los servicios operativos que habilitan el funcionamiento de la emulación. Esta capa combina servicios desplegados en contenedores Docker y servicios instalados directamente en el host (sistemas nativos).
- Capa de virtualización: Herramientas base que permiten ejecutar las topologías emuladas:
  - ✓ Docker Engine: Administra la ejecución de contenedores del Dashboard y de los servicios auxiliares, así como las redes internas y los bridges de comunicación.
  - ✓ GNS3 Server: Servicio nativo que implementa QEMU/KVM y virtualización de routers y firewalls
  - ✓ Containerlab: Orquestador de topologías de red basado en contenedores, utiliza archivos YAML como topology-data.json para la configuración declarativa de la infraestructura emulada.
- Capa de Infraestructura: Sistema operativo base y servicios fundamentales que soportan toda la emulación.
  - ✓ Sistema operativo Ubuntu, que incluye Firewall (UFW) y reglas para puertos configurados.

- ✓ PKI (CA privada + certificados RSA), utilizada para firmar los certificados del Dashboard, del reverse proxy y de los servicios internos.
- ✓ Usuarios del sistema: Entre ellos gitlab-runner, automation y usuarios operativos empleados para CI/CD o tareas de automatización.

Cada una de estas capas cumple funciones específicas que habilitan la capacidad de la plataforma para modelar infraestructura crítica, ejecutar topologías virtuales, proporcionar herramientas de análisis, gestionar contenedores y proteger el flujo de datos bajo buenas prácticas de ciberseguridad.

b. Implementación de la emulación

Herramientas

Las herramientas utilizadas en la plataforma ofrecen una arquitectura modular que separa de manera clara las capas de backend, frontend e infraestructura; este enfoque permite mantener un sistema ordenado y fácilmente extensible, entre los beneficios se destaca:

- Modularidad: Cada componente cumple funciones específicas sin generar dependencias rígidas.
- Escalabilidad: Tecnologías como Docker y GitLab [14] permiten desplegar, replicar y mantener los servicios de forma eficiente, garantizando crecimiento controlado.
- Visualización avanzada: Cytoscape.js ofrece capacidades óptimas para representar gráficamente redes, infraestructuras y sistemas complejos dentro del Dashboard, favoreciendo el análisis y la comprensión de las topologías emuladas.
- Automatización: Herramientas como Ansible [15] y las canalizaciones CI/CD minimizan errores humanos, y aceleran los despliegues.

TABLA V
HERRAMIENTAS

Categoría	Herramienta	Versión	Uso
Backend	Flask	3.0.0	Framework web principal
	Python	3.10.12	Lenguaje de programación
	psutil	>= 7.0.0	Recolección de métricas
Frontend	HTML/CSS/JS	-	Interfaz de usuario
	Cytoscape.js	3.28.1	Visualización de topologías
	Font Awesome	6.4.0	Iconografía
IaC/DevOps	Ansible	>= 8.0.0	Automatización
	GitLab CI/CD	-	Pipelines de despliegue
	Docker	24.0.7	Containerización

c. Gestión de cambios de la emulación

El entorno de emulación permite replicar componentes críticos, validar controles de seguridad, simular incidentes y evaluar escenarios del DRP. Dada su relevancia estratégica como plataforma de pruebas, capacitación y validación de configuraciones, es fundamental asegurar que cualquier modificación en este entorno se gestione de manera controlada, trazable y alineada con los lineamientos del SGSI.

Para preservar la integridad del entorno de emulación y prevenir cambios no autorizados o inconsistentes, se adopta un proceso formal de gestión de cambios. Este proceso define actividades, responsabilidades y flujos de aprobación que permiten evaluar el impacto técnico y de seguridad de cada modificación, asegurar su correcta documentación y mantener la coherencia con los objetivos del SGSI y del DRP. A continuación, se detallan los roles y responsabilidades.

TABLA VI
ROLES Y FUNCIONES

Rol	Responsabilidad
Administrador del Entorno de Emulación (AEE)	Encargado de Proxmox, GNS3, Containerlab y ejecución de cambios técnicos.
Responsable de Seguridad de la Información (RSI)	Valida riesgos, controles y cumplimiento del SGSI/DRP.
Comité de Cambios (CAB)	Autoridad de aprobación y decisiones finales.

La siguiente matriz RACI detalla los roles involucrados y su nivel de participación en cada una de las actividades del proceso de control de cambios.

TABLA VII
MATRIZ RACI GESTIÓN DE CAMBIOS

Actividad	AEE	RSI	CAB
Solicitar e identificar el cambio	R	C	I
Documentar el requerimiento del cambio	R	C	I
Realizar análisis técnico y de seguridad	R	R	I
Revisar conjuntamente el cambio	R	C	I
Aprobar el cambio	C	C	A
Planear y ejecutar el cambio	R	I	I
Realizar pruebas posteriores a la implementación	R	C	I
Generar documentación final y cierre	R	C	A

IX. Conclusiones

- La ejecución de la Fase II permitió avanzar significativamente en la maduración del Sistema de Gestión de Seguridad de la Información y el Plan de Recuperación ante Desastres de la entidad, al establecer la hoja de ruta para las siguientes fases.
- La implementación del entorno de emulación se consolida como un habilitador estratégico de la ciberseguridad, permitiendo simular fallas, ataques y configuraciones inseguras, validar controles antes de su despliegue en producción y probar mejoras de seguridad sin afectar los sistemas reales.
- Los indicadores definidos en esta fase permiten medir el desempeño del SGSI mediante métricas trazables, facilitando la toma de decisiones, la priorización de

riesgos y la justificación técnica de inversiones futuras. El sistema de métricas es adaptable al nivel de madurez actual y escalable para ciclos posteriores.

- Se fortaleció la gestión de incidentes de seguridad, gracias al diseño de un proceso formal y a la definición de una Matriz RACI que clarifica responsabilidades y agiliza la respuesta operativa ante eventos de ciberseguridad.
- DRP unificado y actualizado, alineado al negocio y orientado a la acción, representa una actividad que aporta un marco documental robusto y fácilmente gestionable, que fortalece la preparación organizacional y facilita la adopción, mantenimiento y activación del DRP.
- El proyecto, en conjunto, posiciona a la Entidad para avanzar hacia un entorno más seguro, resiliente y eficiente, alineado con estándares internacionales y preparado para responder de manera oportuna a riesgos emergentes y escenarios de contingencia

REFERENCIAS

[1] "Diseño e implementación del SGSI y diseño del DRP para una entidad pública del estado colombiano." Accessed: Aug. 27, 2025. [Online]. Available: https://sistemas.uniandes.edu.co/maestrias/mesi/proyectos/proyecto.php?id=214

[2] "Colombia ciberataques." Accessed: Aug. 27, 2025. [Online]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-tuvo-mas-de-5-000-intentos-de-ciberataques-al-inicio-del-2023-796252

[3] "Colombia sufrió 12.000 millones de intentos de ciberataques en 2023 según reporte de Fortinet - CCIT - Cámara Colombiana de Informática y Telecomunicaciones." Accessed: Aug. 27, 2025. [Online]. Available: https://www.ccit.org.co/blog/colombia-sufrio-12-000-millones-de-intentos-de-ciberataques-en-2023-segun-reporte-de-fortinet/

[4] "Indicadores de Seguridad de la Información y Ciberseguridad 2024." Accessed: Aug. 28, 2025. [Online]. Available: https://www.superfinanciera.gov.co/publicaciones/10115571/indicadores-de-seguridad-de-la-informacion-y-Ciberseguridad-2024/

[5] "ISO 27001 Controls: Overview of all measures from Annex A." Accessed: Aug. 28, 2025. [Online]. Available: https://www.dataguard.com/iso-27001/annex-a/controls/

[6] "IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs." Accessed: Aug. 27, 2025. [Online]. Available: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

[7] B. von Solms y R. von Solms, "The 10 deadly sins of information security management," Computers & Security, vol. 23, no. 5, pp. 371-376, Jul. 2004. Accessed: Nov. 18, 2025. [Online]. Available: doi:10.1016/j.cose.2004.05.002.

[8] "Manuales — Documentación de Docker," Docker Docs. Accessed: 02-Dec-2025. [Online]. Available: https://docs.docker.com/manuals/

[9] "Getting Started with GNS3 | GNS3 Documentation," GNS3 Docs. Accessed: Dec. 02, 2025. [Online]. Available: https://docs.gns3.com/docs/.

[10] "Topology Definition File — Containerlab," Containerlab Documentation. Accessed: Dec. 02, 2025. [Online]. Available: https://containerlab.dev/manual/topo-def-file/.

[11] "Documentation — NGINX," NGINX. [Online]. Accessed: 02-Dec-2025. Available: https://nginx.org/en/docs/index.html.

[12] "Cytoscape.js," Cytoscape.js Documentation. Accessed: 02-Dec-2025. [Online]. Available: https://js.cytoscape.org/.

[13] "coder/code-server: VS Code in the browser," GitHub. Accessed: 02-Dec-2025. [Online]. Available: https://github.com/coder/code-server.

[14] "gitlab-com / organization," GitLab.com. Accessed: 02-Dec-2025. [Online]. Available: https://gitlab.com/gitlab-com.

[15] "Ansible Documentation," Ansible Docs. Accessed: 02-Dec-2025. [Online]. Available: https://docs.ansible.com/.