Fortalecimiento de la Ciberseguridad Institucional mediante la identificación de amenazas en Deep & Dark web

Autores:
Leidy Tatiana Soler Páez
Leidy Yanire Cordero Silva
Liana Carolina Montaña Carpintero
Luis Andrés Tibata Urrego

Profesor:
Cristhian Fabián Ruiz Ramos

Programa:
Especialización en Gerencia de Proyectos de Servicios con Tic

Escuela de Administración

7/11/2025
Bogotá, Colombia

2025

Declaramos bajo gravedad de juramento, que hemos escrito el presente proyecto integrador de especialización por nuestra propia cuenta, y que, por lo tanto, su contenido es original. Declaramos que hemos indicado clara y precisamente todas las fuentes directas e indirectas de información, y que este proyecto integrador de especialización no ha sido entregado a ninguna otra institución con fines de calificación o publicación.

Leidy Tatiana Soler Páez
Leidy Yanire Cordero Silva
Liana Carolina Montaña Carpintero
Luis Andrés Tibatá Urrego

Fecha: 07/11/2025

Declaración de exoneración de responsabilidad: “Declaro(amos) que la responsabilidad intelectual del presente trabajo es exclusivamente de su(s) autor(es). La Universidad del Rosario no se hace responsable de contenidos, opiniones o ideologías expresadas total o parcialmente en él”.

Leidy Tatiana Soler Páez
Leidy Yanire Cordero Silva
Liana Carolina Montaña Carpintero
Luis Andrés Tibatá Urrego

Fecha: 07/11/2025

Antecedentes

Antecedentes

- Aumento de Ciberataques
- Sector Educativo como blanco

Ambiente actual

- Amenazas cibernéticas en crecimiento
- Mayor digitalización.

Necesidades y problemas

- Falta de monitoreo de amenazas
- Riesgo de filtraciones

Oportunidades de mejoramiento

- Identificación de amenazas en Deep & Dark web
- Reducir tiempos de respuesta ante incidentes de seguridad.

Antecedentes

De acuerdo con un estudio realizado por diferentes compañías de ciberseguridad Colombia ocupa el puesto 29 a nivel mundial y el cuarto lugar en Latinoamérica entre los países más atacados en 2025. Dentro de los sectores más vulnerables se encuentra el sector educativo debido a la falta de inversión en ciberseguridad y a la escasez de talento especializado.

1

Algunas Universidades han sufrido ataques como:

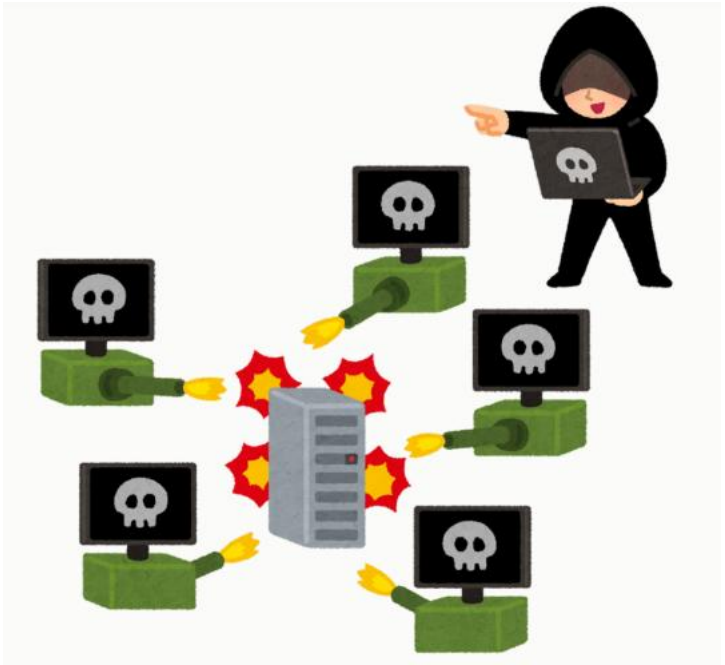
ente:

Fuente: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/primer-simposio-internacional-de-ciberseguridad-del-2024-donde-y-cuando-860448

https://muchohacker.lol/2023/01/universidades-colombianas-bajo-el-ataque-de-ciberdelincuentes/

2

- Universidad El Bosque: sufre ataque y eliminaron importante información:



Fuente: https://www.semana.com/confidenciales/articulo/hackearon-el-portal-de-la-universidad-del-bosque-y-eliminaron-importante-informacion/202125/

https://forbes.co/2021/06/28/actualidad/hackean-a-la-universidad-el-bosque-y-dicen-haber-borrado-rastros-de-calificaciones

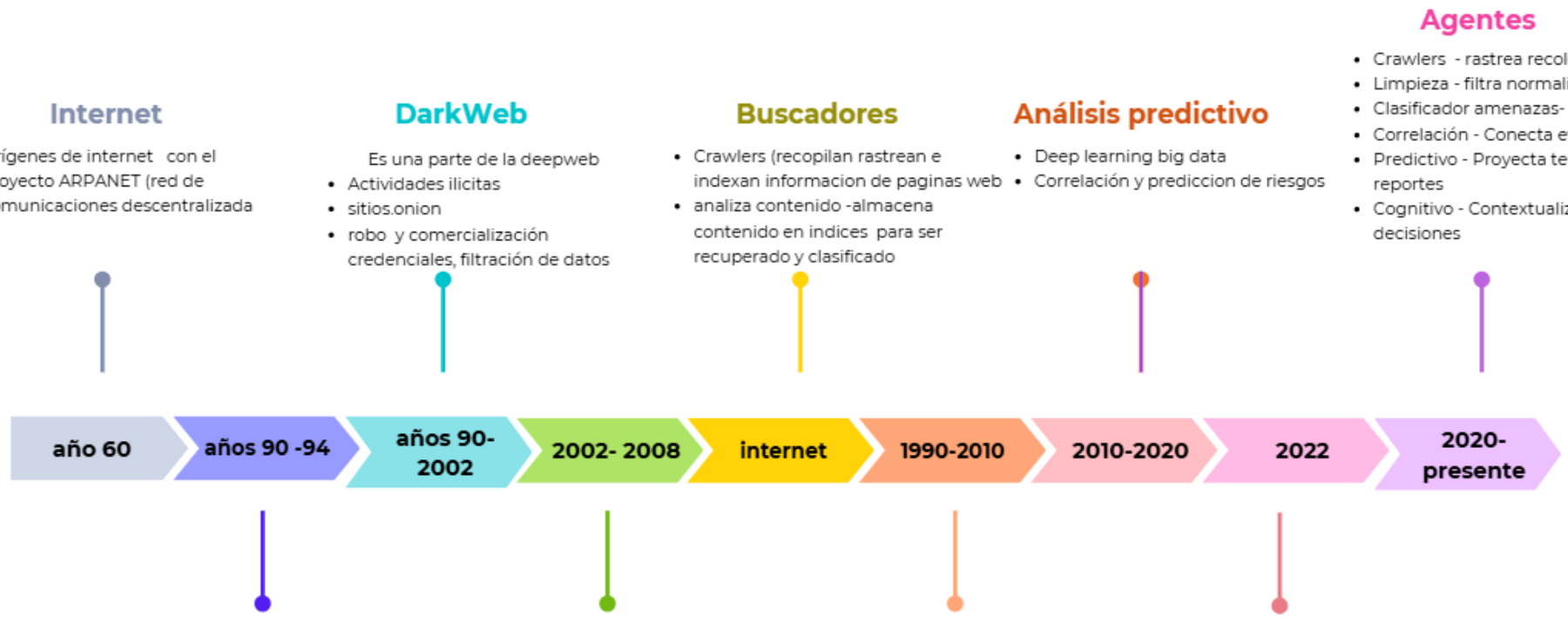
3

- Universidad de la Salle: Pérdida y publicación de información, como pasaportes, de miembros de la comunidad educativa.

Fuente: https://muchohacker.lol/2023/01/universidades-colombianas-bajo-el-ataque-de-ciberdelincuentes/
https://muchohacker.lol/2023/02/publican-informacion-robada-a-la-universidad-de-la-salle/

Marco Teórico

Universidad del Rosario



https://www.youtube.com/watch?v=7OrMheKzuL4&t=382

Objetivo General:

Consolidar una herramienta de monitorización que se apoye en algoritmos y agentes de inteligencia artificial capaces de escanear motores de búsqueda no indexados en la Deep Web y la Dark Web permitiendo detectar filtraciones de información confidencial, sensible y menciones de la Universidad del Rosario.

*"La plataforma de monitoreo con inteligencia artificial "bucea" en esas capas profundas (Deep y Dark Web) para **detectar credenciales filtradas, amenazas o información comprometida**, permitiendo reaccionar antes de que afecte a la Universidad del Rosario."*

Objetivos estratégicos del proyecto

Identificar de manera oportuna las credenciales filtradas y menciones relacionadas con la Universidad del Rosario en espacios en la Deep/Dark Web.

Implementar una estrategia híbrida que permita combinar enfoques algorítmicos automáticos y profundos. (AI + Validación humana)

Diseñar un sistema de alertas que clasifique las amenazas según su nivel de riesgo y criticidad.

Reducir el porcentaje de información que se encuentra expuesta en la Deep/Dark Web.

Alcance

CUBRE

01 Recolección de información en sitios .onion a través de TOR.

02 Tratamiento automatizado y contextual de la información recolectada.

03 Emisión de alertas clasificadas de acuerdo con su nivel de riesgo y criticidad.

04 Centralización de la información mediante un tablero de mando.

05 Manual técnico de uso.

NO CUBRE

01 Intervención legal o rastreo ofensivo de ciberdelincuentes.

02 Monitoreo de redes sociales o web superficial.

03 Análisis de tráfico interno en la red institucional.

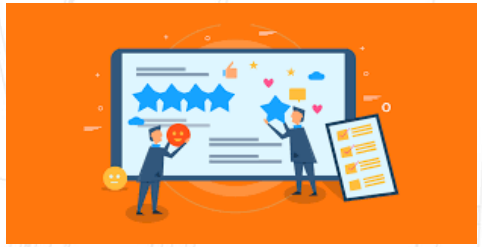
Beneficios

Protección Proactiva

Optimización y Ahorro

Prevención

Automatización



Reputación

Cumplimiento Normativo

Impacto del proyecto

Si NO se desarrolla la idea

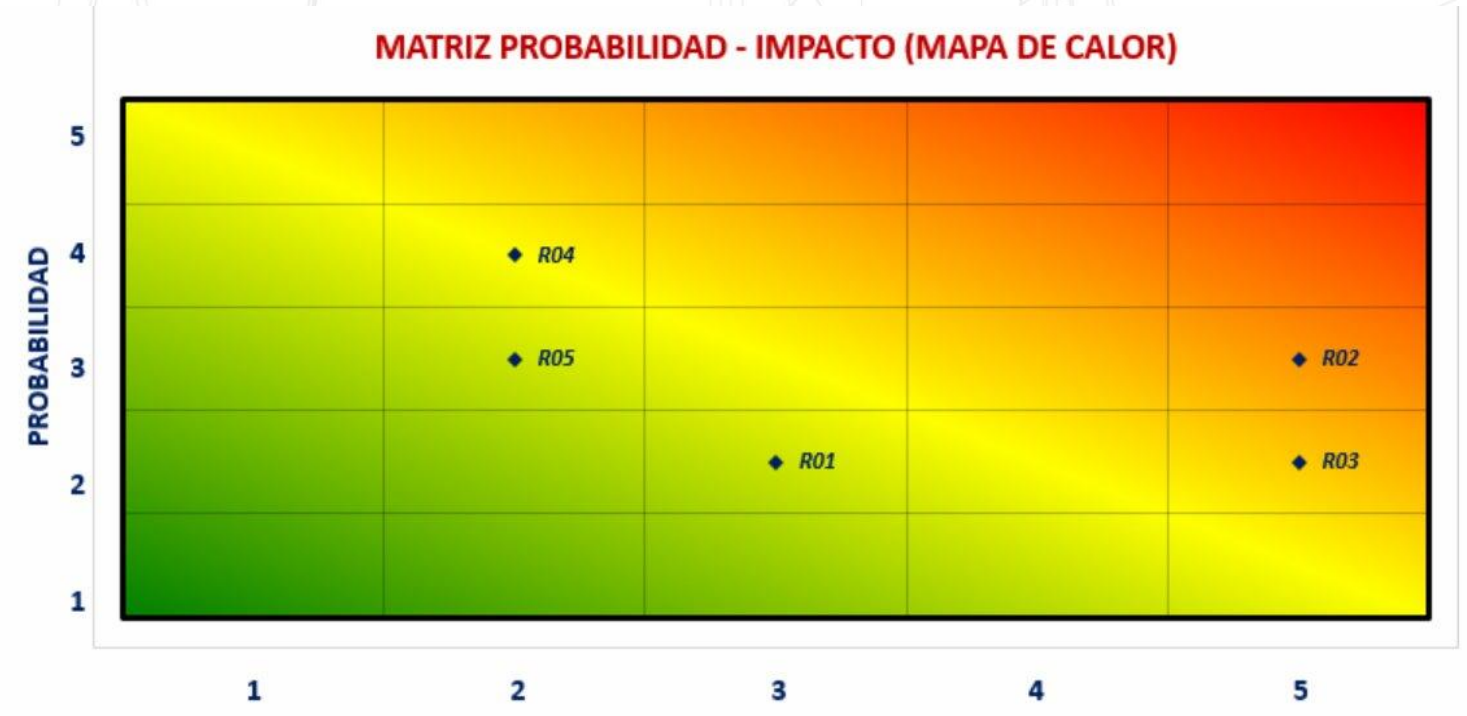
- Mayor riesgo de filtración de datos en la Deep/ Dark Web
- Incremento de fraudes y robo de identidad en la Comunidad Rosarista.
- Daño reputacional y perdida de confianza de estudiantes y afiliados.
- Posibles sanciones legales por incumplir normas de protección de datos.

Ventajas al implementarlo

- Prevención proactiva de incidentes y filtraciones.
- Protección de la Información de estudiantes, docentes y personal administrativo
- Alertas en tiempo real para actuar de inmediato
- Cumplimiento de estándares internacionales de ciberseguridad
- Ahorro de costos por incidentes o sanciones

Riesgos del proyecto

No. Riesgo	DESCRIPCIÓN	Prob.	Imp.
R01	Retraso en la implementación del sistema de monitoreo	2	3
R02	Implementar un sistema que no supla las necesidades de la universidad	3	5
R03	Fallas en la integración de la herramienta con los sistemas internos de la univ	2	5
R04	Ampliar el uso de la herramienta para monitoreo preventivo de otras amenaza	4	2
R05	Resistencia al cambio por parte del personal y usuarios	3	2



Pre- requisitos

Universidad del Rosario

- Definición y aprobación del alcance del proyecto 01
- Prueba de concepto POC 02
- Definición de presupuesto y recursos 03
- Verificación de antecedentes 04

Cumplimiento normativo

Norma / Marco Legal	Obligación Principal	Cumplimiento con la Herramienta
Ley 1581 de 2012 (Habeas Data – Colombia)	Proteger datos personales	Monitoreo enfocado en credenciales institucionales.
Ley 1273 de 2009 (Delitos Informáticos – Colombia)	Prevenir y denunciar accesos no autorizados	Detecta venta de credenciales y accesos indebidos; facilita denuncias
Política Nacional de Seguridad Digital (MinTIC, 2016-2023)	Promover la ciberseguridad en instituciones	Fortalece monitoreo y respuesta temprana
ISO/IEC 27001	Controles para seguridad de la información	Apoya gestión de riesgos, fugas y respuesta a incidentes
NIST Cybersecurity Framework	Identificar, proteger, detectar y responder	Contribuye a fases de identificación, detección y respuesta

Factores clave de éxito

Universidad del Rosario

01

Apoyo de la alta dirección Rectoría - Dirección de TI

Compromiso de Rectoría y Dirección de TI para priorizar el proyecto y asignar recursos

02

Equipo multidisciplinario especializado Líder de proyecto / Gestión Humana

Contar con expertos e ciberseguridad, IA, desarrollo de software y legal

03

Cumplimiento normativo y ético Área Jurídica / Oficial de cumplimiento

Adecuación a la Ley 1581/2012, GDPR e ISO 27001 para manejo de datos

04

Infraestructura tecnológica robusta Dirección de TI / Arquitecto de sistemas

Servicios seguros red confiable y herramientas de IA escalables

05

Capacitación y gestión de cambio Líder de proyecto / Recurso humano

Entrenamiento a usuarios y socialización para aceptación de la plataforma

06

Monitoreo y mejora continua / Líder de proyecto / Equipo de Ciberseguridad

Seguimiento de métricas y KPIs, retroalimentación para optimizar la plataforma

Factores clave de éxito

Táctica

Cómo haremos realidad el proyecto y lo diferenciaremos de lo tradicional

Metodología Ágil: Trabajaremos por fases cortas, entregando avances continuos que permitan ajustar el sistema según los resultados.

AI Adaptativa: La inteligencia artificial aprenderá del comportamiento de los datos para mejorar la detección de amenazas con el tiempo.

Monitoreo multifuente: La plataforma recolectará información desde la Deep Web, Dark Web y otras fuentes para dar una visión completa.

MVP: Se desarrollará una versión inicial funcional para probar el sistema antes de la implementación total.

Co –creación: Involucraremos a expertos en ciberseguridad, estudiantes y administrativos de la universidad en el diseño y validación.

Capacitación: Se entrenará a los usuarios para usar la herramienta y comprender las alertas de riesgo generadas.

Entregables

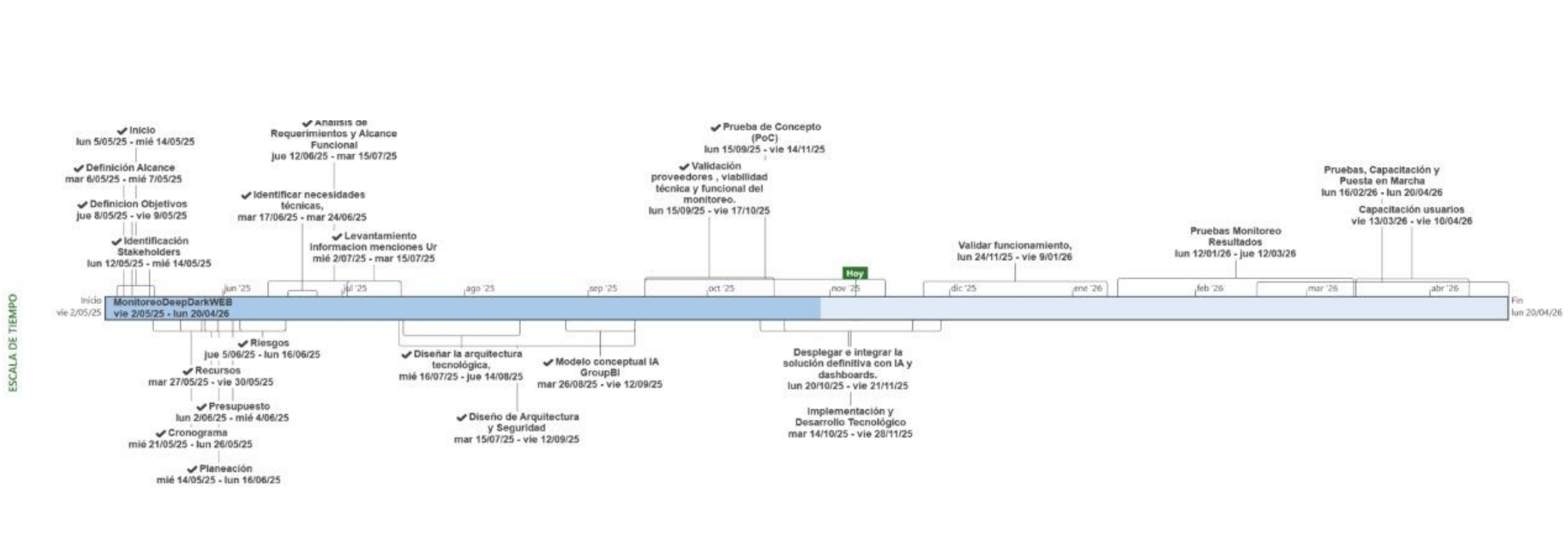
Universidad del Rosario

- FORTALECIMIENTO DE LA CIBERSEGURIDAD IDENTIFICACION DE AMENAZAS EN DEEP & DARK WEB
  - INICIO
    - Definición de alcance
    - Objetivos estratégicos.
    - Identificación de stakeholders
    - Matriz de interesados (RACI).
  - VIABILIDAD TECNICA Y FINANCIERA
    - POC
    - Análisis de costos
    - (software, infraestructura, licencias, nube).
    - Análisis de retorno
  - PLANEACIÓN
    - Cronograma detallado (Gantt).
    - Plan de riesgos (Matriz de riesgo inherente, residual, estrategias).
  - IMPLEMENTACION
    - Arquitectura Técnica
    - Desarrollo e Integración
    - Pruebas funcionales y de seguridad
  - CIERRE
    - Evaluación de Resultados
    - Transferencia de Conocimiento

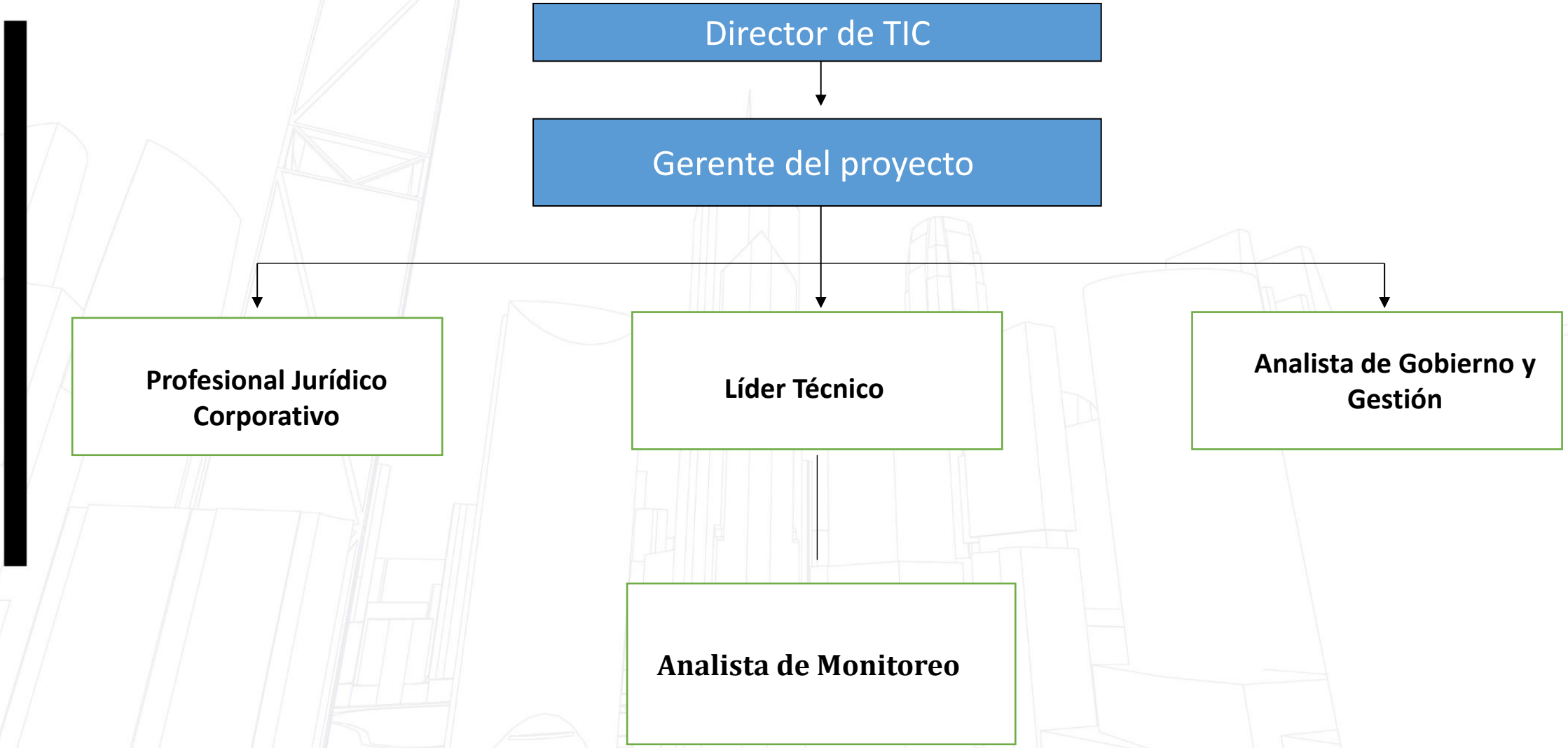
Indicadores preliminares

Tipo de indicar	Indicador	Definición	Resp.	Valor esperado	Como se pude medir
GESTIÓN	Cumplimiento del cronograma	Porcentaje de actividades completadas en las fechas previstas del plan de proyecto	Líder de proyecto	95%	Seguimiento en herramienta de gestión
SEGUIMIENTO	Exactitud de detección	Porcentaje de alertas verdaderas frente a el total de alertas emitidas por la plataforma	Equipo de ciberseguridad	90%	Comparación de alertas con validación manual.
IMPACTO	Reducción de incidentes	Disminución de incidentes de filtración de datos reportados tras la implementación.	Dirección de TI	30% de reducción en 12 mese	Registros de incidentes de seguridad TI.
SEGUIMIENTO	Tiempo promedio de respuesta	Tiempo promedio entre alerta y acción de contención	CSIRT universitario	1 Hora	Logs de plataforma y CSIRT
GESTIÓN	Nivel de adopción de usuarios	Porcentaje de personal de TI que utiliza la plataforma de forma activa y continua.	Talento Humano / TI	85 %	Registros de uso y encuestas internas

Línea de tiempo



Estructura del proyecto



Presupuesto preliminar

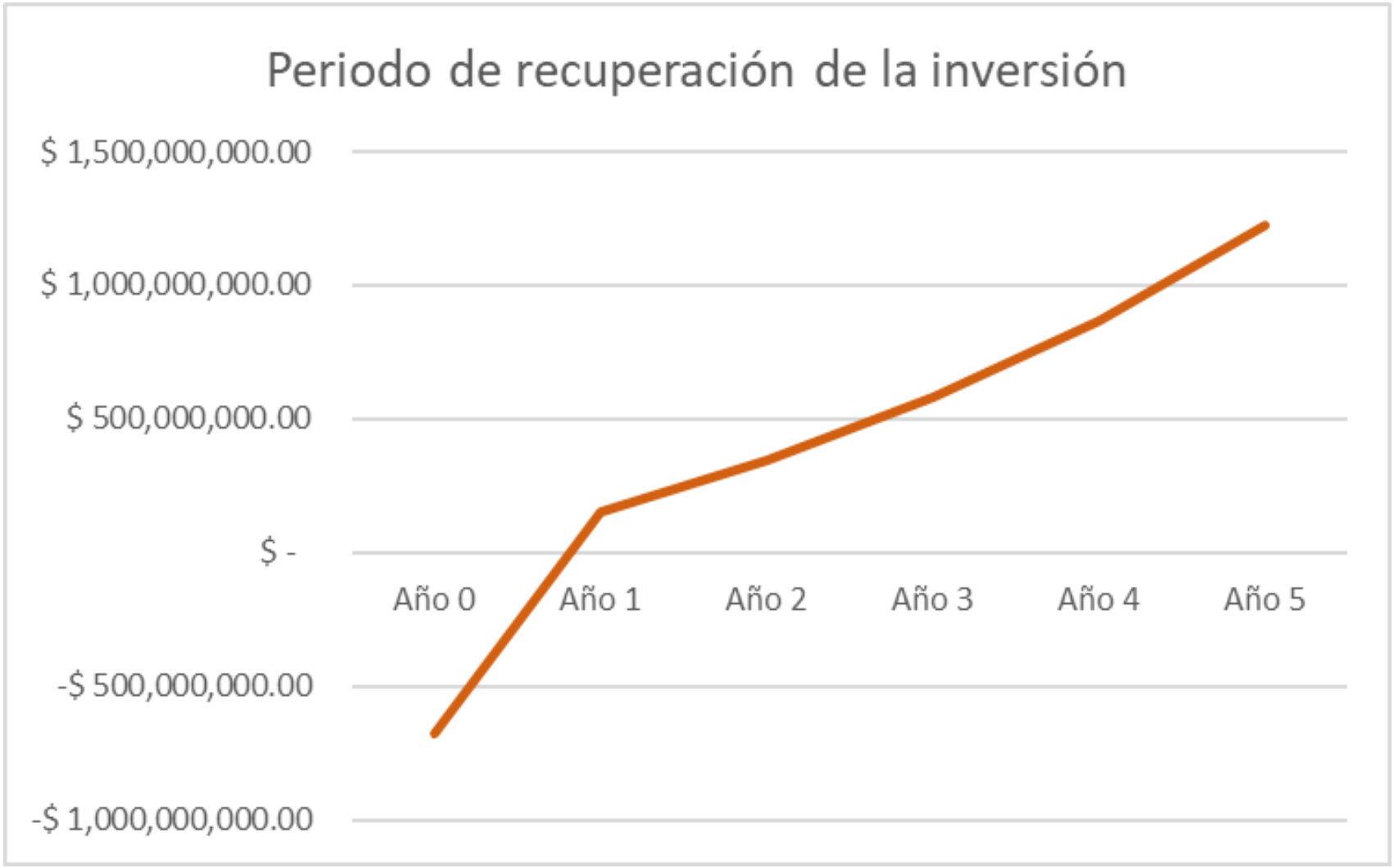
Categoría	Descripción	Naturaleza	Tipo de Costo	Valor Proyecto	% del proyecto
Recursos Humanos (RRHH)	Salarios + prestaciones de los tres cargos definidos	Fijo	Directo	$ 306.000.000	45%
Tecnología (Group-IB)	Licencia, Soporte anual, infraestructura virtual	Fijo	Directo	$ 220.000.000	32%
Servicios tercerizados	Consultoría técnica, capacitación, acompañamiento	Variable	Directo	$ 50.000.000	7%
Infraestructura institucional	Conectividad, energía, seguridad física	Fijo	Indirecto	$ 40.000.000	6.5%
Capacitación	Formación inicial y continua del personal	Variable	Indirecto	$ 20.000.000	3%
Riesgos	Riesgos que pueden ser materializados	Fijo	Indirecto	$ 40.000.000	6.5%
TOTAL, ESTIMADO PROYECTO				$ 676.000.000	

Justificación financiera

BENEFICIOS DEL PROYECTO						
	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Ingresos Operacionales	-	$ 523,000,000.00	$ 627,600,000.00	$ 753,120,000.00	$ 903,744,000.00	$ 1,084,492,800.00
(-) Gastos Operacionales		$ 78,450,000.00	$ 94,140,000.00	$ 112,968,000.00	$ 135,561,600.00	$ 162,673,920.00
(=) Utilidad bruta		$ 444,550,000.00	$ 533,460,000.00	$ 640,152,000.00	$ 768,182,400.00	$ 921,818,880.00
(-) Gastos administrativos		$ 52,300,000.00	$ 62,760,000.00	$ 75,312,000.00	$ 90,374,400.00	$ 108,449,280.00
(=) EBITDA		$ 392,250,000.00	$ 470,700,000.00	$ 564,840,000.00	$ 677,808,000.00	$ 813,369,600.00
(-) Gasto en depreciación		$ -	$ -	$ -	$ -	$ -
(=) Utilidad operacional		$ 392,250,000.00	$ 470,700,000.00	$ 564,840,000.00	$ 677,808,000.00	$ 813,369,600.00
(+) Intereses recibidos		$ -	$ -	$ -	$ -	$ -
(=) EBIT		$ 392,250,000.00	$ 470,700,000.00	$ 564,840,000.00	$ 677,808,000.00	$ 813,369,600.00
(-) Intereses pagados		$ -	$ -	$ -	$ -	$ -
= UAI		$ 392,250,000.00	$ 470,700,000.00	$ 564,840,000.00	$ 677,808,000.00	$ 813,369,600.00
(-) Impuestos		$ 129,442,500.00	$ 155,331,000.00	$ 186,397,200.00	$ 223,676,640.00	$ 268,411,968.00
= Utilidad neta		$ 262,807,500.00	$ 315,369,000.00	$ 378,442,800.00	$ 454,131,360.00	$ 544,957,632.00
(-) Dividendos pagados		$ 105,123,000.00	$ 126,147,600.00	$ 151,377,120.00	$ 181,652,544.00	$ 217,983,052.80
Total beneficios		$ 523,000,000.00	$ 627,600,000.00	$ 753,120,000.00	$ 903,744,000.00	$ 1,084,492,800.00
Total Costos		$ 365,315,500.00	$ 438,378,600.00	$ 526,054,320.00	$ 631,265,184.00	$ 757,518,220.80
Flujo neto		$ 157,684,500.00	$ 189,221,400.00	$ 227,065,680.00	$ 272,478,816.00	$ 326,974,579.20
= Utilidad retenida	-$ 676,000,000.00	$ 157,684,500.00	$ 189,221,400.00	$ 227,065,680.00	$ 272,478,816.00	$ 326,974,579.20

VPN DEL PROYECTO	$ 39,559,269.27
TASA INTERNA DE RETORNO	12.33%

Justificación financiera



Conclusiones

Con este proyecto de monitoreo de la Deep y Dark Web, la Universidad del Rosario contará con una herramienta que fortalece la prevención de incidentes, la vigilancia en tiempo real y la gestión de riesgos cibernéticos.

La integración de algoritmos automáticos y de aprendizaje profundo permitirá detectar amenazas de forma oportuna y mejorar la respuesta institucional ante posibles filtraciones de información sensible.

Finalmente, este proyecto integrador permitió aplicar los conocimientos de la especialización en un caso real, convirtiéndose en un activo estratégico para la protección y reputación digital de la Universidad.

Referencias Bibliográficas

Bajonero Vásquez, G. (2024, marzo 1). *Así será el primer Simposio Internacional de Ciberseguridad del 2024 (¿Dónde y cuándo?)*. *El Tiempo*. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/primer-simposio-internacional-de-ciberseguridad-del-2024-donde-y-cuando-860448

ColdFusion. (2023, marzo 15). *What are AI Agents? A Primer* [Video]. YouTube. https://www.youtube.com/watch?v=EmZhVOi22l4

Confecámaras. (2025). *Universidad del Rosario*. Red de Beneficios para Afiliados. https://confecamaras.org.co/beneficio-afiliado/universidad-del-rosario

Forbes Staff. (2021, junio 28). *Hackean a la Universidad El Bosque y atacantes dicen haber borrado rastros de calificaciones*. *Forbes Colombia*. https://forbes.co/2021/06/28/actualidad/hackean-a-la-universidad-el-bosque-y-dicen-haber-borrado-rastros-de-calificaciones

Hernandez, J. (2025, 10 de marzo). *Brecha de datos en la dark web: cómo responder y proteger tu información*. https://preyproject.com/es/blog/brecha-de-datos-dark-web?
Universidad del Rosario. (s. f.). *Pilares de transformación*. https://urosario.edu.co/pilares-de-transformacion

Hyperconectado. (2023, 5 de enero). *Universidades colombianas bajo el ataque de ciberdelincuentes*. MuchoHacker. https://muchohacker.lol/2023/01/universidades-colombianas-bajo-el-ataque-de-ciberdelincuentes/

Hyperconectado. (2023, febrero 17). *Publican información robada a la Universidad de la Salle*. MuchoHacker.LOL. https://muchohacker.lol/2023/02/publican-informacion-robada-a-la-universidad-de-la-salle

Molina, N. (2025, 25 de septiembre). *El impacto de los ciberataques en universidades de Latinoamérica*. Hackmetrix Blog. https://blog.hackmetrix.com/ciberataques-en-universidades-de-latinoamerica/?

Redacción Confidenciales. (2024, 7 de noviembre). *Hackearon el portal de la Universidad del Bosque y eliminaron importante información*.
Semana. https://www.semana.com/confidenciales/articulo/hackearon-el-portal-de-la-universidad-del-bosque-y-eliminaron-importante-informacion/202125/

S4vitar. (2023, 23 de agosto). *Deep Web: El lado más oscuro de internet* [Video]. YouTube. https://www.youtube.com/watch?v=7OrMheKzuL4

Universidad Católica de Colombia. (2025, 15 de septiembre). *La otra pandemia: el crecimiento de los ciberataques en Colombia y cómo hacerles frente*.
https://www.ucatolica.edu.co/portal/la-otra-pandemia-el-crecimiento-de-los-ciberataques-en-colombia-y-como-hacerles-frente/