UNIVERSIDAD NACIONAL DE TUMBES

ESCUELA DE POSGRADO

DOCTORADO EN ESTADÍSTICA MATEMÁTICA APLICADA

Modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en instituciones públicas del Ecuador, 2022.

TESIS

Para optar por el grado académico de Doctor en Estadística Matemática Aplicada

Autor

Richard Romero Izurieta

Tumbes, 2023

UNIVERSIDAD NACIONAL DE TUMBES

ESCUELA DE POSGRADO

DOCTORADO EN ESTADÍSTICA MATEMÁTICA APLICADA

Modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en instituciones públicas del Ecuador, 2022.

Tesis aprobada en forma y estilo por:

Dr. Jesús Merino Velásquez (Presidente) _____

Dr. Severino Apolinar Risco Zapata (Secretario) _____

Dr. Raúl Alfredo Sánchez Ancajima (Vocal) _____

Dr. Luis Jhony Caucha Morales (Asesor) _____

Tumbes, 2023

UNIVERSIDAD NACIONAL DE TUMBES

ESCUELA DE POSGRADO

DOCTORADO EN ESTADÍSTICA MATEMÁTICA APLICADA

Modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en instituciones públicas del Ecuador, 2022.

Los suscritos declaramos que la tesis es original en su contenido y forma

Mg. Romero Izurieta Richard (Autor) _____

Código ORCID 0002-3387-6661

Dr. Luis Jhony Caucha Morales (Asesor) _____

Código ORCID 0002-4786-9008

Dr. Segundo Moisés Toapanta Toapanta (Coasesor) _____

Código ORCID 0002-9041-0518

Tumbes, 2023

Acta de revisión y sustentación de tesis

UNIVERSIDAD NACIONAL DE TUMBES
Licenciada
Resolución del Consejo Directivo N° 155-2019-SUNEDU/CD
ESCUELA DE POSGRADO
Tumbes – Perú

ACTA DE SUSTENTACION DE TESIS

En Tumbes, siendo las dieciséis horas del catorce de noviembre del dos mil veintidós, se reunieron mediante la modalidad virtual por plataforma de videoconferencia zoom, los miembros del jurado en mérito a la **Resolución N° 0150-2022/UNTUMBES-EPG-D**, del veinticinco Dr. Jesús, Merino Velásquez (presidente), Dr. Severino Apolinar Risco Zapata (secretario), Dr. Raúl Alfredo Sánchez Ancajima (vocal) y como asesor el Dr. Luis Jhony Caucha Morales, para proceder al acto de sustentación y defensa de la tesis titulada: **"Modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en instituciones públicas del Ecuador, 2022"**; presentada por el Mg. Richard Romero Izurieta, para optar el grado académico de Doctor en Estadística y Matemática Aplicada.

Concluido el acto de sustentación y defensa, absueltas las preguntas formuladas y efectuadas las correspondientes observaciones. En conformidad con lo normado en el artículo 91. del Reglamento de Tesis para Pregrado y Posgrado de la Universidad Nacional de Tumbes. El jurado calificador por unanimidad decidió declarar a la tesis del Mg. Richard Romero Izurieta.

APROBADA -MUY BUENA

En consecuencia, queda **APTO** para continuar con los trámites correspondientes a la obtención del Grado Académico de Doctor en Estadística y Matemática Aplicada, de conformidad con lo estipulado en la Ley Universitaria N° 30220, el Estatuto, Reglamento General, Reglamento de Grados y Títulos y Reglamento de Tesis para Pregrado de la Universidad Nacional de Tumbes.

Siendo las diecisiete horas y cincuenta minutos, se dio por concluido el indicado acto académico y en expresión de conformidad se procedió a la suscripción de la presente acta.

Tumbes, 14 de noviembre de 2022.

Dr. Jesús Merino Velásquez
DNI N° 00240035
ORCID N° 0000-0003-3301-4487
(Presidente)

Dr. Severino Apolinar Risco Zapata
DNI: 00219860.
ORCID: 0000-0002—2683-4105
(Secretario)

Dr. Raúl Alfredo Sánchez Ancajima
DNI: 40834005
ORCID: 0000-0003-3341-7382
Vocal

Dr. Luis Jhony Caucha Morales
DNI N°—03585602
ORCID: 0000-0002-4786-9008
(Asesor)

C.c. Jurado de Tesis (3), Asesor (1), sustentante (1), UI (2)

Agradecimiento

En primer lugar, a Dios y a mi padre que esta junto a él por ser mis guías.

A mi esposa e hijos por su apoyo y comprensión, por quitarles un poco de tiempo para lograr terminar este objetivo académico.

A los docentes de Posgrado del Doctorado en Estadística Matemática Aplicada de la Universidad Nacional de Tumbes por los conocimientos y experiencias compartidas en el aula de clases.

A mis asesores, Dr. Luis Caucha y al PhD. Moises Toapanta por su asesoramiento, tanto en esta tesis doctoral, en las ponencias y artículos científicos que realizamos para comunicar a la comunidad científica nuestros resultados.

A los Miembros del Tribunal por los conocimientos compartidos y su apoyo incondicional.

A la Universidad Nacional de Tumbes, sus autoridades, directivos y colaboradores que apoyaron los procesos académicas y administrativos para hacer realidad este sueño.

Informe de Originalidad del Turnitin

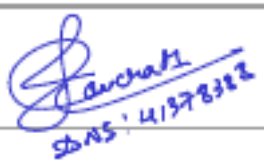
Modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en instituciones públicas del Ecuador, 2022.

INFORME DE ORIGINALIDAD

12%	11%	3%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Estatal de Milagro Trabajo del estudiante	2%
2	repositorio.untumbes.edu.pe Fuente de Internet	1%
3	repositorio.ugto.mx Fuente de Internet	1%
4	dspace.unach.edu.ec Fuente de Internet	1%
5	Submitted to Universidad Nacional de Tumbes Trabajo del estudiante	1%
6	prezi.com Fuente de Internet	1%
7	hdl.handle.net Fuente de Internet	<1%
8	doaj.org Fuente de Internet	<1%



índice general

Índice de tablas

Índice de figuras

Índice de anexos

RESUMEN

Los problemas de seguridad de la información en las organizaciones públicas son persistentes; una de las causas es la escasez de modelos y métodos adecuados para medir la eficiencia de los procesos relacionados con la seguridad informática y la rentabilidad económica de las inversiones en TI. El objetivo de este trabajo es la eficiencia de la gestión de selección de proyectos estratégicos para garantizar mejorar la seguridad de la información de una organización pública. Dado un conjunto de proyectos estratégicos para mejorar la seguridad de la información de una organización pública, el modelo propuesto determina un subconjunto de proyectos a ejecutar en un período de tiempo, para el uso eficiente de los recursos limitados de la organización. Se aplicó una metodología de investigación de enfoque cuantitativa, de tipo aplicada, con diseño de investigación observacional correlacional transversal. Como resultado se obtuvo un modelo matemático que optimiza dos objetivos: maximizar el porcentaje de mejora en seguridad de la información de los proyectos planificados y minimizar los costos de la organización; la implementación en lenguaje Python del algoritmo genético de clasificación No dominada NSGA-II, que brinda a través del frente de Pareto las mejores soluciones que pueden ser consideradas por los Directores de TI. Se concluyó que el modelo de optimización presentado es eficiente, la selección de un subconjunto de proyectos estratégicos permite mejorar la seguridad de la información de una organización pública, en un rango de 85.30% a 89.00%, considerando las limitaciones presupuestarias de la organización, tales como mostrado por las métricas de la simulación realizada. El modelo propuesto es bastante simple de implementar, muy práctico y puede ser un instrumento adecuado para elegir la solución más eficiente, considerando los objetivos y limitaciones de una organización pública.

Palabras Clave: Optimización multiobjetivo, Algoritmo Genético, Seguridad de la Información, Modelo matemático, NSGA-II.

ABSTRACT

Information security problems in public organizations are persistent; One of the causes is the scarcity of adequate models and methods to measure the efficiency of processes related to computer security and the economic profitability of IT investments. The objective of this work is the efficiency of the selection management of strategic projects to guarantee the improvement of the information security of a public organization. Given a set of strategic projects to improve the information security of a public organization, the proposed model determines a subset of projects to be executed in a period of time, for the efficient use of the organization's limited resources. A quantitative approach research methodology was applied, of an applied type, with a cross-sectional correlational observational research design. As a result, a mathematical model was obtained that optimizes two objectives: maximizing the percentage of improvement in information security of the planned projects and minimizing the organization's costs; the implementation in Python language of the NSGA-II Non-dominated classification genetic algorithm, which provides through the Pareto front the best solutions that can be considered by IT Directors. It was concluded that the optimization model presented is efficient, the selection of a subset of strategic projects allows to increase the information security of a database of a public organization, in a range of 85.30% to 89.00%, considering the budgetary limitations. of the organization, such as shown by the metrics of the simulation carried out. The proposed model is quite simple to implement, very practical and can be a suitable instrument to choose the most efficient solution, considering the objectives and limitations of a public organization.

Keywords: Multi-objective optimization, Genetic Algorithm, Information Security, Mathematical model, NSGA-II.

RESUMO

Os problemas de segurança da informação em organizações públicas são persistentes; Uma das causas é a escassez de modelos e métodos adequados para medir a eficiência dos processos relacionados à segurança de computadores e a rentabilidade econômica dos investimentos em TI. O objetivo deste trabalho é a eficiência da gestão de seleção de projetos estratégicos para garantir a melhoria da segurança da informação de uma organização pública. Dado um conjunto de projetos estratégicos para melhorar a segurança da informação de uma organização pública, o modelo proposto determina um subconjunto de projetos a serem executados em um período de tempo, para o uso eficiente dos limitados recursos da organização. Aplicou-se uma metodologia de pesquisa de abordagem quantitativa aplicada, com um desenho de pesquisa observacional correlacional transversal. Como resultado, obteve-se um modelo matemático que otimiza dois objetivos: maximizar o percentual de melhoria na segurança da informação dos projetos planejados e minimizar os custos da organização; a implementação em linguagem Python do Algoritmo Genético de Classificação Não Dominada NSGA-II, que fornece através da frente de Pareto as melhores soluções que podem ser consideradas pelos Diretores de TI. Concluiu-se que o modelo de otimização apresentado é eficiente, a seleção de um subconjunto de projetos estratégicos permite aumentar a segurança da informação de um banco de dados de uma organização pública, na faixa de 85,30% a 89,00%, considerando as limitações orçamentárias. organização, como mostram as métricas da simulação realizada. O modelo proposto é bastante simples de implementar, muito prático e pode ser um instrumento adequado para escolher a solução mais eficiente, considerando os objetivos e limitações de uma organização pública.

Palavras-chave: Otimização multiobjetivo, Algoritmo Genético, Segurança da Informação, Modelo matemático, NSGA-II.

CAPITULO I: INTRODUCCIÓN

El gobierno de TI que implementan las organizaciones públicas no es adecuado para medir la efectividad y eficiencia de las tareas de seguridad para las empresas, necesitan definir objetivos y métricas.(Antoniou 2018; Bitzer, Brinz, and Ollig 2021; Masilela and Nel 2021; Musa 2018; Nyonawan, Suharjito, and Utama 2018; Skrodelis, Strebko, and Romanovs 2020; Sönmez 2019; Yasin et al. 2020; Zaydi and Nassereddine 2018)

Según Schatz & Bashroush (2017), consideran que es difícil identificar enfoques clave y prácticos que permitan optimizar la seguridad informática. Para Kirenberg et al. (2020), es fundamental la necesidad de utilizar modelos y métodos de optimización para la resolución de problemas de seguridad informática y económica en una empresa.

Hashemi et al. (2017), menciona que proporcionar seguridad y privacidad debe estar de acuerdo con las limitaciones de la organización, principalmente de tipo económicas. Algunos investigadores tales como Apelt et al. (2018), Girón (2020), Saiya & Arman (2018), Yastrub & Kredentsar (2018), Yilmaz & Matthes (2021) consideran que las organizaciones deben adoptar una arquitectura empresarial que permitan optimizar sus procesos para alinear todos sus recursos con la misión, visión, estrategias, objetivos y necesidades organizacionales.

Es fundamental una perspectiva estratégica de la dirección de TI para que las empresas sean competitivas, así como tener modelos y herramientas de apoyo a las decisiones que permitan la correcta elección y priorización de proyectos en base a criterios y limitaciones de la organización.(Bushuyev et al. 2021; Klakegg 2017; Mylnikov 2022; Ranjbar, Nasiri, and Torabi 2022; Reis et al. 2020; Tselios and Ipsilandis 2018)

Encontraron varias carencias de seguridad en las organizaciones, sobre todo en lo concerniente a planificación, documentación, análisis de riesgos, revisiones,

auditorias, defensa física, protección virtual, y capacitación de sus empleados (Diesch, Pfaff, and Krcmar 2020; Szczepaniuk et al. 2020).

Todas las evidencias mencionadas nos permiten entender la problemática de las organizaciones públicas de Ecuador en temas de ciberseguridad, que las hacen muy vulnerables ante las amenazas actuales. Es necesario proveer a estas organizaciones de herramientas y soluciones para fortalecer la gestión de TI, que permitan asumir las funciones de brindar los servicios a la población y custodiar la información pública conforme lo exigen las leyes ecuatorianas.

A fin de solucionar la problemática se planteó que la aplicación de un modelo de optimización de la selección de proyectos estratégicos de ciberseguridad permitirá mejorar la seguridad de la información y el uso eficiente de los recursos de una organización pública de Ecuador.

En este contexto se aplicó un enfoque de computación evolutiva, como es el algoritmo genético de clasificación no dominada NSGA-II, para resolver el problema de optimización multiobjetivo de selección de portafolio de proyectos de ciberseguridad para mejorar la seguridad de la información, considerando las variables de decisión a los proyectos estratégicos de ciberseguridad, y criterios técnicos y económicos que permitan clasificar y priorizar los proyectos. Para validar el modelo se implementará el algoritmo en lenguaje Python, se simulará un escenario de prueba, con datos de proyectos estratégicos de ciberseguridad planificados para aumentar la seguridad de la información de una organización pública del Ecuador.

1.1. Situación problemática

Las organizaciones públicas de Ecuador se rigen por un marco legal que determina las responsabilidades de administrar información pública sensible que se genera de la interacción con la comunidad. Tenemos a la “Ley Orgánica de Empresas Públicas” que garantiza la eficiencia, racionalidad, calidad y seguridad de la información (Asamblea Nacional del Ecuador 2009). La “Ley Orgánica de Transparencia y Acceso a la Información Pública” que determina el derecho a la información de personas y entidades sobre los registros públicos (Asamblea Nacional del Ecuador 2004). Todas las organizaciones públicas de Ecuador deben cumplir con lo establecido en las normas de control interno en temas de protección de la información, que se traduce en características de “confidencialidad, integralidad, y disponibilidad” (CID) de la información(Contraloría General del Estado 2009).

En la revisión de la literatura encontramos propuestas con diferentes puntos de vista para solucionar los problemas de seguridad encontrados en organizaciones (Pernul (1994), Trivedi et al. (2016), Hoffmann et al. (2020), Gupta et al. (2020), Joshi et al. (2020), AlYousef & Abdelmajeed (2019), (Miao et al. 2020), Toapanta et al.(2018), Al-Matari et al. (2020)), pero, así como hay nuevos modelos y metodologías, también las amenazas son cada vez mayores y con muchas variantes a nivel tecnológico y social. Para enfrentar estos desafíos las organizaciones deben asumir un enfoque holístico y sistémico de la seguridad, para proteger sus bienes críticos, incluyendo la capacidad de mejoramiento continuo de su gestión(Szczepaniuk et al. 2020).

Debido a la pandemia del COVID-19 se incrementó la actividad digital en todas las actividades humanas, como trabajos, en la educación, etc., que provoco una mayor cantidad de ataques cibernéticos en los países de América del sur y el Caribe, con daños calculados en US$6 billones en el año 2021, cifra que sobrepasa al PIB de cualquier país en vías de desarrollo (BID - OEA, 2020). En la Tabla I podemos observar los indicadores en Capacidad de Ciberseguridad del Modelo de Madurez (CCMM) para Ecuador en el año 2020, se muestra procesos en periodo formativo que todavía no se consolidan.

Tabla I: Indicadores del CCMM Ecuador 2020

Dimensión	Factor	Nivel	Etapa
1. Política y Estrategia de Ciberseguridad	1 Estrategia Nacional de Ciberseguridad	2	Formativa
	2 Respuesta a Incidentes	2	Formativa
	3 Protección de Infraestructura Crítica (IC)	1	Inicial
	4 Gestión de Crisis	1	Inicial
	5 Defensa Cibernética	2	Formativa
	6 Redundancia de Comunicaciones	1	Inicial
2. Cultura Cibernética y Sociedad	1 Mentalidad de Ciberseguridad	2	Formativa
	2 Confianza y Seguridad en Internet	2	Formativa
	3 Comprensión del Usuario de la Protección de Información Personal en Línea	1	Inicial
	4 Mecanismos de Presentación de Informes	1	Inicial
	5 Medios y Redes Sociales	1	Inicial
3. Educación, Capacitación y Habilidades en Ciberseguridad	1 Sensibilización	2	Formativa
	2 Marco para la Educación	2	Formativa
	3 Marco para la Formación Profesional	2	Formativa
4. Marcos Legales y Regulatorios	1 Marcos Legales	2	Formativa
	2 Sistema de Justicia Penal	2	Formativa
	3 Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético	2	Formativa
5. Estándares, Organizaciones y Tecnologías	1 Adhesión a los Estándares	2	Formativa
	2 Resiliencia de Infraestructura de Internet	3	Consolidado
	3 Calidad del Software	1	Inicial
	4 Controles Técnicos de Seguridad	2	Formativa
	5 Controles Criptográficos	1	Inicial
	6 Mercado de Ciberseguridad	1	Inicial
	7 Divulgación Responsable	1	Inicial

Fuente: (BID - OEA, 2020).

En Ecuador existe un plan realizado por el Ministerio de Telecomunicaciones para fortalecer la ciberseguridad a nivel de país, que realiza evaluaciones y seguimiento en las empresas públicas para incrementar la confianza de la ciudadanía en la utilización de los servicios digitales y de información pública(MINTEL, 2018, p. 66).

Esta investigación aporta a la necesidad de las organizaciones públicas de Ecuador de gestionar y prevenir los incidentes de ciberseguridad, partiendo de un esquema de planificación estratégica que permita determinar los proyectos que se deben implementar; se propone un modelo para optimizar la selección de los proyectos estratégicos en ciberseguridad que se pueden ejecutar para mejorar la seguridad de la información, mediante la utilización eficiente de recursos disponibles.

1.2. Planteamiento del problema

¿Un modelo de optimización para la selección de proyectos de ciberseguridad permitirá mejorar la seguridad de la información y uso eficiente de los recursos del estado en las instituciones públicas del Ecuador?

1.3. Justificación de la investigación

Existen muchas limitaciones de carácter normativo, falta de recursos y a nivel cognitivo que impiden una gestión eficiente de ciberseguridad y un adecuado análisis de riesgos. Según Deloitte (2020), el 90 % de las empresas ecuatorianas asumen que la seguridad informática es un riesgo que puede afectar de manera importante las actividades de su negocio.

Según ESET (2020), las organizaciones en América Latina consideran que los controles de acceso no son adecuados, porque el 60% de estas empresas reporto al menos un evento no deseado de seguridad. En Ecuador la situación es más alarmante, el 70% de organizaciones reporto un evento no deseado de seguridad.

El índice nacional de seguridad cibernética deja a Ecuador en la posición 80 de 160 países, y el Índice SAINT (Systemic Analyzer in Network Threats) lo ubica 207 de 218 países(e-Governance Academy Foundation 2019).

Actualmente no se dispone de modelos adecuados de optimización en la selección de proyectos en ciberseguridad, que permita mejorar la seguridad de la información

mediante la utilización eficiente de recursos. Este trabajo propone un aporte mediante modelos de optimización en el área de la seguridad de la información de las organizaciones públicas de Ecuador.

La situación actual de las organizaciones públicas del Ecuador, con un alto riesgo de ataques y vulnerabilidades, sumado a las deficiencias en herramientas de gestión y la falta de una planificación estratégica, hacen vulnerable a estas organizaciones. Por tal motivo el modelo planteado en el presente proyecto permitirá mejorar la seguridad de la información de las organizaciones públicas del Ecuador.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Desarrollar un Modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en instituciones públicas del Ecuador.

1.4.2. Objetivos específicos

1. Analizar el estado actual de la seguridad de la información de las empresas públicas sujetas al poder ejecutivo y tomar como caso de estudio dos organizaciones públicas estratégicas.
2. Analizar las principales variables y factores a considerar para clasificar y priorizar proyectos en ciberseguridad.
3. Diseñar y desarrollar un modelo matemático de optimización para la selección de proyectos en ciberseguridad para mejorar la seguridad de la información y el uso eficiente de recursos en organizaciones públicas del Ecuador.
4. Validar el modelo de optimización para la selección de proyectos en ciberseguridad mediante simulaciones.

CAPITULO II: ESTADO DEL ARTE

Las organizaciones aumentan constantemente su atención en temas de seguridad para proteger sus activos críticos y todo lo relacionado con los datos sensibles que administran. Para contrarrestar las constantes amenazas y vulnerabilidades es necesario contar con nuevas estrategias, aplicar las mejores prácticas de TI, adquirir tecnología de punta e implementar políticas y procedimientos adecuados, que se incluyan en una gestión de mejora continua. La globalización, el internet, las redes sociales y el desarrollo de las Tics ha producido un sin fin de servicios masivos, pero también tiene muchas desventajas, principalmente en incidentes de ciberseguridad. Las investigaciones actuales en el área de seguridad informática ya no se limitan a problemas de tecnología, ahora tiene un alcance holístico, amplio, sistémico e integral, que abarca factores internos y externos de la organización. En la literatura hay publicaciones de trabajos dirigidos a funcionalidades específicas de la administración de la seguridad informática, que han sido buenos aportes a esta área, como soluciones parche, que no eliminan el problema de fondo, solo una gestión integral puede dar una protección eficiente a las organizaciones (Soomro, Shah, and Ahmed 2016).

2.1. Antecedentes

En este apartado detallamos los trabajos más relevantes que utilizamos de base científica en nuestra investigación:

Szczepaniuk et al. (2020) caracterizaron y evaluaron la gestión de la ciberseguridad dentro de las organizaciones pública y determinaron acciones para un incrementar la protección de la información y activos críticos; describieron problemas relacionados al “Sistema de Gestión de Seguridad de la Información” (SGSI), como falencias de organización, documentación no satisfactoria, análisis de riesgos, escaso seguimiento y evaluación, control de acceso, falta de capacitación.

Nasir et al. (2020) propusieron un modelo de “cultura de seguridad de la información” para organizaciones públicas de Malasia. Entre los hallazgos de esta investigación tenemos que no existe una estandarización de factores aplicado al área de seguridad de la información, no hay factores generalizados que sean útiles a cualquier clase de institución.

Sonmez & Kilic (2020) proporcionaron un modelo de amenaza en base a análisis de riesgos de una organización, que considera las restricciones de recursos monetarios.

Hoffmann et al. (2020) presentan dos modelos matemáticos con enfoque en el potencial real de amenazas, que puede servir como herramienta en la evaluación de la seguridad informática de una empresa.

Diesch et al. (2020) desarrollaron un modelo holístico para la gestión de la seguridad de la información de una organización. Clasificaron los factores más importantes en seguridad física, vulnerabilidad, infraestructura, conciencia de seguridad, control de acceso, riesgo, recursos, organización, CIA, continuidad del negocio, gestión de seguridad, cumplimiento y políticas.

Gupta et al. (2020) exploraron métodos de aprendizaje automático con capacidades para evitar ataques cibernéticos.

Al-Matari et al. (2020) propusieron un modelo de madurez de seguridad que considera las tecnologías y la capacidad de proceso de las empresas. Investigaron las brechas de seguridad informáticas que se presentan en el personal, tecnología, estructura organizacional, financieras, administrativas y operativas.

Arbanas & Hrustek (2019) resumen los factores más importantes para la protección de los sistemas de información, como el apoyo a la gestión, la política de seguridad de la información y la capacitación y sensibilización en temas de seguridad.

Zeng & Koutny (2019) realizaron un estudio bajar los costos de tecnologías, mediante una herramienta de apoyo a las decisiones que considera los gastos en ciberseguridad.

Toapanta et al.(2018) desarrollaron un modelo teórico para la gestión del control de acceso del “Registro Civil del Ecuador”, considerando una infraestructura distribuida, y los principales riesgos y vulnerabilidades que pueden incidir en esa empresa pública.

Kirenberg et al. (2020) presentaron un modelo matemático de optimización para evaluar la eficiencia de la planificación empresarial, considerando la relación entre los conceptos de información y seguridad económica.

Stepanov et al. (2019) desarrollaron un modelo matemático basado en un enfoque algoritmo genético, para evaluar el nivel de seguridad de los sistemas de información en una organización.

Awad et al. (2022) utilizaron los algoritmos genéticos NSGA-II y NSGA-III para la gestión eficiente de cartera de proyectos que incluye varios objetivos.

Hesarsorkh et al. (2021) desarrollaron un modelo probabilístico para optimizar la priorización de portafolio de proyectos, mediante un enfoque de programación posibilista, considerando el riesgo técnico de los proyectos y el riesgo de mercado.

Balderas et al. (2019) resuelven el problema multiobjetivo de selección de portafolio de proyectos mediante un algoritmo evolutivo basado en intervalos, considerando los recursos disponibles de la organización.

2.2. Bases teórico-científicas

2.2.1. Factores y variables para gestionar la seguridad de la información en las organizaciones

En la literatura encontramos factores importantes para gestionar la ciberseguridad tenemos:

Szczepaniuk et al. (2020) proponen factores legales, procedimental y organizativo, medidas de protección física y técnica, humano, recursos de la organización; implementación de protección de datos personales y ciberseguridad la comunidad internacional. Nasir et al. (2020) mencionan una cultura de la Seguridad de la Información; política y procedimientos es imprescindible para toda organización,

otros factores a considerar son el comportamiento y la conciencia de seguridad. Sönmez (2019) propone métricas para mejorar la eficiencia de tareas de seguridad; mejora continua en la estructura, el programa y los procesos de seguridad. Hoffmann et al. (2020) presentan una perspectiva de riesgos para evaluar el nivel de protección de la información en cualquier organización. Diesch et al. (2020) reconocen factores “organizativos”, “Recursos”, “CIA” y “Cumplimiento y política”, alineamiento de la alta dirección de la organización. Gupta et al. (2020) desarrollan métodos para tomar decisiones, la identificación y mitigación de ataques. Al-Matari et al. (2021) mencionan brechas de ciberseguridad del personal, tecnología, estructura organizacional, finanzas, gestión y operaciones; el grado de seguridad de la empresa, contramedidas automatizadas. AlYousef & Abdelmajeed (2019) definen un sistema de detección de intrusos. Arbanas & Žajdela Hrustek (2019) consideran factores de éxito como el apoyo de la alta dirección, la política de seguridad y capacitación y concienciación sobre temas seguridad. Zeng & Koutny (2019) mencionan estrategia rentable, mitigación de impacto, la utilización de tecnologías de ciberseguridad. S. M. Toapanta et al. (2019) hablan de ciberseguridad, estándares Internacionales y leyes específicas. M. Toapanta et al. (2018) aplican la autenticación, autorización, auditoría, confidencialidad, integridad, disponibilidad, mitigación, vulnerabilidad de la información.

Factores externos

La seguridad de la información no es una tarea aislada que puede combatir cada organización pública, existe incidencia del contexto donde opera la institución(Almeida and Herrera 2019; Masilela and Nel 2021). Según Szczepaniuk et al. (2020) es importante las acciones de cada país y su marco de cooperación internacional que garanticen la Ciberseguridad y la aplicación de castigos a Cyber-delincuentes. También podemos mencionar los niveles de corrupción de cada país, la inestabilidad de cargos públicos que no permiten una continuidad de las actividades planificadas, entre otros.

Ecuador, de los 24 factores dentro de las cinco dimensiones del “Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones” (MMCC), tenemos 10 en el nivel inicial (41.67%), 13 en el nivel formativo (54.17%), y solo 1 en el nivel consolidado (4.17%)(BID - OEA 2020). Refleja que a nivel de país estamos todavía en nivel inicial, en proceso de pasar a un nivel formativo.

Con el objetivo de lograr un Estado digital seguro en el ciberespacio, para asegurar el estado de derecho, que defiende la infraestructura y los servicios gubernamentales críticos y protege a los ciudadanos en el ciberespacio, se creó en el año 2021 la “Política Nacional de Ciberseguridad”.(MINTEL 2021)

Factores internos

De los muchos elementos que se mencionan en la literatura como factores y variables que son importantes para lograr la seguridad de la información los podemos listar como: apoyo de la gestión, política, procedimientos, cumplimiento, conciencia de seguridad, presupuesto, tecnología, principios, nivel de cultura, controles de seguridad, nivel de comportamiento organizacional, seguridad física, vulnerabilidades, amenazas, infraestructura, riesgos, factores organizativos, recursos, objetivos de seguridad “Confidencialidad, integridad y disponibilidad” (CIA) y Continuidad, nivel de seguridad, detección dinámica de amenazas a la seguridad, grado de madurez de seguridad, técnicas y tecnologías de seguridad, gestión de seguridad, medición de la seguridad informática, sistemas de seguridad, medición de la eficiencia de las tareas de seguridad, cultura de seguridad informática, revisiones, auditorías.

2.2.2. Optimización de portafolio de proyectos

En las organizaciones se generan diversos proyectos para lograr los objetivos estratégicos trazados por la alta dirección, en base a los requerimientos de toda la institución o de un área específica. El problema de portafolio de proyectos es una tarea compleja y desafiante que enfrentan muchas organizaciones, al tener que seleccionar un número limitado de proyectos de acuerdo con sus recursos, especialmente sus restricciones presupuestarias (Harrison, Garanovich, et al. 2022; Jafarzadeh et al. 2022). De la revisión de investigaciones recientes, encontramos algunos métodos y soluciones para priorizar proyectos aplicados en diferentes áreas, cada una con sus propias fortalezas y limitaciones. Se identifican los principales avances, perspectivas y tendencias de la comunidad científica sobre la gestión eficiente de carteras de proyectos (Liesiö et al. 2021; Ostakhov, Artykulna, and Morozov 2018; Saiz et al. 2022). Propone la gestión de la cartera de proyectos considerando la estrategia de resiliencia organizacional (Mahmoudi, Abbasi, and Deng 2022). Utilizan modelos de decisión para optimizar la selección de cartera de proyectos (de Almeida and Vetschera 2021; Calbert et al. 2022; Fernández et al. 2021; Kolisch and Fliedner 2022; Martins et al. 2021; Mussoi and Teive 2021). Presenta un modelo heurístico para gestionar de manera óptima la cartera de proyectos (Harrison, Elsayed, et al. 2022). Proponen computación evolutiva para la selección y programación de carteras de proyectos (Balderas et al. 2019; Fernández et al. 2022; Harrison, Garanovich, et al. 2022; Sarker, Harrison, and Elsayed 2022). Propone un modelo para la gestión eficiente de proyectos considerando algunas variables financieras de la gestión de proyectos (Zolfaghari and Mousavi 2021). Introduce un modelo matemático multicriterio para gestionar la cartera de proyectos a través de la programación de compromisos y la lógica difusa (Rivera et al. 2021). Para obtener los objetivos planificados por la organización, recomienda un modelo de gestión de proyectos eficiente con un enfoque de teoría matemática de grafos (Bai et al. 2021). Resuelve de manera eficiente el problema de gestión de recursos humanos para la planificación de proyectos a través de una técnica de asignación dinámica (Khatun et al. 2021). Presenta un modelo de gestión de proyectos eficiente aplicando lógica difusa, considerando variables aleatorias identificadas por los gerentes de la organización (Wu et al. 2021). Propone modelos y algoritmos utilizando el aprendizaje automático en la gestión de carteras de

proyectos (Marchinares and Rodriguez 2021). Propone un modelo de optimización de gestión de proyectos con un enfoque de capacidad de defensa, que forma grupos de proyectos para mejorar la distribución de recursos (Harrison et al. 2021). Recomienda un modelo de gestión de proyectos eficiente utilizando algoritmos genéticos y programación no lineal, considera métricas de distancia y capacidad (Mokhtari and S. M. Imamzadeh 2021). Propone un modelo de optimización para la gestión de carteras de proyectos, considerando varias funciones objetivo, utilizando rondas de toma de decisiones y realizando análisis de riesgo con simulación Monte Carlo de forma iterativa (Mavrotas and Makryvelios 2021). Presenta un modelo aplicando un enfoque de lógica simbólica con métricas de incertidumbre, para la gestión eficiente de la cartera de proyectos, considerando el valor presente como criterio económico, y el riesgo como criterio técnico.(Hesarsorkh et al. 2021)

Con base en los hallazgos científicos encontrados, identificamos que existen pocas publicaciones referentes al problema de la gestión eficiente de proyectos para el área de protección de la información en las instituciones del Estado; hay investigaciones sobre temas específicos, pero no hay una propuesta de solución integral al problema de estas organizaciones. Podemos determinar que la mayoría de los autores plantean el problema de gestión de cartera de proyectos, a través de un esquema de optimización multiobjetivo; donde simultáneamente, muchos objetivos tienen que ser optimizados, considerando sus criterios y restricciones, dando como resultado un conjunto de soluciones factibles. Su aplicación es muy amplia a nivel de ciencia e ingeniería (Juang and Bui 2020; Li et al. 2020, 2022; Olowu et al. 2020; Rodríguez-Molina et al. 2021). Para el presente trabajo utilizamos un enfoque heurístico clásico llamado “algoritmo genético de clasificación no dominada” NSGA-II, bien conocido, ampliamente probado y utilizado en aplicaciones de búsqueda y optimización, considerando varias funciones objetivo.(Awad et al. 2022; Deb et al. 2002)

2.2.3. Criterios para clasificar y priorizar proyectos de ciberseguridad

Encontramos varios criterios para ordenar y priorizar los proyectos de ciberseguridad, que va depender de cada organización. Estos criterios son importantes para alcanzar los objetivos estratégicos. A continuación, los criterios más utilizados para ordenar y priorizar los proyectos de ciberseguridad que encontramos en la literatura y en la práctica de organizaciones públicas en Ecuador:

Según INCIBE (2016) por tipo de proyecto los podemos clasificar en:

- Organizativo: cuando modifica estructura y/o procesos de la organización.
- Técnico: cuando tienen un importante contenido técnico.
- Regulatorio: cuando alinea algún aspecto concreto de nuestra organización a alguna norma o regulación.

Según INCIBE (2016) y la práctica empresarial, podemos clasificar a los proyectos por coste, que generalmente se establece rangos de coste de referencia como bajo, medio y alto, que van a ser subjetivos dependiendo del tamaño de la organización. Otra forma de clasificar es según el origen del incumplimiento, si vienen de incidente de seguridad, un análisis de riesgos, una auditoría o una evaluación de seguridad. Otro criterio muy utilizado para priorizar proyectos es el tiempo de ejecución. Otro criterio que no puede faltar son los recursos necesarios para la ejecución, tanto recursos propios y externos. Por último, tenemos la ratio ganancia / esfuerzo, también muy utilizado para priorizar proyectos, donde se da mayor importancia a los proyectos que generan más ganancia y que necesitan de menos esfuerzo en su aplicación.

2.2.4. Problemas de optimización multiobjetivo

La mayoría de los estudios se han centrado en desarrollar y aplicar variantes utilizando algoritmos evolutivos, debido a la manera eficiente y práctica en que estos métodos manejan los problemas de optimización. Los enfoques de inteligencia artificial se han aplicado con éxito en algunas áreas, como la ciberseguridad y la seguridad de la información. Los desarrollos en estos temas son evidentes, utilizando la computación evolutiva para desarrollar combinaciones de algoritmos y técnicas para aplicar a una variedad de problemas de clasificación y

optimización (Abdalla and Karabatak 2020). Se requiere crear enfoques, metodologías y técnicas de inteligencia computacional, que evolucionen junto con las necesidades de seguridad de la información de las organizaciones, las cuales se encuentran en un entorno complejo y cambiante, con altas posibilidades de ser atacadas por sus riesgos, vulnerabilidades y amenazas (Wang and Ji 2020). Sugiere un marco que utiliza el algoritmo de clasificación genética no dominada NSGA-II y la lógica difusa, que busca la eficiencia para problemas con muchos objetivos (Yang et al. 2021). Desarrolló un modelo con leyes de distribución de probabilidad de mutaciones cromosómicas y lo comparo con los algoritmos genéticos de colonia de hormigas y el algoritmo de Holland (Katsupeev, Shcherbakova, and Vorobyev 2016). Propuso un método utilizando factores ponderados que resuelve el problema de la diversidad de soluciones óptimas de Pareto (Ahrari et al. 2021). Aplican un modelo de computación evolutiva, con criterios de riesgos para seguridad de la información (Li et al. 2018). Recomienda un modelo de optimización utilizando computación evolutiva para la distribución eficiente de recursos de ciberseguridad, aplicando lógica difusa (Lakhno et al. 2020). Estableció un modelo de optimización matemática, que estima los riesgos de ataques y vulnerabilidades de una organización, utilizando algoritmos de computación evolutiva y aprendizaje automático (Song et al. 2016). Con la herramienta MATLAB se evalúa el desempeño de una versión del NSGA-II (Acar and Aliqui 2020). Desarrollar un modelo meta heurístico para la cartera de proyectos de construcción, considerando tiempo, costo y calidad (Kebriyaii et al. 2021). Hay una variedad de investigaciones que combinan varias técnicas usando el algoritmo NSGA-II, para obtener mayor eficiencia y mejores soluciones (Abouhawwash and Deb 2021; Algarni, Alazwari, and Safaei 2021; Awad et al. 2022; Chen, Du, and Xiao 2021; Deb et al. 2002; Liu, Zhu, and Li 2021). Otras investigaciones comparan la eficiencia de sus algoritmos genéticos con el algoritmo clásico NSGA-II experimentando con un problema de optimización multiobjetivo (Akhmetov et al. 2019; Atta, Mahapatra, and Mukhopadhyay 2021; Hashemi et al. 2017).

Tabla II: Clasificación de métodos para problemas de optimización multiobjetivo.

Determinísticos	Probabilísticos

Algoritmos exactos
• Ramificación y poda
• Divide y vencerás
• Programación dinámica
• Geometría algebraica
	Heurísticas
	• Meta heurísticas
	  ○ Algoritmos genéticos
	  ▪ No Pareto
	  ▪ Pareto
	  ▪ A base de transformación
	  ○ Búsqueda tabú
	  ○ Reconocido simulado
	• Heurísticas especificas

Fuente: Adaptado de Crespo Sánchez, Pérez Abril, and García Sánchez (2022).

La Tabla II muestra una clasificación de métodos para resolver problemas de optimización multiobjetivo, donde podemos apreciar que la tendencia es hacia métodos probabilísticos, heurísticos, metaheurísticos. Los que se aplicarán en el presente trabajo son los Algoritmos genéticos basados en Pareto.

2.2.5. Criterios utilizados para la seguridad de la información

Podemos clasificar los principales criterios para problemas de optimización de ciberseguridad en criterios de eficiencia económicos y técnicos (Akhmetov et al., 2019; Bojanc & Jerman-Blažič, 2012; Hashemi et al., 2017; Klyaus & Gatchin, 2020; Lakhno et al., 2020; Ramalingam et al., 2018; Zeng & Koutny, 2019). Otros autores utilizan criterios de Costo-Beneficio (Arora et al. 2004; Kirenberg et al. 2020; Schatz and Bashroush 2017; Zegzhda et al. 2020). Ejemplos de beneficios como reducción de costos, ingresos, eficiencia económica; Ejemplos de costos como costo de producción, costo de oportunidad, costos operativos, costos totales. Los criterios ampliamente utilizados en este campo de la seguridad de la información son: amenaza, como la eficiencia de los atacantes, la posibilidad de riesgo; criterios de impacto, como daño potencial, probabilidad de amenazas; criterios de

vulnerabilidad, como factor de exposición, factor de riesgo (Kirenberg et al. 2020; Li et al. 2018; Schatz and Bashroush 2017; Stepanov et al. 2019). Otra categoría utilizada es la de recursos, por ejemplo presupuestos de una organización, bienes o capacidad de los hackers; utilizar algunos modelos de predicción y matemáticas difusas.(Schatz and Bashroush 2017)

2.2.6. Métricas para problemas de optimización multiobjetivo

En la literatura existen algunos indicadores y métricas utilizadas por los investigadores para verificar la calidad y desempeño de los resultados obtenidos en los diversos algoritmos; según sus características podemos clasificarlos en indicadores de distribución, dispersión, convergencia y cardinalidad (Audet et al. 2021; Okabe, Jin, and Sendhoff 2003; Riquelme, Von Lücken, and Baran 2015). En el presente trabajo solo mencionaremos algunos indicadores que encontramos en la literatura: El indicador de hipervolumen y la diferencia de hiperárea son buenas medidas de las propiedades de dominancia y distribución de las soluciones, además, no requiere saber el óptimo de Pareto de antemano (Amine 2019; Ishibuchi et al. 2018; Nartey et al. 2022). El tiempo de cómputo o tiempo de CPU en segundos que mide la ejecución de una tarea, es muy utilizado en la comparación de programas, aplicaciones, algoritmos, entre otros (Abouhawwash and Deb 2021; Biswas and Acharyya 2021). El número de puntos en el frente aproximado o el número de soluciones no dominadas se consideran medidas de calidad de los algoritmos (Okabe et al. 2003; Tavakoli-Someh and Rezvani 2019). La medida de proximidad Karush-Kuhn-Tucker (KKTPM) (Abdalla and Karabatak 2020; Algarni et al. 2021). El SPREAD cuantifica la disparidad o falta de uniformidad de las soluciones obtenidas en el frente de Pareto (Algarni et al. 2021). En cuanto a las métricas de convergencia, la distancia generacional y la Distancia Generacional Inversa son ampliamente utilizadas (Abouhawwash and Deb 2021; Riquelme et al. 2015).

2.3. Computación evolutiva

La ubicamos dentro de la “Inteligencia Artificial” (IA), se denomina “Computación Evolutiva” porque sus modelos computacionales se basan en los enunciados de “selección natural” expuestos por el inglés Charles Darwin (Suárez and Galán 2021). Se clasifican en las siguientes técnicas: La Programación Evolutiva, las Estrategias Evolutivas, los Algoritmos Genéticos (AG), y en la Programación Genética. Ésta investigación se centrará en los Algoritmos Genéticos.

2.3.1. Algoritmos genéticos

Holland (1992) fue el creador de los Algoritmos Genéticos y los definió como procedimientos del tipo adaptativo empleados para resolución de problemas complejos. En estos algoritmos existe un proceso de selección, que se fundamenta en la supervivencia del más fuerte.

Entre las ventajas de utilizar los Algoritmos Genéticos esta la diversidad, que permite una exploración total que evita óptimos locales, facilita el cruce para obtener una mejor evolución, soporta la toma de decisiones y obtenemos soluciones robustas (Doerr and Neumann 2019).

Estos algoritmos son fáciles de implementar, porque la estructura es siempre la misma, independientemente del problema. La única configuración que se debe cambiar para cada problema es la creación de la función fitness, que tiene sus objetivos particulares.

Los algoritmos genéticos utilizan la siguiente terminología:

Individuo: también llamado cromosoma, son las posibles soluciones al problema que estamos tratando.

Gen: Forman los cromosomas, son parte de la cadena.

Población: conjunto de soluciones.

Función fitness: función que evalúa a los individuos y les asigna una puntuación en función de los criterios del problema.

Operador genético: es una función empleada para garantizar la diversidad genética de los individuos de una población. Los más empleados son:

- **Selección:** esta función escoge los individuos que van a reproducirse en la siguiente generación. Por ejemplo, en la selección por ruleta, a cada cromosoma se incorpora una parte proporcional a su ajuste de una ruleta. Si es selección por torneo, se hacen comparaciones directas entre individuos.
- **Cruce:** esta función recombina los individuos para generar los hijos que se incorporar en la proxima generación.
- **Mutación:** esta función provoca que alguno de los genes de un individuo varíe su valor de forma aleatoria.

Generaciones: es el número de veces que se realiza el proceso de evolución de la población.

El proceso de un AG se desarrolla haciendo estos pasos: se crea de manera aleatoria una población inicial de individuos. Luego se evalúa cada solución de la población con la función fitness. Después se aplican los operadores genéticos de selección, cruce y mutación. Este proceso se repite hasta que se cumpla con la condición de terminación definida, que puede ser por ejemplo un número de generaciones determinadas. El resultado es una nueva generación, generalmente mejor que la inicial.

2.3.2. NSGA-II

Deb et al. (2002) fue el creador del algoritmo genético de clasificación no dominada elitista NSGA-II, de tipo elitista, para superar los inconvenientes de otros algoritmos evolutivos, desarrolló un enfoque de ordenamiento rápido no dominado con una complejidad computacional menor a los otros algoritmos de esa época. El NSGA-II demostró su capacidad para resolver la mayoría de los problemas de optimización, con una distribución de soluciones mucho mejor en comparación con la estrategia de evolución archivada de Pareto y la estrategia evolutiva de Pareto de fuerza. El NSGA-II ha sido ampliamente utilizado en aplicaciones de todas las areas, sobre todo en las ciencias y la ingeniería.

El NSGA-II es de tipo elitista, debido a su mecanismo de conservación de las soluciones dominantes a través de varias generaciones, es decir, un proceso evolutivo. Al inicio, el algoritmo de clasificación no dominada NSGA-II crea aleatoriamente la población inicial, luego evaluamos usando la función objetivo definida en base a los criterios definidos en el modelo, evaluamos los individuos y luego procedemos a ordenar la población no dominada. Posteriormente, aplicamos los procesos de selección por torneo, cruzamiento y mutación, lo que da como resultado una mejor población. Este proceso es iterativo y solo finalizará cuando se cumpla el número de generaciones que definimos en los parámetros de ejecución del algoritmo.

2.3.3. Dominancia y óptimo de Pareto

El óptimo de Pareto o eficiencia de Pareto es la mejor de solución que buscan los problemas de optimización multiobjetivo, tratando de cumplir simultáneamente todos sus objetivos, es utilizado por los algoritmos evolutivos.

De acuerdo a Novoa-Hernández (2015), una solución X de Pareto domina a otra Y, cuando X es por lo menos tan buena como Y en todos los objetivos, y superior a Y en al menos uno de estos objetivos. Una solución X es Pareto óptima si no existe otra solución Y que la domine. Al conjunto de soluciones Pareto óptimas se le conoce como “Conjunto de Pareto”, mientras que la imagen de este conjunto de soluciones se la denomina “Frente de Pareto”. El algoritmo NSGA-II, basado en los conceptos de dominancia y óptimo de Pareto, se lo reconoce por su amplia aplicación en la mayoría de las areas, algunos ejemplos han sido referenciados en la presente revisión literaria en las secciones de “Optimización de portafolio de proyectos” y “Problemas de optimización multiobjetivo”.

La Figura 1 muestra un ejemplo de frente de Pareto con 2 objetivos entre los que se debe asignar una serie de recursos. La solución P1 significa que se reparten más al objetivo1 que al 2, pero se están repartiendo todos los recursos. En la solución P2 también se reparten todos, pero se asigna más al objetivo 2 que al 1. Esta situación es la que pasa cuando se tienen varios objetivos requiriendo los mismos recursos, mientras un objetivo mejora la asignación, el otro empeora, pero tanto P1, como P2 son óptimos de Pareto y soluciones no dominadas, siempre van

a estar en el frente de Pareto. En cambio las soluciones P3, P4 y P5 son soluciones dominadas.

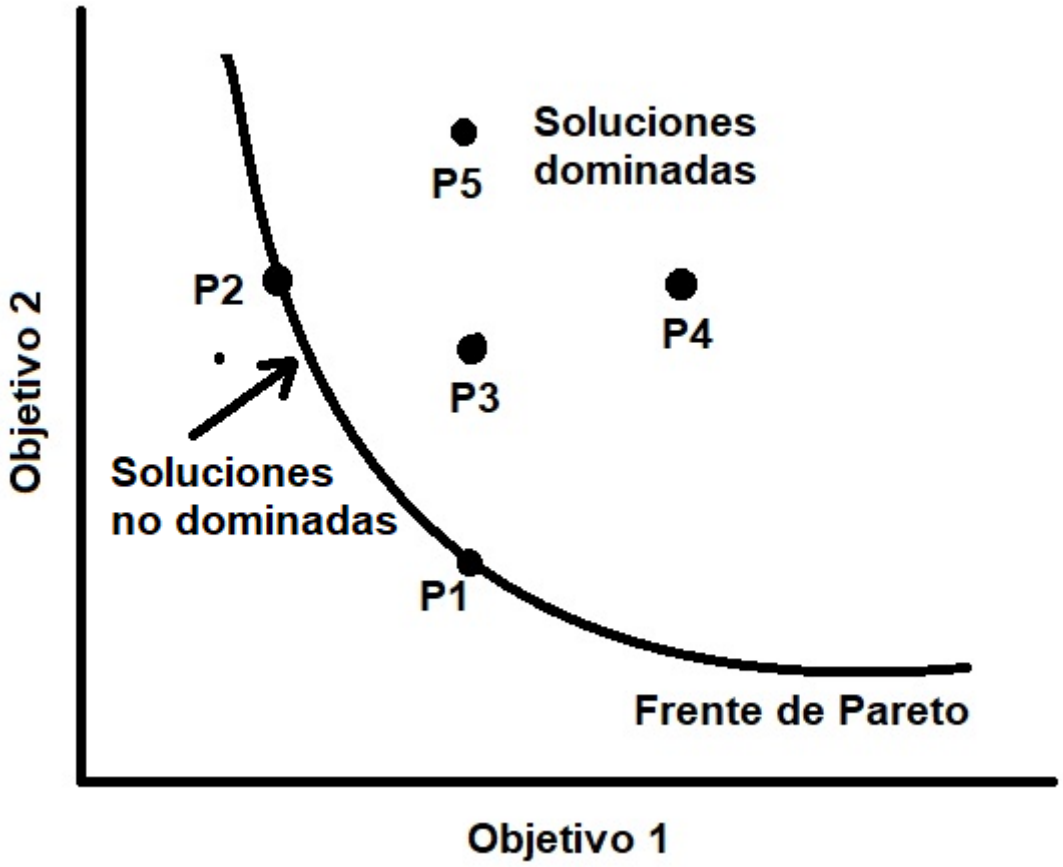


Figura 1: Dominancia y óptimo de Pareto

2.4. Definición de términos básicos

Ciberseguridad

“La ciberseguridad es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales”(IBM 2022). Conocida como seguridad informática, son acciones desarrolladas para enfrentar las amenazas contra sistemas y aplicaciones que trabajan en red.

Seguridad de la información

Son medidas de protección de datos reservados para evitar el acceso no autorizado, y sus respectivas consecuencias.(IBM 2022)

EGSI

Es el Esquema Gubernamental de Seguridad de la Información, implementado por el gobierno de Ecuador, que busca preservar la confidencialidad, integridad y disponibilidad de la información en las organizaciones públicas a cargo de la función ejecutiva.(MINTEL 2020b)

Variables de decisión

Son las n variables que son definidas por las soluciones del modelo, dentro del espacio del problema X. Se simbolizan como: X1, X2, X3, hasta Xn.(López 2013)

Función objetivo

Es la correspondencia entre las variables de decisión, que define el problema a optimizar, ya sea un máximo o mínimo, considerando ciertas restricciones. El resultado es la medida de la utilidad del modelo, y conforman el conjunto de las soluciones encontradas. (López 2013)

Restricciones

Son la correspondencia de las variables de decisión con los recursos limitados del modelo. También se definen restricciones de no negatividad de las variables de decisión (Vorobioff et al. 2022).

Convergencia

Es asegurar que, al realizar un número de iteraciones, las aproximaciones obtenidas deben acercarse al valor buscado. Es la virtud del algoritmo para obtener un óptimo local o global. (Vorobioff et al. 2022)

Auditoría de seguridad

Tiene como propósito comparar los resultados con un estándar o conjunto de estándares específicos, y encontrar fallas de seguridad porque no se cumple la norma.

Evaluación de seguridad

El objetivo es que los evaluadores utilicen su experiencia y conocimientos prácticos, junto con otros estándares y directrices reconocidos para la ciberseguridad. La evaluación de seguridad proporciona al cliente una lista de acciones a tomar para mitigar los problemas.

Evaluación de riesgo de ciberseguridad

proporciona un proceso replicable y medible que informa a la administración sobre los riesgos que tiene la organización y su grado de preparación en ciberseguridad.

Incidente de seguridad de la información

Sucede con la unión de sucesos de ciberseguridad que pueden de exponer la información y/o activos críticos, que impacten la operación normal de la empresa o su imagen.

CAPITULO III: MATERIALES Y METODOS.

3.1. Tipo de estudio y diseño de investigación.

Definimos el trabajo realizado con una metodología de investigación de enfoque cuantitativa, de tipo aplicada, con diseño de investigación observacional correlacional transversal.

Es una investigación cuantitativa, realizamos un análisis de la realidad objetiva del problema planteado, mediante mediciones y cuantificación numérica de las variables del modelo de optimización de la gestión de proyectos estratégicos para mejorar la seguridad de la información de una organización pública de Ecuador, apoyado en las ciencias matemáticas y la estadística.

Es una investigación aplicada, porque se propone un modelo para contribuir a solucionar una necesidad reconocida de los problemas de seguridad de la información de una base de datos, en el contexto de las organizaciones públicas de Ecuador. Para evaluar la validez del modelo de optimización propuesto, realizamos simulaciones para establecer la viabilidad de las soluciones.

Es una investigación observacional correlacional transversal, porque se determinó que el modelo de optimización para la selección de proyectos estratégicos de ciberseguridad permite mejorar la seguridad de la información y el uso eficiente de recursos de una organización pública de Ecuador. Esto se realizó en un solo momento determinado y sin influir es las variables de estudio.

3.2. Población, muestra y muestreo.

Este trabajo tiene como finalidad estudiar las Organizaciones Pública de Ecuador en aspectos relacionados con la selección de los proyectos estratégicos en ciberseguridad planificados para mejorar la seguridad de la información y uso eficiente de los recursos disponibles. Establecimos como unidad de análisis a las Organización públicas de Ecuador, con sede en la ciudad de Guayaquil. Definimos

como población a los proyectos estratégicos de ciberseguridad planificados por las organizaciones públicas de Ecuador para mejorar la seguridad de la información.

Para la recolección de datos de los proyectos estratégicos de ciberseguridad, se realizó un muestreo por conveniencia, considerando la facilidad de acceso y la disponibilidad de los datos, ya que se trata de información sensible que no puede ser divulgada. Como aplicamos un método no determinista de las técnicas meta heurísticas, se realizaron varias simulaciones para garantizar la fiabilidad de los resultados, por tal motivo se crearon varios escenarios de prueba y escogemos uno para validar el modelo.

El criterio de inclusión para la selección de la Organización Pública de Ecuador fue: que esté en el “Ranking de evaluación del cumplimiento a la calidad de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI)” del año 2020 (MINTEL 2020a), y la facilidad de acceso a la información de proyectos estratégicos de ciberseguridad del área de TI. Se nos facilitó información de 30 proyectos estratégicos de ciberseguridad planificados el año 2021 para mejorar la seguridad de una organización pública de Ecuador, los datos se muestran en la Tabla III.

Tabla III: Lista de proyectos estratégicos de ciberseguridad planificados.

No.	Tipo de proyecto	Origen incumplimiento	Clasificación proyecto PDS	Clasificación Tiempo ejecución	Tiempo ejecución (días)	Tipo de costo	Costo (USD)	Recursos
1	Técnico	AU	PST	Corto	60.00	M	1,912.00	Externos
2	Regulatorio	ER	PSA	Largo	220.00	A	1,204.00	Internos
3	Regulatorio	AU	PFO	Corto	45.00	A	3,253.00	Internos
4	Técnico	IS	PPE	Largo	260.00	M	3,006.00	Ambos
5	Técnico	ER	PSE	Corto	80.00	M	2,828.00	Ambos
6	Técnico	ER	PFO	Medio	120.00	M	2,143.00	Ambos
7	Técnico	ES	PSA	Largo	200.00	A	1,839.00	Externos
8	Organizativo	ES	PSA	Largo	340.00	B	5,467.00	Ambos
9	Organizativo	AU	PSE	Corto	60.00	B	1,712.00	Ambos
10	Técnico	AU	PPE	Largo	240.00	A	5,837.00	Internos
11	Técnico	ES	PSE	Largo	320.00	B	4,456.00	Externos
12	Técnico	IS	PSE	Medio	160.00	A	1,260.00	Externos
13	Técnico	ES	PPE	Largo	280.00	A	6,489.00	Internos
14	Técnico	ES	PFO	Corto	90.00	M	7,536.00	Externos
15	Organizativo	IS	PSE	Corto	45.00	B	9,583.00	Ambos
16	Técnico	IS	PPE	Medio	160.00	A	9,812.00	Ambos
17	Técnico	IS	PSE	Medio	140.00	A	14,280.00	Internos
18	Técnico	AU	PPE	Largo	200.00	B	6,435.00	Ambos
19	Técnico	ER	PSA	Largo	210.00	A	9,258.00	Externos
20	Técnico	ES	PPE	Corto	80.00	B	14,929.00	Internos
21	Técnico	ES	PSA	Medio	140.00	A	12,874.00	Externos
22	Técnico	ES	PST	Largo	220.00	M	9,612.00	Externos
23	Regulatorio	ES	PSE	Medio	100.00	A	13,360.00	Ambos
24	Técnico	ER	PFO	Largo	320.00	A	10,558.00	Internos
25	Técnico	AU	PPE	Largo	300.00	M	6,107.00	Internos
26	Organizativo	AU	PFO	Largo	340.00	B	8,616.00	Internos
27	Organizativo	AU	PFO	Medio	120.00	B	12,925.00	Ambos
28	Técnico	IS	PFO	Corto	70.00	M	37,299.00	Internos
29	Técnico	AU	PSE	Corto	80.00	M	33,211.00	Internos
30	Organizativo	AU	PST	Corto	90.00	B	25,190.00	Internos
							282,991.00	

Fuente: Elaboración propia, basado en datos de Organización pública de Ecuador, 2021.

Abreviatura de origen de incumplimiento: ER=Evaluación de riesgo, AU=Auditoría, ES=Evaluación de Seguridad, IS=Incidente de seguridad.

Abreviatura de clasificación de proyectos: PFO=Proyecto de Formación, PSE=Proyecto de Seguridad de Eventos, PSA=Proyecto de Seguridad de Accesos, PST= Proyecto de Seguridad de Activos, PPE=Proyecto del Plan de Evaluación

Abreviatura de tipo de costo: B=Bajo, M=Medio, A=Alto

3.3. Métodos, técnicas e instrumentos de recolección de datos.

Se diseñó un algoritmo genético para desarrollar el modelo de optimización propuesto en este trabajo de investigación. Utilizamos la técnica de observación para verificar el funcionamiento del algoritmo genético. El instrumento se implementó en lenguaje de programación Python.

Se utilizó el método deductivo, para verificar que el modelo de optimización propuesto contribuye a mejorar la seguridad de la información y el uso eficiente de recursos en una organización pública.

3.4. Plan de procesamiento y análisis de datos.

3.4.1. Análisis de la seguridad de la información de las organizaciones públicas del Ecuador

Para cumplir con este objetivo de investigación se analizó la información disponible sobre factores y variables más importantes relacionados con la Seguridad de la Información de las organizaciones públicas. Además, se revisó las vulnerabilidades, deficiencias, limitantes y restricciones de las organizaciones para enfrentar los actuales ataques y riesgos informáticos. Con este análisis se propuso mejoras en la Seguridad de la Información de las organizaciones.

Después, se analizó y se clasificó los factores, tanto externos e internos relacionados a la Seguridad de la Información de una organización; para poder crear un modelo conceptual que permita reflejar sus relaciones partiendo de una perspectiva estratégica. Los 5 factores del modelo se muestran la Tabla III.

Se diseñó un modelo conceptual que evalúa la capacidad de gestión de la seguridad de la información basado en la planificación estratégica, para asegurar el direccionamiento de la empresa de un estado actual a un estado deseado; donde toda la estructura de la organización, gestión y recursos apoyen la estrategia y objetivos, mediante un sistema de mejoramiento continuo. La Fig. 1 muestra el modelo conceptual para evaluar la capacidad de gestión de la seguridad de la información basado en la planificación estratégica.

Se aplicó este modelo de la capacidad de gestión de la seguridad de la información, a dos organizaciones públicas que se encuentran entre las 82 empresas del en el "Ranking de evaluación del cumplimiento a la calidad de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI)" del año 2020. Una que este valorada como "Buena" (ponderación 100% a 90%), y otra valorada como "Regular" (ponderación 89% a 60%)(MINTEL 2020a). Con esto cubrimos el 91.5% de las 82 organizaciones públicas.

3.4.2. Modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en instituciones públicas del Ecuador

Para lograr los objetivos de diseñar y desarrollar el modelo de optimización propuesto, se realizó lo siguiente:

Primero se revisó la información disponible en la literatura referente a marcos de trabajo, componentes y los factores críticos de éxito más importantes sobre arquitectura empresarial de TI para organizaciones, luego diseñamos un marco de trabajo general de arquitectura empresarial de TI para una organización pública. El marco de trabajo general para una organización pública se muestra en la Figura 4.

También se revisó información disponible sobre los modelos, metodologías, factores, variables y criterios más importantes relacionados con la selección de la cartera de proyectos de ciberseguridad. Además, se revisó las alternativas de solución a problemas de optimización multiobjetivo, las tendencias actuales, así como las principales métricas e indicadores de calidad de los resultados. una vez organizada la información, se analizó los datos para comprender y plantear el proceso de planificación de proyectos estratégicos para mejorar la seguridad de la información de una organización pública. El proceso de planificación de proyectos estratégicos se muestra en la Figura 4.

El problema crítico que se resolvió para la gestión de TI es la selección óptima de los proyectos que la organización debe implementar considerando el criterio económico que tiene un presupuesto asignado, que generalmente es menor al costo total de todos los proyectos planificados. También para la selección de proyectos se consideró los criterios técnicos que permitan la priorización de los proyectos planificados.

Para plantear el modelo de optimización se eligió un enfoque de computación evolutiva, como el algoritmo genético de clasificación no dominada NSGA-II, porque resuelve de manera eficiente los problemas de optimización con pocas funciones objetivo(Duan et al. 2022; Guerrero et al. 2018; Li, Tam, and Yeung 2021; Montes Dorantes et al. 2018; Pellegrini et al. 2020; Sawczuk da Silva et al. 2018; Tavakoli-Someh and Rezvani 2019; Tawfiq et al. 2021; Torquato et al. 2021). Las variables de decisión representarán todos los proyectos estratégicos de ciberseguridad planificados para mejorar la seguridad de la información de la organización; el modelo debe obtener un subconjunto de proyectos a ejecutar, que son las soluciones óptimas, que permiten alcanzar los objetivos del modelo, que se escogen de los principales factores encontrados en la revisión de la literatura y de la práctica, también se consideran las restricciones de la organización, que permiten encontrar el subconjunto de soluciones factibles del problema. La figura 6 muestra el diagrama de flujo del algoritmo NGA-II para el modelo propuesto.

3.4.3. Simulación

Para la simulación se crearon varios escenarios basados en datos de los proyectos, y se realizarán diferentes corridas. Se eligió un escenario para mostrar los resultados del modelo de optimización a proponer. Se definió los parámetros en base a pruebas y evidencias de trabajos similares para la ejecución del AG. El programa se desarrolló en lenguaje de programación Python que se muestra en el Anexo 3.

3.4.4. Análisis de correlación

Se analizó la correlación de las variables del modelo de optimización, tomando la información resultante de la simulación, mediante el coeficiente de correlación de Pearson calculado según Kumar & Jena (2020) y Yan et al. (2021). Las variables son número de proyectos de solución, presupuesto y % de CMSI. Para mostrar los resultados se utilizó diagramas de dispersión y matriz de correlación de Pearson.

3.4.5. Evaluación del modelo

Se comparó los resultados obtenidos en la simulación con resultados de otras investigaciones que se encuentren en la revisión de la literatura.

3.5. Hipótesis

Un Modelo de optimización para la selección de proyectos en ciberseguridad permite mejorar la seguridad de la información y el uso eficiente de recursos en instituciones públicas del Ecuador.

CAPITULO IV: RESULTADOS Y DISCUSIÓN

4.1. Resultados

4.1.1. Analizar la seguridad de la información de las empresas públicas de Ecuador

Identificación de factores para la seguridad de la información

En base a la revisión de la literatura desarrollamos una escala para medir la Capacidad de la Seguridad de la Información (CSI) de una organización en base a 5 factores del modelo propuesto. La escala se muestra en la Tabla V.

Tabla IV: Principales factores de la seguridad de la información.

Nro.	Factores	Descripción
1	Estratégicos	* La organización cuenta con un direccionamiento estratégico para la Seguridad de la Información, estrategia, objetivos definidos. * Hay una visión compartida de Seguridad de la Información en toda la organización. * Se percibe una cultura organizacional de la Seguridad de la Información. * Se definieron los proyectos y planes de acción para llegar todos los niveles: estratégico, táctico y operativo.
2	Recursos y competencias	* Existen los recursos y competencias para mantener la operación diaria y para la continuidad del negocio. * Existen los recursos y competencias para implementar los proyectos y planes de acción resultados de la planificación estratégica.
3	Organización / Gestión	* Existe una estructura organizacional que pueda gestionar eficientemente los activos y todos los elementos y procesos relacionados a la Seguridad de la Información de acuerdo a los objetivos estratégicos. * Todos los elementos, componentes y sistemas críticos de la Seguridad de la Información se están gestionando de manera eficiente. * Utiliza Normas, Estándares Internacionales, Mejores Prácticas de Tics y de Seguridad de la Información.
4	Mejoramiento continuo	* Todos los elementos y procesos gestionados relacionados con la Seguridad de la Información están sujetos a una revisión constante y mejoramiento continuo, tanto a nivel estratégico, táctico y operativo. * Se registra y se gestiona los incidentes de la Seguridad de la Información. Se maneja estadísticas. * Se reúnen periódicamente para tomar decisiones sobre la Seguridad de la Información, a nivel estratégico, táctico y operativo.
5	Contexto local, nacional e internacional	* Los gobiernos a nivel local, nacional e internacional generan seguridad de la información: Políticas y estrategias, cultura de seguridad en ciudadanos, marcos legales y regulatorios, control de riesgo, estándares internacionales y tecnología.

Tabla V: Escala de valoración de cumplimiento de factores

Escala	Valor	Criterio
Todo	5	Cumple todos
Alto	4	Cumple la mayoría
Bueno	3	Cumplimiento aceptable
Medio	2	Cumple parcialmente
Bajo	1	Cumple lo mínimo
Nada	0	No cumple con nada

Tabla VI: Escala de capacidad de gestión de la seguridad de la información

Escala	Valor	Criterio
Optimizada	(80 - 100]	Organización preparada
Estratégica	(60 - 80]	Organización semi-preparada
Administrada	(40 - 60]	Organización vulnerable
Formativa	(20 - 40]	Organización en peligro
Inicial	[0 - 20]	Organización indefensa

Modelo para medir la capacidad de gestión de la seguridad de la información

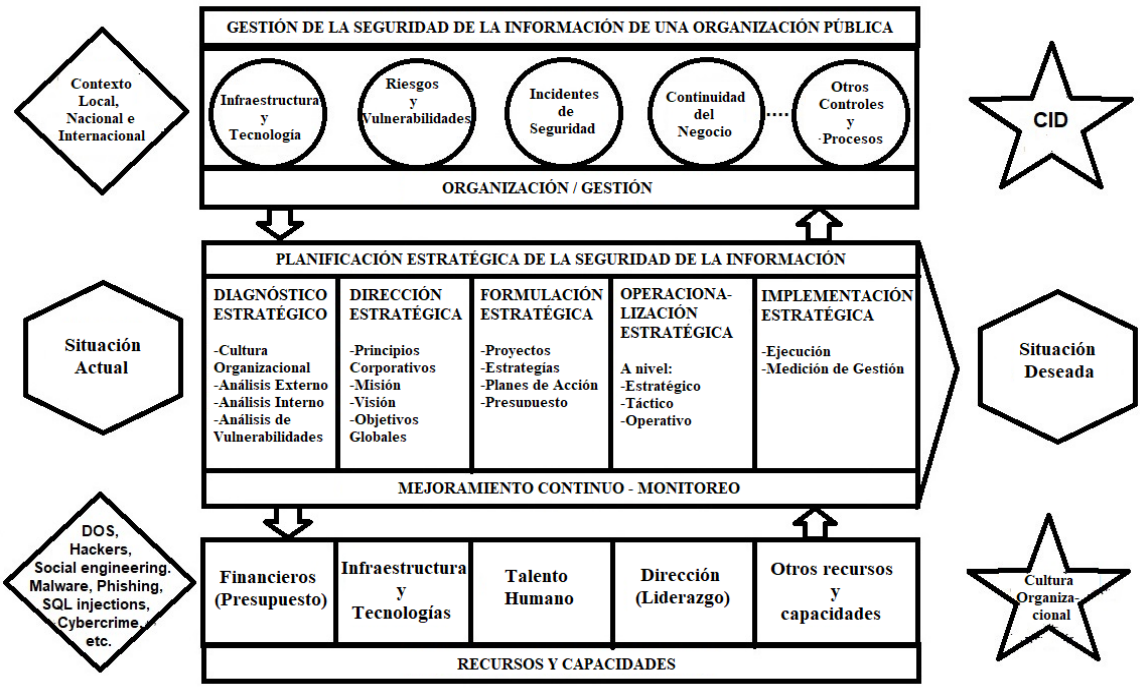


Figura 2: Modelo de Gestión de la Seguridad de la Información de una Organización Pública.

De la revisión de trabajos científicos realizada creamos el modelo conceptual de la Fig. 2, y luego establecimos el proceso de cálculo de Capacidad de Gestión de la Seguridad de la Información (CSI) de una Organización Pública de la Fig. 3, que considera las Tablas IV, V y VI.

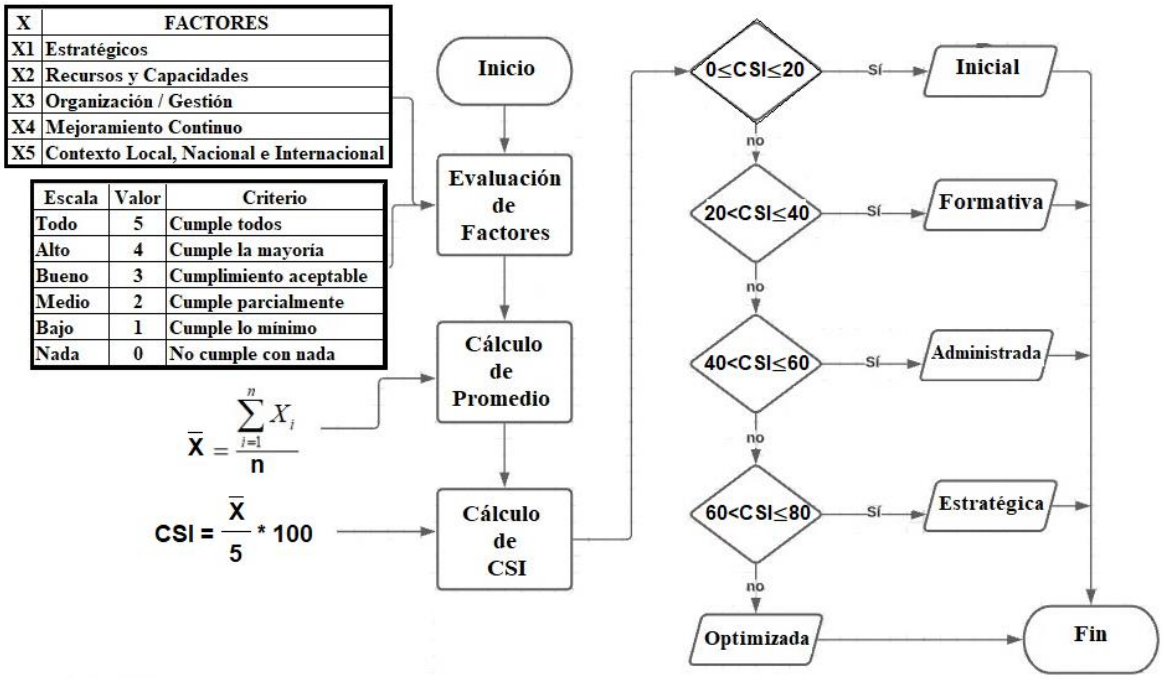


Figura 3: Proceso de cálculo de CSI de una Organización Pública.

El proceso inicia con la valoración de los 5 factores de la Tabla IV para una organización, luego se calcula la media de estas valoraciones, de esta forma:

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{5} \qquad (1)$$

Donde:

$\bar{X}$: es la media de las valoraciones de los factores.

X_i : son cada uno de las valoraciones de los factores.

Para establecer el % CSI de una organización, la media de las valoraciones dividido para 5 y multiplicando por 100; de esta manera:

$$CSI = \frac{\bar{X}}{5} * 100 \quad (2)$$

Donde:

CSI: es el % de Capacidad de Seguridad de la Información en una organización.

$\bar{X}$: es la media de las valoraciones de los factores.

Con el % CSI calculado se buscó en qué nivel de la escala de capacidad se encuentra la organización en la Tabla V. Este proceso para calcular la CSI de una Organización Pública, se resume en la Figura 4.

Aplicación de casos de estudio del cálculo de Capacidad de Gestión de la Seguridad de la Información

Se realizó la evaluación de la CSI de 2 organizaciones públicas:

1) **Caso de estudio organización con ranking EGSI "Buena"**

Se valoró los 5 factores de la Tabla IV en base a la escala de la Tabla V; luego calculamos la media de estas valoraciones con la formula (1), reemplazando los datos tenemos:

$$\bar{X}_{Buena} = \frac{3+3+3+2+1}{5} = 2.4 \quad (3)$$

Se calculó el porcentaje de Capacidad de Gestión Seguridad de la Información usando (2), reemplazando los datos se obtiene:

$$* CSI_{Buena} = \frac{2.4}{5} * 100 = 48\% \quad (4)$$

La Tabla VII, muestra el resumen de los cálculos realizados para la organización con ranking EGSI "Buena"; tiene 48%, de acuerdo al criterio de la Tabla VI la denominamos "Administrada", es una empresa vulnerable, que, a pesar de poseer buena cantidad de recursos, capacidades, una estructura que le permite gestionar sus activos y procesos relacionados con la Seguridad de la Información, no tiene una estrategia, objetivos, y una visión compartida por la organización para que sus esfuerzos sumen a esta planificación.

Tabla VII: Evaluación de CSI de organización con ranking EGSI "Buena"

Nro.	Factores	Valor	Escala
1	Estratégicos	3	Bueno
2	Recursos y competencias	3	Bueno
3	Organización / Gestión	3	Bueno
4	Mejoramiento continuo	2	Medio
5	Contexto local, nacional e internacional	1	Bajo
	PROMEDIO	2.4	Medio
	CAPACIDAD DE LA ORGANIZACIÓN	48%	Administrada

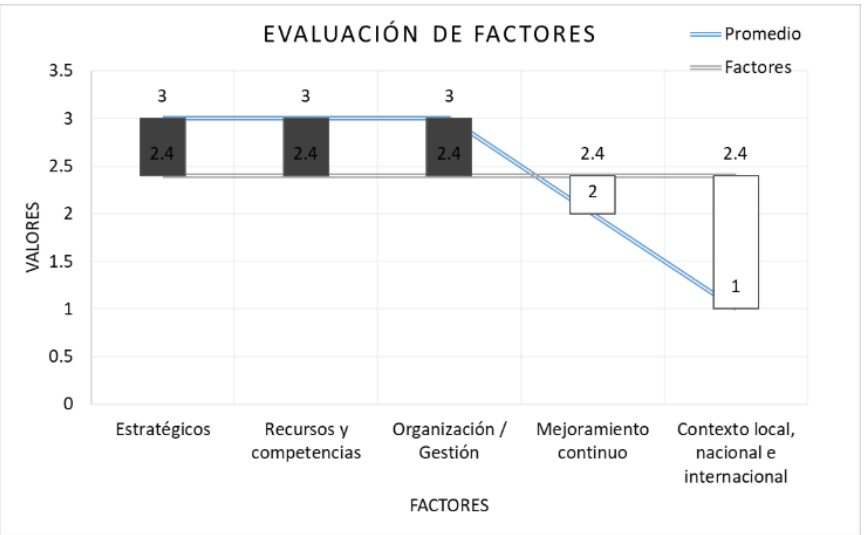


Figura 4: Evaluación de Factores organización con ranking EGSI "Buena"

En la Figura 4 podemos observar el resultado de la evaluación de los 5 factores de la Seguridad de la Información de una organización con ranking EGSI "Buena", donde los 3 primeros factores, estratégicos, recursos y competencias y organización/gestión tienen una valoración buena sobre el promedio. El punto más bajo lo tiene en el factor externo, el contexto local, nacional e internacional.

2) Caso de estudio organización con ranking EGSI "Regular"

Se valoró los 5 factores de la Tabla IV en base a la escala de la Tabla V; luego calculamos la media de estas valoraciones con la formula (1), reemplazando los datos tenemos:

$$\bar{X}_{Regular} = \frac{2+2+2+1+1}{5} = 1.6 \qquad (5)$$

Se calculó el porcentaje de Capacidad de Gestión Seguridad de la Información usando (2), reemplazando los datos tenemos:

$$CSI_{\text{Re gular}} = \frac{1.6}{5} * 100 = 32\% \qquad (6)$$

La Tabla VIII, muestra el resumen de la organización con ranking EGSI “Regular”; tiene 32%, que de acuerdo al criterio de la Tabla VI la denominamos “Formativa”, es una empresa en peligro, que, solo cumple parcialmente lo relacionado a factores Estratégicos, Recursos y competencias y Organización / Gestión; tiene un cumplimiento mínimo en los factores Mejoramiento continuo y Contexto local, nacional e internacional.

En la Figura 5 podemos observar el resultado de la evaluación de los 5 factores de la Seguridad de la Información de la organización con ranking EGSI “Regular”; los 3 primeros factores, estratégicos, recursos y competencias y organización/gestión tienen una valoración media, sobre el promedio; bajo la media, se encuentran los factores mejoramiento continuo, y el contexto local, nacional e internacional.

Aproximadamente el 22% de las organizaciones públicas de Ecuador se encuentran en el mejor de los casos con un nivel de Capacidad de Gestión de la Seguridad de la Información “Administrada”, que son organizaciones vulnerables; El 70% de organizaciones públicas van a tener un nivel de Capacidad de Gestión de la Seguridad de la Información “Formativa”, que son organizaciones en peligro.

Tabla VIII: Evaluación de CSI organización con ranking EGSI “Regular”

Nro.	Factores	Valor	Escala
1	Estratégicos	2	Medio
2	Recursos y competencias	2	Medio
3	Organización / Gestión	2	Medio
4	Mejoramiento continuo	1	Bajo
5	Contexto local, nacional e internacional	1	Bajo
	PROMEDIO	1.6	Medio
	CAPACIDAD DE LA ORGANIZACIÓN	32%	Formativa

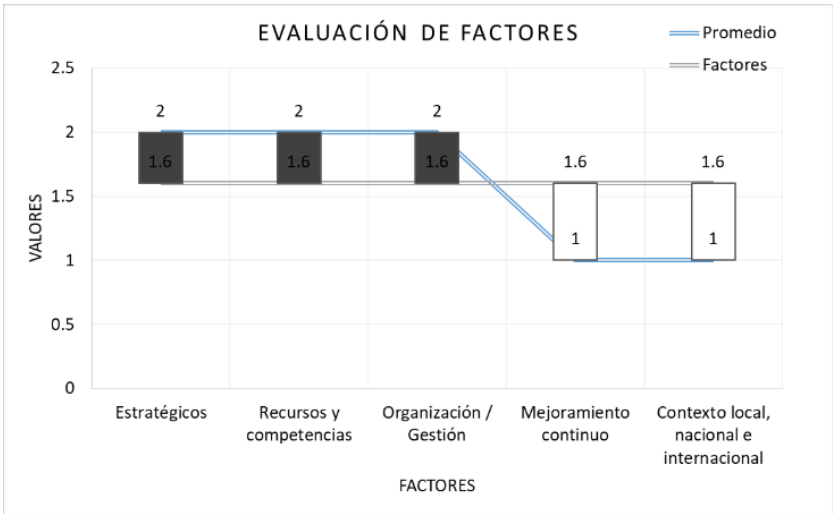


Figura 5: Evaluación de Factores organización con ranking EGSI “Regular”

4.1.2. Modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en instituciones públicas del Ecuador

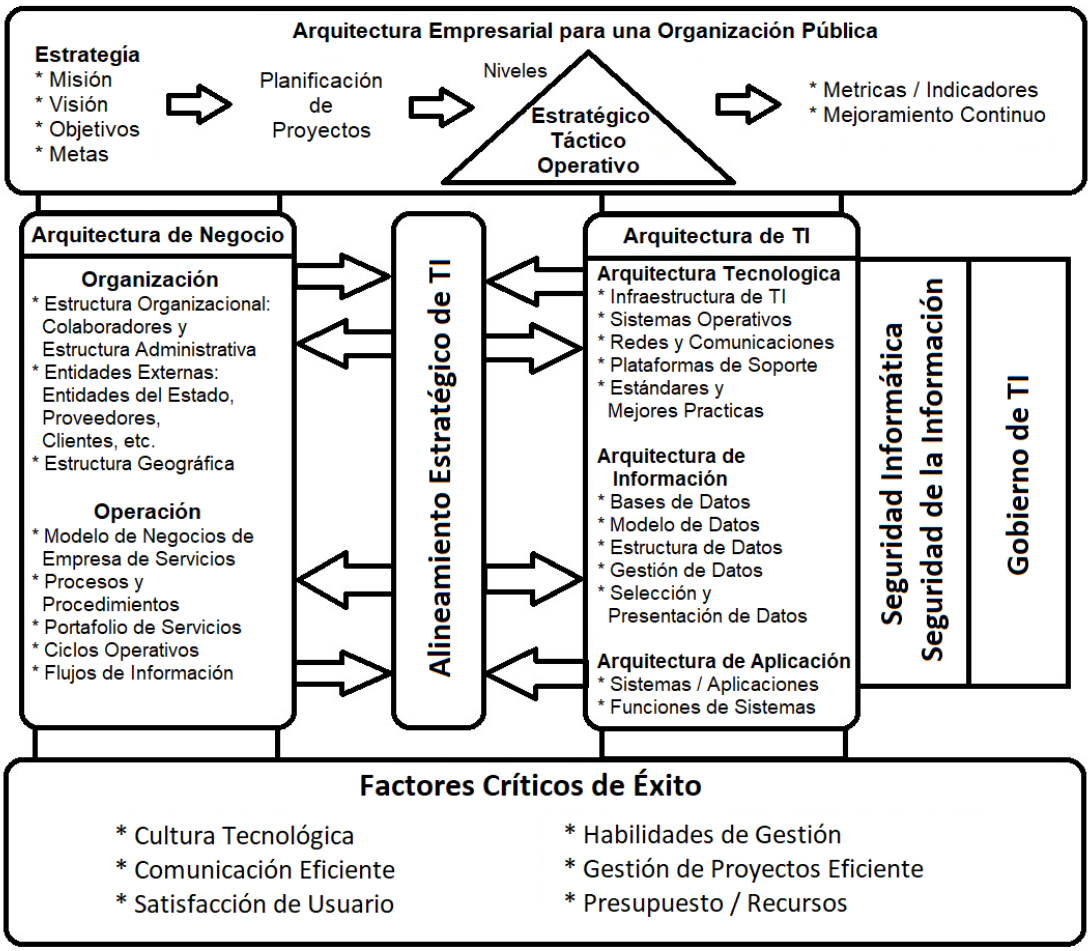


Figura 6: Marco general de arquitectura empresarial para una organización pública.

Planteamiento del modelo de optimización

Como punto de partida representamos un marco de trabajo general de arquitectura empresarial para una organización pública, considerando los principales componentes y factores encontrados en la revisión de la literatura, que se observa en la Figura 6. Luego planteamos un proceso de planificación de proyectos estratégicos para mejorar la seguridad de la información, en la Figura 7, que inicia con el análisis de la situación actual de la seguridad de la información de la organización mediante el modelo para calcular la capacidad de gestión de la seguridad de la información propuesto y esquematizado en la Figura 3.

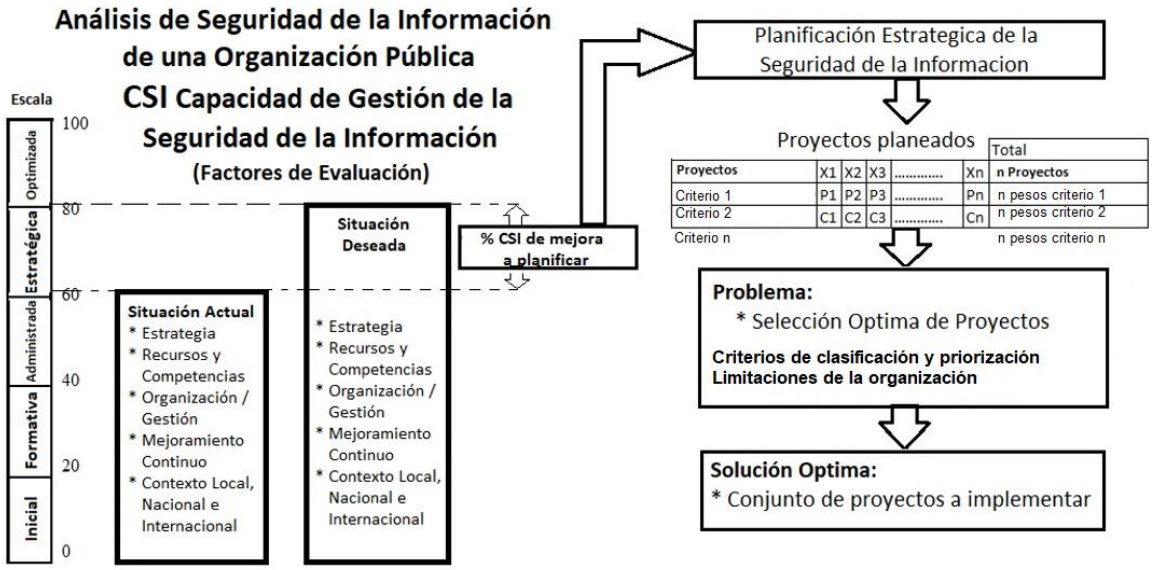


Figura 7: Proceso de planificación de proyectos estratégicos para la seguridad de la información de una organización pública.

Modelo de optimización

Dadas las n variables de decisión, x = (x1, x2, x3,…, xn), representando todos los proyectos planificados para mejorar la seguridad de la información de la organización; el modelo debe obtener un subconjunto de proyectos a ejecutar, que son las soluciones óptimas, que permiten alcanzar cinco objetivos, 1) minimización de costos, 2) maximización origen de cumplimiento, 3) maximización de la relación ganancia/esfuerzo, 4) maximización del tiempo de ejecución y 5) maximización de recursos; limitados por las restricciones, que permiten encontrar el subconjunto de soluciones factibles del problema.

Criterios de optimización

$$Min \rightarrow Y_1 = f_1(x) = \sum_{i=1}^{n} c_i x_i \qquad (7)$$

$$Max \rightarrow Y_2 = f_2(x) = \sum_{i=1}^{n} o_i x_i \qquad (8)$$

$$Max \rightarrow Y_3 = f_3(x) = \sum_{i=1}^{n} g_i x_i \qquad (9)$$

$$Max \rightarrow Y_4 = f_4(x) = \sum_{i=1}^{n} t_i x_i \qquad (10)$$

$$Max \rightarrow Y_5 = f_5(x) = \sum_{i=1}^{n} r_i x_i \qquad (11)$$

Restricciones

$$\sum_{i=1}^{n} c_i x_i \leq P \qquad (12)$$

$$\sum_{i=1}^{n} o_i x_i = 100\% \qquad (13)$$

$$\sum_{i=1}^{n} g_i x_i = 100\% \qquad (14)$$

$$\sum_{i=1}^{n} t_i x_i = 100\% \qquad (15)$$

$$\sum_{i=1}^{n} r_i x_i = 100\% \qquad (16)$$

$$i \succ 0; P \succ 0 \qquad (17)$$

Donde:

c: son los costos requeridos por los proyectos planificados por la organización, que van desde i=1 a “n” proyectos planificados.

o: son las valoraciones de mejora de la seguridad de la información que agrega cada proyecto debido al origen del incumplimiento del proyecto, expresada en términos porcentuales, de los “n” proyectos planificados.

g: son las valoraciones de la relación ganancia/esfuerzo de cada proyecto, expresada en términos porcentuales, de los “n” proyectos planificados.

t: son las valoraciones en base al tiempo de ejecución de cada proyecto, expresada en términos porcentuales, de los “n” proyectos planificados.

r: son las valoraciones de los tipos de recursos requeridos para cada proyecto, expresada en términos porcentuales, de los “n” proyectos planificados.

P: es el presupuesto que la organización ha destinado para ejecutar los proyectos seleccionados.

Modelo simplificado Costo Beneficio

Dado el modelo de las formulas 7 a la 17, de cinco criterios, podemos simplificar el modelo a dos criterios considerando el criterio 1) minimización del costo del proyecto y el criterio 2) maximización de la mejora de la seguridad de la información que aporta cada proyecto en base a la valoración del origen del incumplimiento, la relación ganancia/esfuerzo, el tiempo de ejecución y los tipos de recursos.

Criterios de optimización

$$Min \rightarrow Y_1 = f_1(x) = \sum_{i=1}^{n} c_i x_i \qquad (18)$$

$$Max \rightarrow Y_2 = f_2(x) = \sum_{i=1}^{n} b_i x_i \qquad (19)$$

Restricciones

$$\sum_{i=1}^{n} c_i x_i \leq P \qquad (20)$$

$$\sum_{i=1}^{n} b_i = 100\% \qquad (21)$$

$$\sum_{i=1}^{n} b_i \geq E \qquad (22)$$

$$i \succ 0; P_j \succ 0; E \succ 0 \qquad (23)$$

$$0 \prec E \prec 100\% \qquad (24)$$

Donde:

c: son los costos requeridos por los proyectos planificados por la organización, que van desde i=1 a “n” proyectos planificados.

b: son los beneficios calculados o la contribución de mejora a la seguridad de la información de cada proyecto planificado (CMSI), expresada en términos porcentuales, de los “n” proyectos planificados.

P: es el presupuesto que la organización ha destinado para ejecutar los proyectos seleccionados.

E: es el % de CMSI que la organización espera obtener del 100% de los n proyectos planificados.

Las consideraciones para calcular el % de CMSI de cada proyecto planificado se aprecian en las Tablas IX, X, XI y XII para los criterios origen de incumplimiento, relación ganancia/esfuerzo, tiempo de ejecución y tipo de recurso respectivamente. En el anexo 2 se puede revisar una Tabla con el cálculo del %CMSI para los 30 proyectos planificados, que es un promedio de las contribuciones los cuatro criterios, que luego generamos el %CMSI por medio de la frecuencia relativa porcentual. En el anexo 2 podemos ver el cálculo realizado para él %CMSI de los 30 proyectos planificados; en la Tabla XIII está el resumen de este cálculo, con su respectivo costo y el %CMSI calculado para cada proyecto.

Tabla IX: Valoración por origen de incumplimiento

Abreviatura	Origen de incumplimiento	Valoración
ER	Evaluación de riesgo	25%
AU	Auditoría	50%
ES	Evaluación de Seguridad	75%
IS	Incidente de seguridad	100%

Tabla X: Valoración por relación ganancia/esfuerzo

Abreviatura	Relación ganancia / esfuerzo	Valoración
PFO	Proyecto de Formación	100%
PSE	Proyecto de Seguridad de Eventos	90%
PSA	Proyecto de Seguridad de Accesos	75%
PST	Proyecto de Seguridad de Activos	50%
PPE	Proyecto del Plan de Evaluación	25%

Tabla XI: Valoración por tiempo de ejecución

Tiempo de ejecución	Valoración
Corto	100%
Medio	75%
Largo	50%

Tabla XII: Valoración por tipo de recurso

Recursos	Valoración
Internos	100%
Ambos	50%
Externos	25%

Tabla XIII: Listado de costo y %CMSI de proyectos planificados

No.	Costo (USD)	%CMSI	No.	Costo (USD)	%CMSI	No.	Costo (USD)	%CMSI
1	1,912.00	2.93%	11	4,456.00	3.10%	21	12,874.00	3.22%
2	1,204.00	2.93%	12	1,260.00	3.69%	22	9,612.00	2.63%
3	3,253.00	4.10%	13	6,489.00	2.93%	23	13,360.00	3.69%
4	3,006.00	2.93%	14	7,536.00	3.80%	24	10,558.00	3.22%
5	2,828.00	3.39%	15	9,583.00	4.27%	25	6,107.00	2.63%
6	2,143.00	3.22%	16	9,812.00	3.22%	26	8,616.00	3.51%
7	1,839.00	2.93%	17	14,280.00	4.27%	27	12,925.00	3.51%
8	5,467.00	3.22%	18	6,435.00	2.34%	28	37,299.00	4.68%
9	1,712.00	3.69%	19	9,258.00	2.34%	29	33,211.00	3.98%
10	5,837.00	2.63%	20	14,929.00	3.51%	30	25,190.00	3.51%
					Total, Costo y %CMSI		**282,991.00**	**100.00%**

Aplicación del algoritmo NSGA-II al modelo simplificado

La figura 8 muestra el diagrama de flujo del algoritmo NGA-II para el modelo de optimización simplificado con dos objetivos, la minimización del costo y la maximización del % de CMSI.

El algoritmo de clasificación no dominada NSGA-II crea aleatoriamente la población inicial o conjunto de soluciones iniciales, que para la simulación realizada cada individuo es una solución que tiene la selección de los proyectos estratégicos planificados a ejecutar. Luego esta población inicial va ser sometida a un proceso de mejoramiento en base a un número determinado de iteraciones o generaciones. Para cada generación el algoritmo combina la población actual con la descendencia

resultante para cada iteración. Evaluamos a cada individuo mediante la función objetivo definida en base a los dos criterios definidos en el modelo, costo y %CMSI, luego procedemos a ordenar la población no dominada en frentes, donde los individuos se clasifican mediante la distancia de hacinamiento o apilamiento. Posteriormente, aplicamos los procesos de selección por torneo, cruzamiento y mutación, se seleccionan los individuos ordenados de mejor a peor, lo que da como resultado una mejor población en cada generación. El proceso finaliza cuando se cumpla el número de generaciones definidas en los parámetros de ejecución del algoritmo. Este proceso se muestra en la Fig. 10.

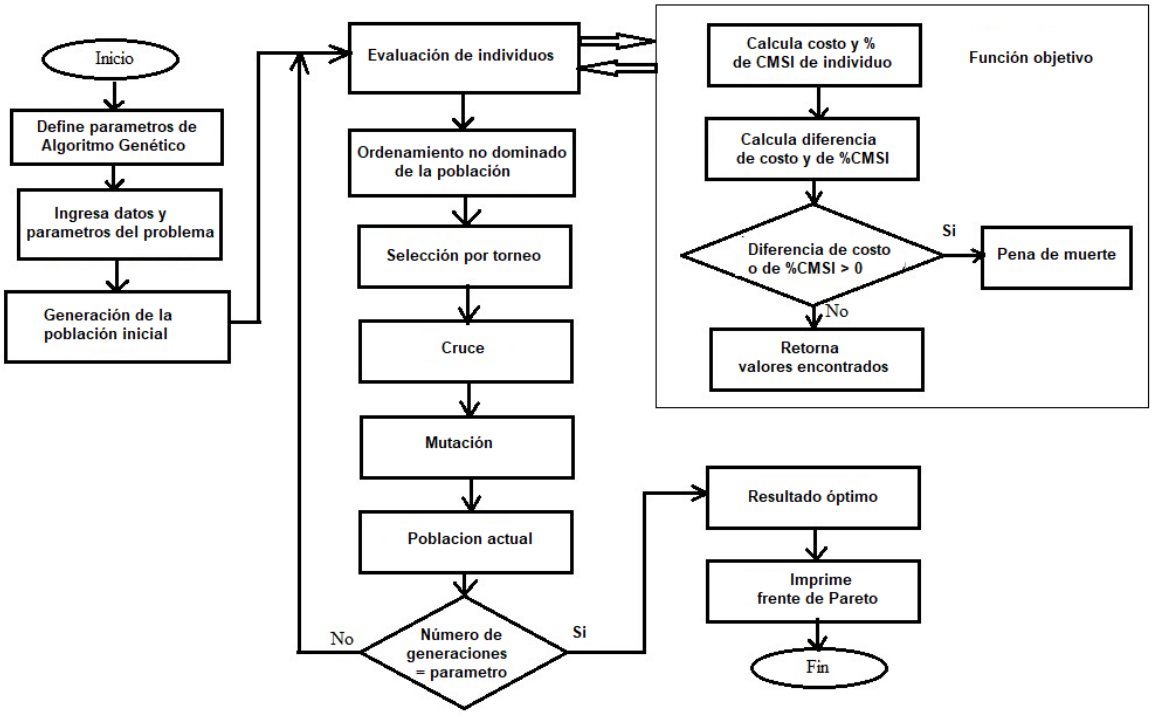


Figura 8: Algoritmo NSGA-II para el modelo de optimización simplificado.

Figura 9: Codificación binaria de cromosoma de 30 genes.

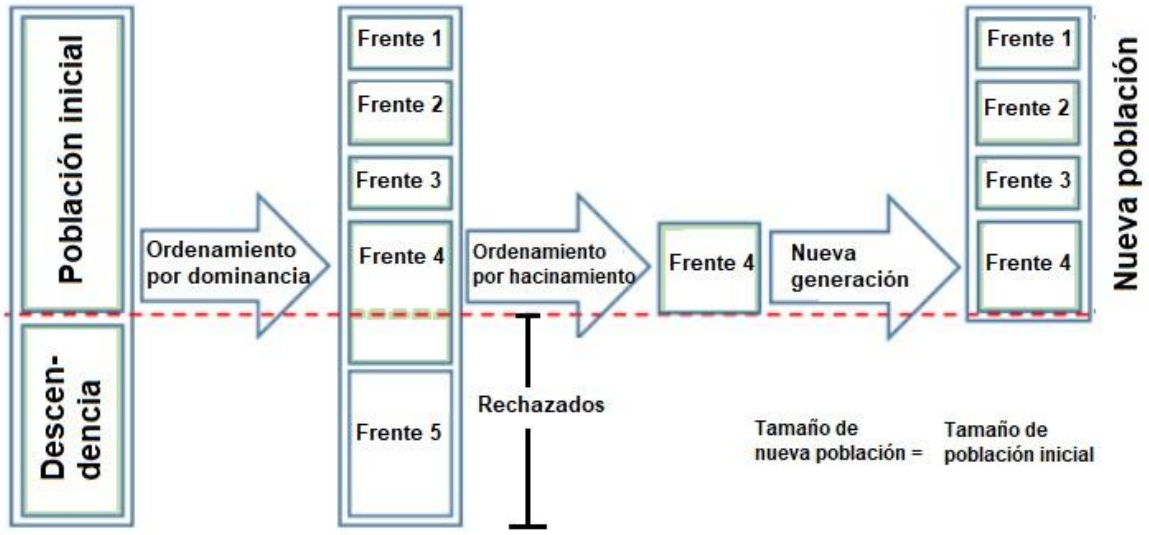


Figura 10: Proceso para crear nueva población en cada generación AG.

A continuación, detallamos las definiciones utilizadas al aplicar el algoritmo genético NSGA-II al modelo de optimización simplificado costo beneficio:

Individuo: Cada individuo o solución lo podemos representar como un cromosoma que tiene 30 genes, que corresponden a los 30 proyectos estratégicos planificados, ver Fig. 9.

Gen: Empleamos la codificación binaria para el algoritmo genético del modelo simplificado, donde cada gen del cromosoma corresponde a un bit (0 o 1), cero significa que en esa solución no se considera ese proyecto, y uno significa que en esa solución si se considera ese proyecto.

Población: En la simulación realizada creamos una población inicial de forma aleatoria de 300 individuos, para garantizar diversidad y representación en las soluciones.

Función fitness: Creamos la función objetivo que evalúa a cada individuo mediante los dos criterios definidos en el modelo, costo y %CMSI. Para el primer criterio se calcula el costo total de la solución y lo compara contra el presupuesto definido por la organización, si la diferencia es mayor que cero aplica pena de muerte y retorna los valores, es decir se le otorga un valor muy elevado para que el proceso siguiente no lo considere. Para el segundo criterio se calcula el %CMSI de la solución y lo compara con el objetivo de este criterio, que para la simulación

es del 80%, si la diferencia es mayor que cero aplica pena de muerte y retorna los valores. Si no existen diferencia retorna los valores calculados en ambos criterios para que sea considerado en el proceso.

Operadores genéticos: Para el mejoramiento de la población, considerando la diversidad genética, en cada iteración se utilizan 3 operadores, la selección, el cruce y la mutación.

Selección: Utilizamos la selección por torneo, donde de forma aleatoria seleccionamos un número de individuos de la población, para reemplazar la descendencia de menor puntuación por la de mejor puntuación según la función objetivo, cumpliendo con el proceso de mejora de la población. Esta selección asegura que solo los mejores padres tengan la posibilidad de tener hijos.

Cruce: Utilizamos el cruce de 2 puntos, el proceso copia al descendiente 1 los genes del cromosoma progenitor 1 desde el inicio hasta el punto 1 de cruce, luego se copia los genes del progenitor 2 desde el inicio del punto de cruce 1 hasta el punto 2; por último, se copia los genes del progenitor 1 desde el punto de cruce 2 hasta el final. Ver Fig. 11. En la simulación realizada se utilizó una probabilidad de cruce de 0.7.

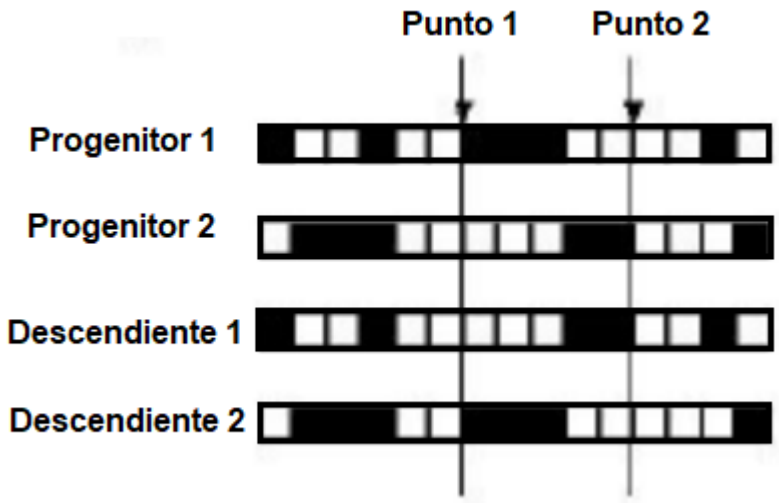


Figura 11: Proceso de cruce de 2 puntos.

Mutación: En la mutación, por tratarse de una codificación binaria, se realiza la inversión del gen mutado de forma aleatoria, si es cero se pone uno, y si es uno se

pone cero. Siempre la probabilidad de mutación del algoritmo genético debe ser bajo porque puede traer problemas contraproducentes en la generación de la nueva población, convirtiéndose en una búsqueda aleatoria. En la simulación realizada se utilizó una probabilidad de mutación de 0.3.

Generaciones: Para la simulación se definió 200 generaciones para que se repita el proceso de evolución de la población. Como se ve en el Anexo 4, las 200 generaciones son suficientes para el proceso de mejora de la población porque se observa una convergencia de las soluciones en la generación 48.

Proceso del AG: Se crea de manera aleatoria una población inicial de 300 individuos. Luego para cada una de las 200 generaciones se evalúan los individuos de la población con la función fitness de los 2 criterios costo y %CMSI. Después se realiza el ordenamiento no dominado de la población en los diferentes frentes, para aplicar los operadores genéticos de selección por torneo, cruce de 2 puntos y mutación. Este proceso se repite hasta que se cumpla con las 200 generaciones definidas. Como resultado se obtiene una nueva población de 300 individuos o soluciones no dominadas, de las cuales se debe determinar cuántas soluciones son diferentes, que serán la base para la toma de decisiones de elegir la mejor o más conveniente.

4.1.3. Simulación

Para facilitar la visualización de los resultados, se ha trabajado con un modelo simplificado de dos objetivos, el costo de cada proyecto en USD y el %CMSI. El %CMSI es un cálculo realizado en base a criterios técnicos como el origen del incumplimiento, la relación ganancia/esfuerzo, el tiempo de ejecución y el tipo de recurso a usar en cada proyecto.

Los parámetros definidos para la simulación son el presupuesto asignado para los proyectos planificados P=$200,000.00 y el % mínimo de CMSI propuesto para el período planificado, para esta simulación es E=80%. Fácilmente podemos analizar que el problema para los administradores de TI de la organización es implementar un subconjunto de proyectos para lograr el mayor % de CMSI con el presupuesto asignado, sabiendo que el 100% del costo de los proyectos planeados exceden el

presupuesto de la organización; para esta simulación el costo total es de $282,991.00.

Considerando los datos de la Tabla III, los parámetros definidos por la organización (presupuesto y % CMSI deseado) y los parámetros definidos para el algoritmo genético de la Tabla XIV, el modelo de optimización obtiene un subconjunto de soluciones factibles.

La ejecución del algoritmo implementado en lenguaje Python versión 3.7, ver Anexo 3. La ejecución se realizó en una computadora con procesador Intel(R) Core(TM) i3-5005U 2.00GHz, con 6.00 GB de RAM y sistema operativo de 64 bits. Los datos de prueba se toman de un escenario creado con información de una organización pública correspondiente a 30 proyectos de mejora de seguridad de bases de datos distribuidas.

El tiempo de respuesta promedio de la ejecución del algoritmo con los datos presentados fue de 25 segundos, lo cual es un costo computacional bastante aceptable, aspecto importante a la hora de implementar herramientas prácticas que ayuden en la planificación y optimización de tareas relacionadas con la seguridad. de la información en las organizaciones.

La Fig. 12 muestra la ventaja que proporciona el subconjunto de soluciones representado por el óptimo de Pareto, donde podemos ver todas las soluciones posibles; La decisión de elegir la mejor solución a implementar se puede tomar analizando la información detallada del óptimo de Pareto, pero adicionalmente podemos comparar las características de los proyectos planificados.

Tabla XIV: Parámetros del Algoritmo Genético

Parámetro	Valor
Probabilidad de cruce	0.7
Probabilidad de mutación	0.3
Número de generaciones	200
Tamaño del torneo	3
Número de cromosomas	30
Número de individuos	300
Rango de variables de decisión	[0 1]

Tabla XV: Soluciones del frente de Pareto

No.	Repeticiones	Población optimizada (frente de Pareto)	Proyectos	%CMSI	Costo (USD)
1	2	[1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1]	26	85.31	200041.00
2	2	[1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1]	26	86.07	200217.00
3	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0]	26	86.25	200686.00
4	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0]	26	86.83	201632.00
5	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1]	27	88.12	201923.00
6	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1]	27	88.71	202869.00
7	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1]	27	89.00	203223.00
8	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0]	27	89.17	210890.00
9	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0]	27	89.47	211244.00
10	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1]	28	91.34	212481.00
11	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0]	28	91.81	220502.00
12	4	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0]	28	92.51	224590.00
13	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1]	28	92.69	236080.00
14	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1]	28	92.98	236434.00
15	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1]	28	93.39	240168.00
16	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1]	28	93.68	240522.00
17	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1]	29	95.32	245692.00
18	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1]	29	96.02	249780.00
19	4	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0]	29	96.49	257801.00
20	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1]	29	96.78	270117.00
21	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1]	29	97.37	273379.00
22	2	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1]	29	97.66	273733.00
23	252	[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]	30	100.00	282991.00

Se encontraron 23 soluciones diferentes no dominadas distribuidas en el frente de Pareto, correspondientes al 7.67% de los 300 individuos finales del proceso. En la Tabla XV podemos ver todas las soluciones óptimas, de las cuales 7 cumplen con el criterio de presupuesto y % de CMSI, tenemos soluciones con % de CMSI de 85.30% a 89.00%, superior al 80% requerido, con un presupuesto cercano a $200,000.00, asignado por la organización. Si el Director de TI tiene la capacidad de lograr un presupuesto más alto, podrá encontrar soluciones que tengan un % de CMSI cercano al 100 %. La explicación que en la Tabla XV la solución 23 se repita 252 veces de las 300, es decir un 84%, se debe a que en la simulación la corrida converge en la iteración 48 como podemos observar en el Anexo 4, luego de cual el algoritmo ya no encuentra mejores soluciones no dominadas y por eso para formar la nueva población mejorada toma el mejor elemento que es la solución 23 que cumple con el 100% del presupuesto establecido.

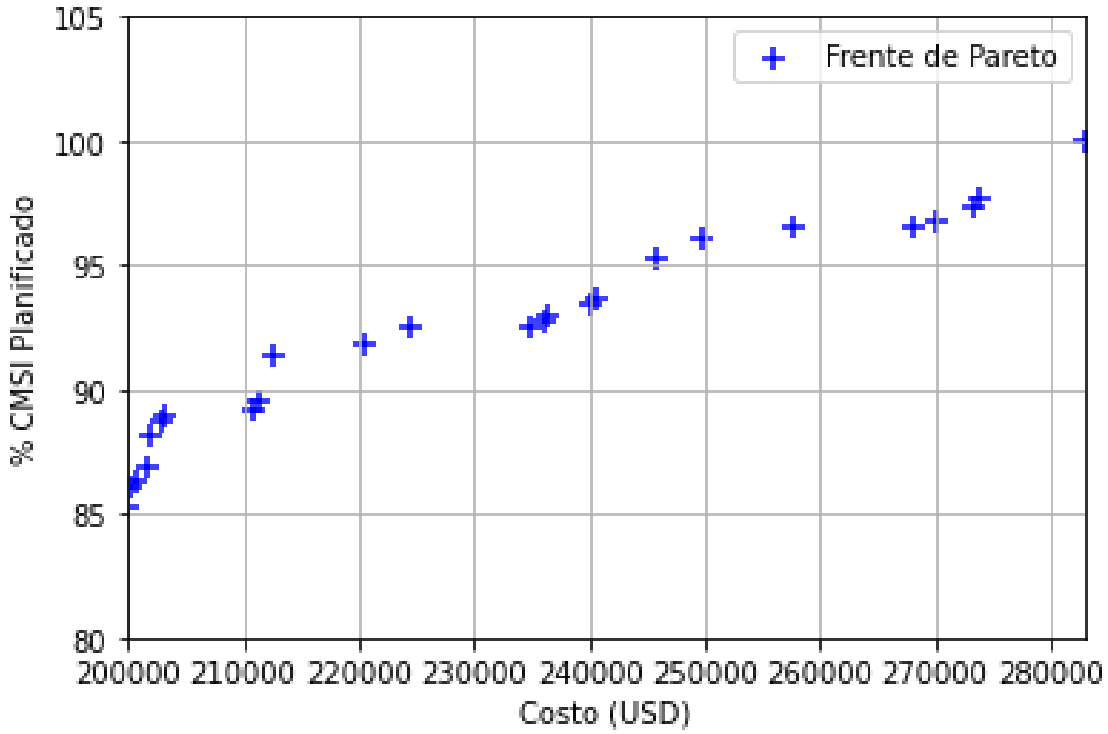


Figura 12: Frente de Pareto (Soluciones Optimas)

4.1.4. Análisis de correlación de variables

Tabla XVI: Matriz de correlación

Número de proyectos	1.00		
Costo (USD)	0.92	1.00	
%CMSI	0.98	0.97	1.00
	Número de proyectos	Costo (USD)	%CMSI

La matriz de correlación de la Tabla XVI muestra los valores calculados del coeficiente de correlación de Pearson para cada par de variables. Los resultados muestran coeficientes de correlación positivas muy altas, tanto para la relación entre el %CMSI y el número de proyectos de la solución con 0,98, como para él %CMSI y el costo con 0,97 y para el número de proyectos y costo es de 0,92. Esta correlación se refleja en las Figuras 12, 13 y 14 que muestran la dependencia de cada par de variables. Las relaciones se describen de la siguiente manera:

- Si aumenta el costo, se aumenta el %CMSI.
- Si aumenta el costo, aumente el número de proyectos a ejecutar.
- Si aumenta el %CMSI, aumentan los proyectos a ejecutar.

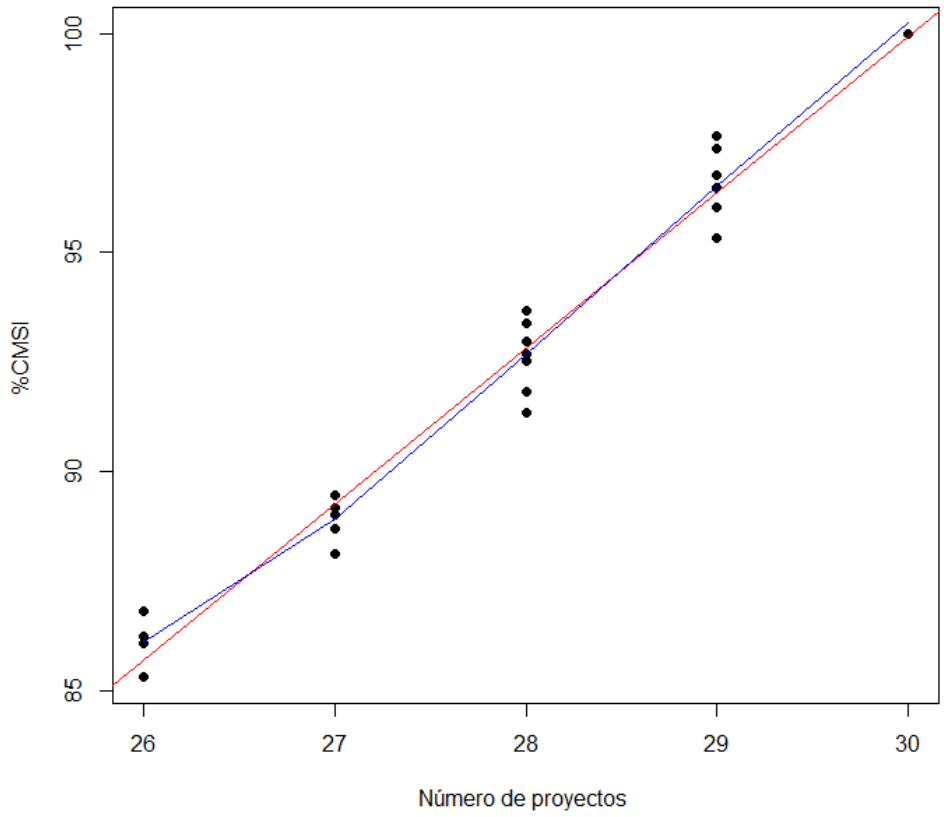


Figura 13: Gráfico de dispersión entre número de proyectos y presupuesto

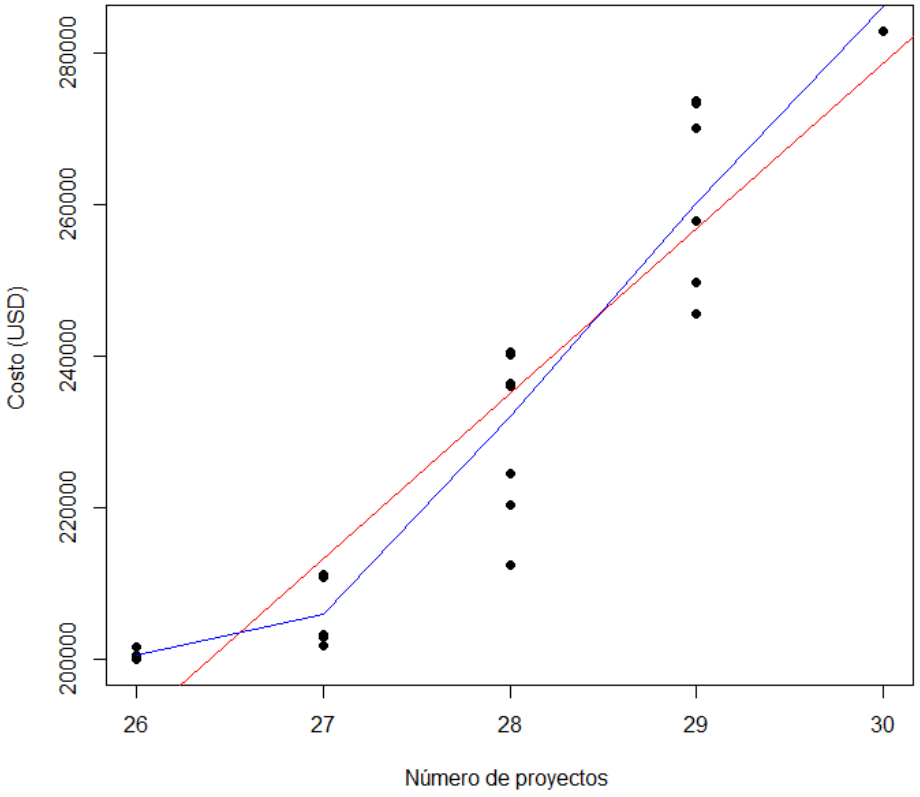


Figura 14: Gráfico de dispersión entre número de proyectos y % IISPP.

4.2. Discusión

4.2.1. Seguridad de la información de las empresas públicas de Ecuador

Este estudio encontró que el 22% de las organizaciones públicas de Ecuador se encuentran en un nivel de CSI “Administrada”, que son organizaciones vulnerables; El 70% de organizaciones públicas con un nivel de CSI “Formativa”, que son organizaciones en peligro. Esto significa que son organizaciones vulnerables, que tiene muchas brechas por cerrar dentro de los 5 factores evaluados.

Entre las condiciones que influyen en estos resultados obtenidos del bajo nivel de gestión de la seguridad de la información de las organizaciones públicas de Ecuador, además del incremento y sofisticación de los ataques cibernéticos, podemos mencionar la falta de una planificación estratégica que direccione los recursos disponibles a la consecución de los objetivos a conseguir. También el limitado presupuesto asignado para estos fines por parte del estado, que pasa por crisis socioeconómicas y peor después de la pandemia del Covid-19. El anterior gobierno diseño un plan para implementar el sistema de gestión de seguridad de la información EGSI en las empresas públicas y creó la Política Nacional de Ciberseguridad, el actual gobierno de Ecuador no le dio la importancia y los recursos necesarios para su continuación.

En Ecuador S. M. Toapanta et al. (2019) encontró resultados similares del 58.6% en mitigación de riesgos, reconociendo que las organizaciones públicas están expuestas a problemas con la ciberseguridad. A nivel internacional Szczepaniuk et al. (2020) también coincidió que existen muchos problemas y vulnerabilidades, se hace necesario implementar y mejorar el SGSI, pero con apoyo del gobierno y colaboración internacional constante en el ámbito de la gestión de la ciberseguridad en las entidades públicas. Estos resultados también coinciden con el reporte de la BID - OEA (2020), para países de América Latina y el Caribe respeto a los avances en temas de ciberseguridad, donde se observan niveles bajos en la mayoría de indicadores del modelo de madurez. Las investigaciones de CHANG (2020), Almeida y Herrera (2019), Aguilar (2019) y Leyva-Méndez (2021), coinciden con nuestros resultados en el bajo nivel de seguridad de Ecuador con relación a otros países de la región, presenta falencias en la identificación de riesgos, faltan

herramientas jurídicas que apoyen a las organizaciones a elevar la seguridad, debe haber una mayor participación del estado y de la comunidad internacional.

4.2.2. Modelo de optimización propuesto

El modelo de optimización implementado es eficiente, se ejecuta en un tiempo bastante aceptable de 25 segundos y ofrece soluciones óptimas para resolver el problema planteado, así lo demuestra las 23 diferentes soluciones no dominadas de la Fig. 9, y el rango de soluciones factibles de acuerdo al presupuesto, que fue un % de CMSI de 85.30% a 89.00%. Decidimos utilizar estos indicadores y no métricas que utilizan la frontera de Pareto real, porque no se la conoce; el cálculo de una aproximación basada en realizar muchas ejecuciones del algoritmo puede interpretarse como un sesgo hacia los resultados obtenidos.

Para facilitar la verificación de los resultados, se simplifico el modelo, no se han considerado criterios como los tiempos de ejecución de los proyectos, ni el porcentaje de éxito al momento de implementar los proyectos. Una limitación de la investigación es la obtención y divulgación de la información de las organizaciones públicas en areas de seguridad, ya que es crítica, poco accesible, no divulgable, que puede ser mal utilizada por gente inescrupulosa.

Los resultados obtenidos en la simulación demuestran la calidad y robustez de las soluciones producidas por el modelo matemático de optimización propuesto. Estos resultados confirman los argumentos teóricos y prácticos de nuestra revisión científica en temas de selección y programación de portafolio de proyectos, problemas de optimización multiobjetivo, algoritmos evolutivos como el NSGA-II, teoría de decisión, entre otros.

Los mejores resultados se obtendrán cuantos más recursos o presupuesto tenga la organización, ya que tanto el % CMSI como los proyectos a ejecutar aumentan con un mayor presupuesto, son variables con una alta correlación positiva.

Este problema de optimización de 2 objetivos, uno de minimización y otro de maximización, se cumple la teoría de dominancia y óptimo de Pareto, los objetivos se encuentran en conflicto, esto implica que no se puede mejorar uno sin perjudicar el otro. En este caso el costo y el % CMSI, son objetivos en conflicto. Este problema

multiobjetivo no tienen solución única, sino un conjunto de soluciones, que se denomina “Frente Pareto” de la Fig. 12, donde encontramos las mejores soluciones o soluciones no dominadas. La simulación realizada con el conjuntos de 30 proyectos estratégicos planificados con el algoritmo NSGA-II, genera múltiples conjuntos de Pareto, exactamente 23, que deben ser evaluados con el fin de encontrar el mejor de ellos para implementar. Lo que este modelo propuesto facilita es una herramienta para mejorar la toma de decisiones de los Directores de TI o los encargados de administrar los proyectos a implementar.

Candia-García, López-Castro, and Jaimes-Suárez (2020), De Greiff and Rivera (2018), Balderas et al. (2019), ACAR and ALIOUI (2020), Abouhawwash and Deb (2021), Awad et al. (2022), Stepanov et al. (2019), Stepanov et al. (2019), Abido & Elazouni (2021), Awad et al. (2022) y Kebriyaii et al. (2021), aplicaron algoritmos genéticos, tanto para el problema critico de selección de portafolio de proyectos y de otros problemas de optimización multiobjetivo con resultados similares al de este trabajo; que permitió a los tomadores de decisiones tener un conjunto de soluciones optimas, de calidad, a un tiempo razonable, que se pueden implementar en aplicaciones prácticas. La mayoría de estos trabajos se han centrado en la comparación con varios algoritmos evolutivos. Este trabajo se diferencia de los encontrados en la literatura porque muestra un alto porcentaje de cumplimiento práctico de la simulación realizada, del 85,30% al 89,00%, en un área diferente.

CAPÍTULO V: CONCLUSIONES.

1. Mediante este trabajo se demostró que el modelo de optimización propuesto para la selección de proyectos en ciberseguridad permite mejorar la seguridad de la información en el rango del CMSI de 85.30% a 89.00%, además se mejora la eficiencia de utilización de recursos en organizaciones públicas del Ecuador. Este modelo de optimización puede generalizarse para encontrar las mejores soluciones a cualquier problema de selección de proyectos planificado en base a dos criterios opuestos, donde uno se maximiza y el otro se minimiza.
2. Los ataques e incidentes de ciberseguridad se han incrementado a en todo el mundo, y cada vez son más sofisticados tecnológicamente, que los hace más efectivos y peligrosos, frente a Organizaciones Públicas que no están preparadas para afrontar estos ataques. Esto lo confirma las estadísticas y casos de conocimiento público de empresas nacionales e internacionales que han sido objeto de incidentes que han provocado enormes pérdidas. El presente trabajo determino que las organizaciones públicas de Ecuador tienen un bajo nivel de capacidad de Gestión de la Seguridad de la Información; el 70% se encuentran en un nivel “Formativo” y el 22% en un nivel “Administrado”; son organizaciones con deficiencias y carencias, que se encuentran vulnerables a todos los peligros, amenazas y ataques a la Seguridad de la Información.
3. De la revisión de la literatura y de la práctica en las organizaciones públicas encontramos muchas variables y factores a considerar para clasificar y priorizar proyectos en ciberseguridad, sin embargo, consideramos los más importantes los costos requeridos por los proyectos planificados, el origen del incumplimiento del proyecto, la relación ganancia/esfuerzo de cada proyecto, el tiempo de ejecución de cada proyecto y los tipos de recursos requeridos para cada proyecto. Mediante un enfoque costo/beneficio logramos resumir estos 5 factores para presentar un modelo de optimización que mejora a la ciberseguridad de las organizaciones públicas en base a un indicador de beneficio que creamos denominado CMSI.

4. El modelo matemático expresado en las fórmulas (18) - (24) es un problema de optimización multiobjetivo con dos criterios contrapuestos, como son la minimización de los recursos disponibles por parte de la organización y la maximización del % de CMSI. El modelo propuesto es fácil de implementar, muy práctico y puede ser una herramienta de apoyo a la gestión de TI y la toma de decisiones en una organización pública.
5. La simulación verificó que el modelo propuesto es eficiente, encontramos un grupo de soluciones no dominadas en el óptimo de Pareto con un % de CMSI de 85.30% a 89.00%, las cuales cumplen con el presupuesto establecido por la organización.

CAPÍTULO VI: RECOMENDACIONES

1. Las organizaciones públicas deben adoptar modelos y herramientas que sean prácticos y de fácil implementación, que permita a los directivos de las organizaciones públicas tomar mejores decisiones, con el uso eficiente de los recursos asignados, como el modelo propuesto en este trabajo.
2. Otra herramienta a considerar para las organizaciones públicas, es el modelo de Capacidad de Gestión de la Seguridad de la Información CSI, que permite analizar y evaluar la situación actual de ciberseguridad en base a 5 factores: 1 Estratégicos, 2 Recursos y Competencias, 3 Organización / Gestión, 4 Mejoramiento Continuo, y 5 Contexto local, nacional e internacional. El quinto factor implica que la Gestión de la Seguridad de la Información de las Organizaciones sea acompañada del apoyo del gobierno y la colaboración internacional permanente en el ámbito de la gestión de la seguridad de la información.
3. Es importante a nivel de país estandarizar los criterios para clasificar y priorizar proyectos de ciberseguridad, para que las herramientas y modelos se puedan implementar en todas las organizaciones públicas.
4. Para tener éxito las organizaciones públicas deben aplicar en su arquitectura empresarial y gobernanza de TI, una gestión de proyectos eficiente. Por eso el modelo de optimización propuesto es un acercamiento importante a este tipo de herramientas para apoyo de la gestión de TI y para la toma de decisiones.
5. Para los próximos trabajos, se propone ampliar el conjunto de datos de prueba considerando todos los proyectos previstos para mejorar la seguridad de la información de una organización pública; también debe incluir otros criterios para clasificar y priorizar, otros tipos de recursos que se utilizan en la planificación del proyecto, no solo el costo, de esta forma tendremos una mejor validación del modelo propuesto. Se debe realizar una comparación con otros algoritmos de optimización y se debe combinar el NSGA-II con métodos de inteligencia artificial que permitan obtener las soluciones más eficientes.

6. Para una mejor implementación del modelo de optimización para la selección de proyecto s estratégicos de ciberseguridad en las organizaciones, se recomienda seguir los procedimientos del Anexo 5 que se describe un plan implementación para una organización pública y el Anexo 6 que detalla un cronograma de implementación.

REFERENCIAS BIBLIOGRÁFICAS

Abdalla, Mohammed Hussein, and Murat Karabatak. 2020. “To Review and Compare Evolutionary Algorithms in Optimization of Distributed Database Query.” Pp. 1–5 in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*.

Abido, Mohammad A., and Ashraf Elazouni. 2021. “Modified Multi-Objective Evolutionary Programming Algorithm for Solving Project Scheduling Problems.” *Expert Systems with Applications* 183(July 2020). doi: 10.1016/j.eswa.2021.115338.

Abouhawwash, Mohamed, and Kalyanmoy Deb. 2021. “Reference Point Based Evolutionary Multi-Objective Optimization Algorithms with Convergence Properties Using KKTPM and ASF Metrics.” *Journal of Heuristics* 27(4):575–614. doi: 10.1007/s10732-021-09470-4.

Acar, Reşat, and Youssef Aliqui. 2020. “An Evaluation of a Constrained Multi-Objective Genetic Algorithm.” *Journal of Scientific Perspectives* 4(2):137–46. doi: 10.26900/jsp.4.011.

Aguilar, Juan Antonio Manuel. 2019. “Hechos Ciberfísicos: Una Propuesta de Análisis Para Ciberamenazas En Las Estrategias Nacionales de Ciberseguridad.” *URVIO Revista Latinoamericana de Estudios de Seguridad* (25):24–40.

Ahrari, Ali, Saber Elsayed, Ruhul Sarker, Daryl Essam, and Carlos A. Coello Coello. 2021. “Weighted Pointwise Prediction Method for Dynamic Multiobjective Optimization.” *Information Sciences* 546:349–67. doi: 10.1016/j.ins.2020.08.015.

Akhmetov, Berik, Valeriy Lakhno, Bakhytzhan Akhmetov, Yuri Myakuhin, Asselkhan Adranova, and Lazat Kydyralina. 2019. “Models and Algorithms of Vector Optimization in Selecting Security Measures for Higher Education Institution’s Information Learning Environment.” Pp. 135–42 in *Intelligent Systems in*

Cybernetics and Automation Control Theory, edited by R. Silhavy, P. Silhavy, and Z. Prokopova. Cham: Springer International Publishing.

Al-Matari, Osamah M. M., Iman M. A. Helal, Sherif A. Mazen, and Sherif Elhennawy. 2021. “Adopting Security Maturity Model to the Organizations’ Capability Model.” *Egyptian Informatics Journal* 22(2):193–99. doi: 10.1016/j.eij.2020.08.001.

Algarni, Mohammed, Mashhour A. Alazwari, and Mohammad Reza Safaei. 2021. “Optimization of Nano-Additive Characteristics to Improve the Efficiency of a Shell and Tube Thermal Energy Storage System Using a Hybrid Procedure: DOE, ANN, MCDM, MOO, and CFD Modeling.” *Mathematics* 9(24):3235. doi: 10.3390/math9243235.

Almeida, Carlos Arturo Tates, and L. R. Herrera. 2019. “La Ciberseguridad En El Ecuador, Una Propuesta de Organización.” *Revista de Ciencias de Seguridad y Defensa, IV* 7:156–69.

de Almeida, Jonatas Araùjo, and Rudolf Vetschera. 2021. “Bounds in Tree-Based Approaches to Generate Project Portfolios in the Presence of Interactions.” *International Journal of Decision Support System Technology (IJDSST)* 13(4):50–70.

AlYousef, Mutep Y., and Nabih T. Abdelmajeed. 2019. “Dynamically Detecting Security Threats and Updating a Signature-Based Intrusion Detection System’s Database.” *Procedia Computer Science* 159:1507–16. doi: https://doi.org/10.1016/j.procs.2019.09.321.

Amine, Khalil. 2019. “Multiobjective Simulated Annealing: Principles and Algorithm Variants.” *Advances in Operations Research* 2019. doi: 10.1155/2019/8134674.

Antoniou, George S. 2018. “A Framework for the Governance of Information Security: Can It Be Used in an Organization.” Pp. 1–30 in *SoutheastCon 2018*. IEEE.

Apelt, Stefan, Hanna Geppert, Hussein Hasso, and Thomas Kudla. 2018. “Measuring the Coverage of Requirements through Enterprise Architecture Models.” Pp. 1–5 in *2018 International Conference on Military Communications*

and Information Systems (ICMCIS). IEEE.

Arbanas, Krunoslav, and Nikolina Žajdela Hrustek. 2019. “Key Success Factors of Information Systems Security.” *Journal of Information and Organizational Sciences* 43(2):131–44. doi: 10.31341/jios.43.2.1.

Arora, Ashish, Dennis Hall, C. A. Piato, Dwayne Ramsey, and Rahul Telang. 2004. “Measuring the Risk-Based Value of IT Security Solutions.” *IT Professional* 6(6):35–42. doi: 10.1109/MITP.2004.89.

Asamblea Nacional del Ecuador. 2004. *LOTAIP*. Ecuador.

Asamblea Nacional del Ecuador. 2009. *LOEP*. Ecuador.

Atta, Soumen, Priya Ranjan Sinha Mahapatra, and Anirban Mukhopadhyay. 2021. “A Multi-Objective Formulation of Maximal Covering Location Problem with Customers’ Preferences: Exploring Pareto Optimality-Based Solutions.” *Expert Systems with Applications* 186:115830. doi: 10.1016/j.eswa.2021.115830.

Audet, Charles, Jean Bigeon, Dominique Cartier, Sébastien Le Digabel, and Ludovic Salomon. 2021. “Performance Indicators in Multiobjective Optimization.” *European Journal of Operational Research* 292(2):397–422.

Awad, Mahmoud, Mohamed Abouhawwash, and HN Agiza. 2022. “On NSGA-II and NSGA-III in Portfolio Management.” *Intelligent Automation & Soft Computing* 32(3):1893–1904.

Bai, Libiao, Xiao Han, Hailing Wang, Kaimin Zhang, and Yichen Sun. 2021. “A Method of Network Robustness under Strategic Goals for Project Portfolio Selection.” *Computers & Industrial Engineering* 161:107658. doi: 10.1016/j.cie.2021.107658.

Balderas, Fausto, Eduardo Fernandez, Claudia Gomez-Santillan, Nelson Rangel-Valdez, and Laura Cruz. 2019. “An Interval-Based Approach for Evolutionary Multi-Objective Optimization of Project Portfolios.” *International Journal of Information Technology & Decision Making* 18(4):1317–58. doi: 10.1142/S021962201950024X.

BID - OEA. 2020. *Ciberseguridad Riesgos, Avances y El Camino a Seguir En América Latina y El Caribe*.

Biswas, Surama, and Sriyankar Acharyya. 2021. “Multi-Objective Simulated Annealing Variants to Infer Gene Regulatory Network: A Comparative Study.” *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 18(6):2612–23. doi: 10.1109/TCBB.2020.2992304.

Bitzer, Michael, Nicolas Brinz, and Philipp Ollig. 2021. “Disentangling the Concept of Information Security Properties: Enabling Effective Information Security Governance.” in *ECIS 2021 Research Papers*. Vol. 134.

Bojanc, Rok, and Borka Jerman-Blažič. 2012. “Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System.” *JMISHR* 45(6). doi: 10.2478/v10051-012-0027-z.

Bushuyev, Sergey, Nataliya Gaydukova, Nataliya Bushuyeva, and Igor Achkasov. 2021. “Evaluation of the Investment Projects Portfolio Efficiency.” Pp. 351–54 in *2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT)*. Vol. 2. IEEE.

Calbert, Gregory, Terence Weir, Ivan L. Garanovich, and Carlos C. N. Kuhn. 2022. “A Temporal Knapsack Approach to Defence Portfolio Selection.” Pp. 159–91 in *Evolutionary and Memetic Computing for Project Portfolio Selection and Scheduling*. Springer Science and Business Media Deutschland GmbH.

Candia-García, Cristian David, Luis Francisco López-Castro, and Sonia Alexandra Jaimes-Suárez. 2020. “Selección Óptima Del Portafolio de Proyectos Utilizando Metaheurísticas de Población y Trayectoria Meta-Optimizadas.” *Revista EIA* 17(34):271–88.

Chang, Jorge Enrique Alvarado. 2020. “Análisis de Ataques Cibernéticos Hacia El Ecuador.” *Editora Adjunta* 2:18.

Chen, Jing, Tiantian Du, and Gongyi Xiao. 2021. “A Multi-Objective Optimization for Resource Allocation of Emergent Demands in Cloud Computing.” *Journal of Cloud Computing* 10(1):1–17. doi: 10.1186/s13677-021-00237-7.

Contraloría General del Estado. 2009. “Normas de Control Interno de La Contraloria General Del Estado.” *Registro Oficial Suplemento* 87.

Crespo Sánchez, Gustavo, Ignacio Pérez Abril, and Zaid García Sánchez. 2022. “Exploración Científica de Los Algoritmos Evolutivos En La Reconfiguración

Óptima de Redes de Distribución Eléctrica.” *Revista Universidad y Sociedad* 14(1):303–19.

Deb, Kalyanmoy, Amrit Pratap, Sameer Agarwal, and Tamt Meyarivan. 2002. “A Fast and Elitist Multiobjective Genetic Algorithm: NSGA-II.” *IEEE Transactions on Evolutionary Computation* 6(2):182–97. doi: 10.1109/4235.996017.

Deloitte. 2020. *Estado Actual de La Ciberseguridad Ecuador 2020*.

Diesch, Rainer, Matthias Pfaff, and Helmut Krcmar. 2020. “A Comprehensive Model of Information Security Factors for Decision-Makers.” *Computers & Security* 92:101747. doi: 10.1016/j.cose.2020.101747.

Doerr, Benjamin, and Frank Neumann. 2019. “Theory of Evolutionary Computation: Recent Developments in Discrete Optimization.”

Duan, Youxiang, Ning Chen, Lunjie Chang, Yongjing Ni, S. V. N. Santhosh Kumar, and Peiying Zhang. 2022. “CAPSO: Chaos Adaptive Particle Swarm Optimization Algorithm.” *IEEE Access* 10:1–1. doi: 10.1109/access.2022.3158666.

e-Governance Academy Foundation. 2019. “National Cyber Security Index NCSI.” *CSIRT*. Retrieved March 8, 2021 (https://csirt.celec.gob.ec/en/contenidos/estadisticas).

ESET. 2020. *Security Report Latinoamérica 2020*.

Fernández, Eduardo, Nelson Rangel-Valdez, Laura Cruz-Reyes, and Claudia Gomez-Santillan. 2021. “A New Approach to Group Multi-Objective Optimization under Imperfect Information and Its Application to Project Portfolio Optimization.” *Applied Sciences* 11(10):4575. doi: 10.3390/app11104575.

Fernández, Eduardo, Efrain Solares, Carlos A. Coello Coello, and Victor De-León-Gómez. 2022. “An Overall Characterization of the Project Portfolio Optimization Problem and an Approach Based on Evolutionary Algorithms to Address It.” Pp. 65–88 in *Evolutionary and Memetic Computing for Project Portfolio Selection and Scheduling*. Springer Science and Business Media Deutschland GmbH.

Girón, Carolina León. 2020. “Enterprise Architecture Model Oriented to Architecture, Engineering and Construction Industry: Integration of Geospatial Concepts in a Specific Framework.” Pp. 1–6 in *2020 15th Iberian Conference on Information*

Systems and Technologies (CISTI). IEEE.

De Greiff, Samuel, and Juan Carlos Rivera. 2018. “Optimización de Portafolios de Inversión Con Costos de Transacción Utilizando Un Algoritmo Genético Multiobjetivo: Caso Aplicado a La Bolsa de Valores de Colombia.” *Estudios Gerenciales* 34(146):74–87.

Guerrero, Carlos, Isaac Lera, Belen Bermejo, and Carlos Juiz. 2018. “Multi-Objective Optimization for Virtual Machine Allocation and Replica Placement in Virtualized Hadoop.” *IEEE Transactions on Parallel and Distributed Systems* 29(11):2568–81. doi: 10.1109/TPDS.2018.2837743.

Gupta, Rajesh, Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar. 2020. “Machine Learning Models for Secure Data Analytics: A Taxonomy and Threat Model.” *Computer Communications* 153:406–40. doi: 10.1016/j.comcom.2020.02.008.

Harrison, Kyle Robert, Saber M. Elsayed, Ivan L. Garanovich, Terence Weir, Sharon G. Boswell, and Ruhul Amin Sarker. 2022. “A New Model for the Project Portfolio Selection and Scheduling Problem with Defence Capability Options.” Pp. 89–123 in *Evolutionary and Memetic Computing for Project Portfolio Selection and Scheduling*. Springer Science and Business Media Deutschland GmbH.

Harrison, Kyle Robert, Saber Elsayed, Ruhul A. Sarker, Ivan L. Garanovich, Terence Weir, and Sharon G. Boswell. 2021. “Project Portfolio Selection with Defense Capability Options.” Pp. 1825–26 in *Proceedings of the Genetic and Evolutionary Computation Conference Companion*. Association for Computing Machinery, Inc.

Harrison, Kyle Robert, Ivan Leonidovich Garanovich, Terence Weir, Sharon G. Boswell, Saber M. Elsayed, and Ruhul Amin Sarker. 2022. “Evolutionary and Memetic Computing for Project Portfolio Selection and Scheduling: An Introduction.” Pp. 1–8 in *Evolutionary and Memetic Computing for Project Portfolio Selection and Scheduling*. Springer Science and Business Media Deutschland GmbH.

Hashemi, Seyed Mahmood, Jingsha He, and Alireza Ebrahimi Basabi. 2017. “Multi-Objective Optimization for Computer Security and Privacy.” *Int. J. Netw. Secur.*

19(3):394–405.

Hesarsorkh, Aghil Hamidi, Jalal Ashayeri, and Ali Bonyadi Naeini. 2021. “Pharmaceutical R&D Project Portfolio Selection and Scheduling under Uncertainty: A Robust Possibilistic Optimization Approach.” *Computers & Industrial Engineering* 155:107114. doi: 10.1016/j.cie.2021.107114.

Hoffmann, Romuald, Jarosław Napiórkowski, Tomasz Protasowicki, and Jerzy Stanik. 2020. “Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach.” *Procedia Manufacturing* 44:647–54. doi: 10.1016/j.promfg.2020.02.244.

Holland, John H. 1992. “Genetic Algorithms.” *Scientific American* 267(1):66–73.

IBM. 2022. “¿Qué Es La Ciberseguridad?” *IBM*. Retrieved June 7, 2022 (https://www.ibm.com/es-es/topics/cybersecurity#:~:text=La ciberseguridad es la práctica,confidencial de los ataques digitales.).

INCIBE. 2016. “6 Criterios Para Categorizar y Priorizar Tus Proyectos de Ciberseguridad En La Empresa.” *Instituto Nacional de Ciberseguridad*. Retrieved July 29, 2022 (https://www.incibe.es/protege-tu-empresa/blog/criterios-clasificar-y-priorizar-proyectos-ciberseguridad-en-empresa).

Ishibuchi, Hisao, Ryo Imada, Yu Setoguchi, and Yusuke Nojima. 2018. “How to Specify a Reference Point in Hypervolume Calculation for Fair Performance Comparison.” *Evolutionary Computation* 26(3):411–40.

Jafarzadeh, H., J. Heidary-Dahooie, P. Akbari, and A. Qorbani. 2022. “A Project Prioritization Approach Considering Uncertainty, Reliability, Criteria Prioritization, and Robustness.” *Decision Support Systems*. doi: 10.1016/j.dss.2022.113731.

Joshi, Mahesh, Bodhisatwa Mazumdar, and Somnath Dey. 2020. “A Comprehensive Security Analysis of Match-in-Database Fingerprint Biometric System.” *Pattern Recognition Letters* 138:247–66. doi: https://doi.org/10.1016/j.patrec.2020.07.024.

Juang, Chia-Feng, and Trong Bac Bui. 2020. “Reinforcement Neural Fuzzy Surrogate-Assisted Multiobjective Evolutionary Fuzzy Systems With Robot

Learning Control Application." *IEEE Transactions on Fuzzy Systems* 28(3):434–46. doi: 10.1109/TFUZZ.2019.2907513.

Katsupeev, A. A., E. A. Shcherbakova, and S. P. Vorobyev. 2016. "Comparison of Evolutionary Algorithms Used to Solve the Optimization Problem of Information Security of Distributed Systems." Pp. 1–3 in *2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*.

Kebriyaii, Omid, Ali Heidari, Mohammad Khalilzadeh, Jurgita Antucheviciene, and Miroslavas Pavlovskis. 2021. "Application of Three Metaheuristic Algorithms to Time-Cost-Quality Trade-Off Project Scheduling Problem for Construction Projects Considering Time Value of Money." *Symmetry* 13(12):2402. doi: 10.3390/sym13122402.

Khatun, M. T., K. Hiekata, Y. Takahashi, and I. Okada. 2021. *Dynamic Modeling of Resource Allocation for Project Management in Multi-Project Environment*. Vol. 16. edited by M. B. R. M. B. R. J. S. W. N. Newnes L. Lattanzio S. IOS Press BV.

Kirenberg, Aleksandr, Aleksey Medvedev, and Evgeniya Prokopenko. 2020. "A Mathematical Model of Information Security for a Mining Company." P. 4012 in *E3S Web of Conferences*. Vol. 174.

Klakegg, Ole Jonny. 2017. "Project Delivery Models — Situational or Fixed Design?" Pp. 202–6 in *2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)*. Vol. 2. Institute of Electrical and Electronics Engineers Inc.

Klyaus, T. K., and Yu A. Gatchin. 2020. "Mathematical Model For Information Security System Effectiveness Evaluation Against Advanced Persistent Threat Attacks." Pp. 1–5 in *2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*.

Kolisch, Rainer, and Thomas Fliedner. 2022. "A Decision Support System for Planning Portfolios of Supply Chain Improvement Projects in the Semiconductor Industry." Pp. 193–212 in *EEvolutionary and Memetic Computing for Project Portfolio Selection and Scheduling*. Vol. 26. Springer Science and Business Media Deutschland GmbH.

Kumar, Ganivada Phanindra, and Premalata Jena. 2020. “Pearson’s Correlation Coefficient for Islanding Detection Using Micro-PMU Measurements.” *IEEE Systems Journal* 15(4):5078–89. doi: 10.1109/JSYST.2020.3021922.

Lakhno, Valeriy, Bakhytzhan Akhmetov, Saltanat Adilzhanova, Andrii Blozva, Rzaieva Svitlana, and Rzaiev Dmytro. 2020. “The Use of a Genetic Algorithm in the Problem of Distribution of Information Security Organizational and Financial Resources.” Pp. 251–54 in *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*.

Leyva-Méndez, Alan Eduardo. 2021. “Análisis de Políticas Públicas de Seguridad Cibernética. Estudio Del Caso Ecuatoriano.” *Polo Del Conocimiento* 6(3):1229–50.

Li, Jing, Wei Zuo, E. Jiaqiang, Yuntian Zhang, Qingqing Li, Ke Sun, Kun Zhou, and Guangde Zhang. 2022. “Multi-Objective Optimization of Mini U-Channel Cold Plate with SiO2 Nanofluid by RSM and NSGA-II.” *Energy* 242:123039. doi: 10.1016/j.energy.2021.123039.

Li, Senyu, Fangming Bi, Wei Chen, Xuzhi Miao, Jin Liu, and Chaogang Tang. 2018. “An Improved Information Security Risk Assessments Method for Cyber-Physical-Social Computing and Networking.” *IEEE Access* 6:10311–19. doi: 10.1109/ACCESS.2018.2800664.

Li, Yuanzheng, Zhixian Ni, Tianyang Zhao, Minghui Yu, Yun Liu, Lei Wu, and Yong Zhao. 2020. “Coordinated Scheduling for Improving Uncertain Wind Power Adsorption in Electric Vehicles—Wind Integrated Power Systems by Multiobjective Optimization Approach.” *IEEE Transactions on Industry Applications* 56(3):2238–50. doi: 10.1109/TIA.2020.2976909.

Li, Zhixi, Vincent Tam, and Lawrence K. Yeung. 2021. “An Adaptive Multi-Population Optimization Algorithm for Global Continuous Optimization.” *IEEE Access* 9:19960–89.

Liesiö, J., A. Salo, J. M. Keisler, and A. Morton. 2021. “Portfolio Decision Analysis: Recent Developments and Future Prospects.” *European Journal of Operational Research* 293(3):811–25. doi: 10.1016/j.ejor.2020.12.015.

Liu, Yuan, Ningbo Zhu, and Miqing Li. 2021. “Solving Many-Objective Optimization

Problems by a Pareto-Based Evolutionary Algorithm with Preprocessing and a Penalty Mechanism." *IEEE Transactions on Cybernetics* 51(11):5585–94. doi: 10.1109/TCYB.2020.2988896.

López, Javier. 2013. "Optimización Multiobjetivo: Aplicaciones a Problemas Del Mundo Real." *Buenos Aires, Argentina, Universidad Nacional de La Plata*.

Mahmoudi, Amin, Mehdi Abbasi, and Xiaopeng Deng. 2022. "A Novel Project Portfolio Selection Framework towards Organizational Resilience: Robust Ordinal Priority Approach." *Expert Systems with Applications* 188:116067. doi: 10.1016/j.eswa.2021.116067.

Marchinares, Augusto Hayashida, and Ciro Rodriguez Rodriguez. 2021. "Online Solution Based on Machine Learning for IT Project Management in Software Factory Companies." Pp. 150–54 in *2021 13th International Conference on Computational Intelligence and Communication Networks (CICN)*. Institute of Electrical and Electronics Engineers Inc.

Martins, Carolina Lino, Pascale Zaraté, Adiel Teixeira de Almeida, Jônatas Araújo de Almeida, and Danielle Costa Morais. 2021. "Web-Based DSS for Resource Allocation in Higher Education." *International Journal of Decision Support System Technology (IJDSST)* 13(4):71–93. doi: 10.4018/IJDSST.2021100105.

Masilela, Lucia, and Danielle Nel. 2021. "The Role of Data and Information Security Governance in Protecting Public Sector Data and Information Assets in National Government in South Africa." *Africa's Public Service Delivery and Performance Review* 9:10. doi: https://doi.org/10.4102/apsdpr.v9i1.385.

Mavrotas, George, and Evangelos Makryvelios. 2021. "Combining Multiple Criteria Analysis, Mathematical Programming and Monte Carlo Simulation to Tackle Uncertainty in Research and Development Project Portfolio Selection: A Case Study from Greece." *European Journal of Operational Research* 291(2):794–806. doi: 10.1016/j.ejor.2020.09.051.

Miao, Meixia, Yunling Wang, Jianfeng Wang, and Xinyi Huang. 2020. "Verifiable Database Supporting Keyword Searches with Forward Security." *Computer Standards & Interfaces* 103491. doi: https://doi.org/10.1016/j.csi.2020.103491.

MINTEL. 2018. *Libro Blanco de La Sociedad de La Información y Del Conocimiento*.

Quito: Ministerio de Telecomunicaciones y de la Sociedad de la Información.

MINTEL. 2020a. *Ranking de Evaluación a Las Entidades Públicas Del Cumplimiento a La Calidad de La Implementación Del Esquema Gubernamental de Seguridad de La Información (EGSI)*.

MINTEL. 2020b. *Ranking de Evaluación a Las Entidades Públicas Del Cumplimiento de La Calidad de La Implementación Del EGSI V1.0*.

MINTEL. 2021. *Política de Nacional de Cyberseguridad*. Ecuador.

Mokhtari, G., and E. S. M. Imamzadeh. 2021. "Balancing the Portfolio of Urban and Public Projects with Distance-Dependent Coverage Facilities." *Scientia Iranica* 28(4):2374–85. doi: 10.24200/SCI.2019.52470.2730.

Montes Dorantes, Pascual Noradino, Pedro Henoc Ireta Sanchez, Jose Manuel Velarde Cantu, Ernesto Linan Garcia, and Gerardo Maximiliano Mendez. 2018. "Design and Optimization of Distribution Routes Using Evolutionary Strategy and Type-1 Singleton Neuro-Fuzzy Systems." *IEEE Latin America Transactions* 16(5):1499–1507. doi: 10.1109/TLA.2018.8408447.

Musa, Nadianatra. 2018. "A Conceptual Framework of IT Security Governance and Internal Controls." Pp. 1–4 in *2018 Cyber Resilience Conference (CRC)*. IEEE.

Mussoi, F. L. R., and R. C. G. Teive. 2021. "An Integrated Multicriteria Decision-Making Approach for Distribution System Expansion Planning." *International Journal of Intelligent Systems* 36(9):4962–89. doi: 10.1002/int.22498.

Mylnikov, Leonid. 2022. "Efficiency Management of Discrete Production Systems under the Dynamics of Project Portfolio." *Computers & Industrial Engineering* 163:107807. doi: https://doi.org/10.1016/j.cie.2021.107807.

Nartey, Clement, Eric Tutu Tchao, James Dzisi Gadze, Bright Yeboah-Akowuah, Henry Nunoo-Mensah, Dominik Welte, and Axel Sikora. 2022. "Blockchain-IoT Peer Device Storage Optimization Using an Advanced Time-Variant Multi-Objective Particle Swarm Optimization Algorithm." *EURASIP Journal on Wireless Communications and Networking* 2022(1):1–27. doi: 10.1186/s13638-021-02074-3.

Nasir, Akhyari, Ruzaini Abdullah Arshah, Mohd Rashid Ab Hamid, Syahrul Fahmy, and MohdTamizan Abu Bakar. 2020. "Information Security Culture Model for

Malaysian Organizations: A Review." *International Journal* 9(1.3):117–21. doi: 10.30534/ijatcse/2020/1691.32020.

Novoa-Hernández, P. 2015. "Optimización Evolutiva Multi-Objetivo En La Planificación de Controles a Clase En La Educación Superior Cubana." *Computación y Sistemas* 19(2):321–35.

Nyonawan, Marwandy, Suharjito, and Ditdit Nugeraha Utama. 2018. "Evaluation of Information Technology Governance in STMIK Mikroskil Using COBIT 5 Framework." Pp. 137–42 in *2018 International Conference on Information Management and Technology (ICIMTech)*. IEEE.

Okabe, Tatsuya, Yaochu Jin, and Bernhard Sendhoff. 2003. "A Critical Survey of Performance Indices for Multi-Objective Optimisation." Pp. 878–85 in *The 2003 Congress on Evolutionary Computation, 2003. CEC '03.* Vol. 2, edited by IEEE.

Olowu, Temitayo O., Hassan Jafari, Masood Moghaddami, and Arif I. Sarwat. 2020. "Multiphysics and Multiobjective Design Optimization of High-Frequency Transformers for Solid-State Transformer Applications." *IEEE Transactions on Industry Applications* 57(1):1014–23. doi: 10.1109/TIA.2020.3035129.

Ostakhov, Volodymyr, Nadiia Artykulna, and Viktor Morozov. 2018. "Analysis of Models for IT Projects Prioritization in Telecommunication Company Portfolio." Pp. 245–50 in *2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*.

Pellegrini, Alessandro, Pierangelo Di Sanzo, Beatrice Bevilacqua, Gabriella Duca, Domenico Pascarella, Roberto Palumbo, Juan Jose Ramos, Miquel Angel Piera, and Gabriella Gigante. 2020. "Simulation-Based Evolutionary Optimization of Air Traffic Management." *IEEE Access* 8:161551–70. doi: 10.1109/ACCESS.2020.3021192.

Pernul, Günther. 1994. "Database Security." Pp. 1–72 in Vol. 38, edited by M. C. B. T.-A. in C. Yovits. Elsevier.

Ramalingam, Dharmalingam, Shivasankarappa Arun, and Neelamegam Anbazhagan. 2018. "A Novel Approach for Optimizing Governance, Risk Management and Compliance for Enterprise Information Security Using DEMATEL and FoM." *Procedia Computer Science* 134:365–70. doi:

10.1016/j.procs.2018.07.197.

Ranjbar, Mojtaba, Mohammad Mahdi Nasiri, and S. Ali Torabi. 2022. “Multi-Mode Project Portfolio Selection and Scheduling in a Build-Operate-Transfer Environment.” *Expert Systems with Applications* 189:116134. doi: 10.1016/j.eswa.2021.116134.

Reis, Ana Carla Bittencourt, Guilherme Mendonça de Moraes, Wallace Sanches de Oliveira, Everaldo Silva Júnior, and Simone Boges Simão. Monteiro. 2020. “Modelo Para Priorização de Execução de Projetos de TI Em Uma Instituição Financeira.” *Revista Iberica de Sistemas e Tecnologias de Informacao* (E27):319–32.

Riquelme, Nery, Christian Von Lücken, and Benjamin Baran. 2015. “Performance Metrics in Multi-Objective Optimization.” Pp. 1--11 in *2015 Latin American computing conference (CLEI)*, edited by IEEE.

Rivera, Gilberto, Rogelio Florencia, Mario Guerrero, Raúl Porras, and J. Patricia Sánchez-Solís. 2021. “Online Multi-Criteria Portfolio Analysis through Compromise Programming Models Built on the Underlying Principles of Fuzzy Outranking.” *Information Sciences* 580:734–55.

Rodríguez-Molina, Alejandro, Miguel G. Villarreal-Cervantes, Efrén Mezura-Montes, and Mario Aldape-Pérez. 2021. “Adaptive Controller Tuning Method Based on Online Multiobjective Optimization: A Case Study of the Four-Bar Mechanism.” *IEEE Transactions on Cybernetics* 51(3):1272–85. doi: 10.1109/TCYB.2019.2903491.

Saiya, Angelia Alberthina, and Arry Akhmad Arman. 2018. “Indonesian Enterprise Architecture Framework: A Platform for Integrated and Connected Government.” Pp. 1–6 in *2018 International Conference on ICT for Smart Society (ICISS)*. IEEE.

Saiz, Miguel, Marisa A. Lostumbo, Angel A. Juan, and David Lopez-Lopez. 2022. “A Clustering-Based Review on Project Portfolio Optimization Methods.” *International Transactions in Operational Research* 29:172–99. doi: 10.1111/itor.12933.

Sarker, Ruhul Amin, Kyle Robert Harrison, and Saber M. Elsayed. 2022.

"Evolutionary Approaches for Project Portfolio Optimization: An Overview." *Evolutionary and Memetic Computing for Project Portfolio Selection and Scheduling* 9–35.

Sawczuk da Silva, Alexandre, Hui Ma, Yi Mei, and Mengjie Zhang. 2018. "A Hybrid Memetic Approach for Fully Automated Multi-Objective Web Service Composition." Pp. 26–33 in *2018 IEEE international conference on web services (ICWS)*. IEEE.

Schatz, Daniel, and Rabih Bashroush. 2017. "Economic Valuation for Information Security Investment: A Systematic Literature Review." *Information Systems Frontiers* 19(5):1205–28. doi: 10.1007/s10796-016-9648-8.

Skrodelis, Heinrihs Kristians, Julija Strebko, and Andrejs Romanovs. 2020. "The Information System Security Governance Tasks in Small and Medium Enterprises." Pp. 1–4 in *2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, edited by IEEE.

Song, Yongqiang, Yongjun Shen, Guidong Zhang, and Yuming Hu. 2016. "The Information Security Risk Assessment Model Based on GA-BP." Pp. 119–22 in *2016 7th IEEE international conference on software engineering and service science (ICSESS)*.

Sonmez, F. O., and B. G. Kilic. 2020. "A Decision Support System for Optimal Selection of Enterprise Information Security Preventative Actions." *IEEE Transactions on Network and Service Management*. doi: 10.1109/TNSM.2020.3044865.

Sönmez, Ferda Özdemir. 2019. "A Conceptual Model for a Metric Based Framework for the Monitoring of Information Security Tasks' Efficiency." Pp. 181–88 in *Procedia Computer Science*. Vol. 160.

Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review." *International Journal of Information Management* 36(2):215–25. doi: https://doi.org/10.1016/j.ijinfomgt.2015.11.009.

Stepanov, LV, AS Koltsov, AV Parinov, and AS Dubrovin. 2019. "Mathematical

Modeling Method Based on Genetic Algorithm and Its Applications." P. 12082 in *Journal of Physics: Conference Series*. Vol. 1203.

Suárez, Enrique J. Carmona, and Severino Fernández Galán. 2021. *Fundamentos de Computación Evolutiva*. Marcombo.

Szczepaniuk, Edyta Karolina, Hubert Szczepaniuk, Tomasz Rokicki, and Bogdan Klepacki. 2020. "Information Security Assessment in Public Administration." *Computers & Security* 90:101709. doi: 10.1016/j.cose.2019.101709.

Tavakoli-Someh, Sanaz, and Mohammad Hossein Rezvani. 2019. "Utilization-Aware Virtual Network Function Placement Using NSGA-II Evolutionary Computing." Pp. 510–14 in *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*. IEEE.

Tawfiq, Aiman Abd Elkader, Mohamed Osama Abed El-Raouf, Mohamed I. Mosaad, Amal Farouk Abdel Gawad, and Mohamed Abd Elfatah Farahat. 2021. "Optimal Reliability Study of Grid-Connected PV Systems Using Evolutionary Computing Techniques." *IEEE Access* 9:42125–39. doi: 10.1109/ACCESS.2021.3064906.

Toapanta, Moisés, Enrique Mafla, and José Orizaga. 2018. "Conceptual Model for Identity Management to Mitigate the Database Security of the Registry Civil of Ecuador." *Materials Today: Proceedings* 5(1, Part 1):636–41. doi: https://doi.org/10.1016/j.matpr.2017.11.127.

Toapanta, Segundo Moisés, Alexander Jimenez, and Luis Enrique Mafla. 2019. "An Approach of National and International Cybersecurity Laws and Standards to Mitigate Information Risks in Public Organizations of Ecuador." Pp. 61–66 in *Proceedings of the 2019 2nd International Conference on Education Technology Management*.

Torquato, Matheus F., Germán Martínez-Ayuso, Ashraf A. Fahmy, and Johann Sienz. 2021. "Multi-Objective Optimization of Electric Arc Furnace Using the Non-Dominated Sorting Genetic Algorithm II." *IEEE Access* 9:149715–31. doi: 10.1109/ACCESS.2021.3125519.

Trivedi, Devanshu, Pavol Zavarsky, and Sergey Butakov. 2016. "Enhancing Relational Database Security by Metadata Segregation." *Procedia Computer Science* 94:453–58. doi: https://doi.org/10.1016/j.procs.2016.08.070.

Tselios, D., and P. Ipsilandis. 2018. “Telecommunication Projects Portfolio Scheduling Using the IFM Approach.” Pp. 1–4 in *2017 25th Telecommunications Forum, TELFOR 2017 - Proceedings*. Vols. 2017-Janua.

Vorobioff, Juan, Santiago Cerrotta, Nicolas Eneas Morel, and Ariel Amadio. 2022. “Inteligencia Artificial y Redes Neuronales. Fundamentos, Ejercicios y Aplicaciones Con Python y Matlab.”

Wang, Ruili, and Wanting Ji. 2020. “Computational Intelligence for Information Security: A Survey.” *IEEE Transactions on Emerging Topics in Computational Intelligence* 4(5):616–29. doi: 10.1109/TETCI.2019.2923426.

Wu, Liang-Hong, Liangchuan Wu, Jianming Shi, and Yang-Tai Chou. 2021. “Project Portfolio Selection Considering Uncertainty: Stochastic Dominance-Based Fuzzy Ranking.” *International Journal of Fuzzy Systems* 23(7):2048–66. doi: 10.1007/s40815-021-01069-y.

Yan, Qi, Jinyan Wang, Songfeng Liu, and De Li. 2021. “Differentially Private Decision Tree Based on Pearson’s Correlation Coefficient.” Pp. 77–86 in *2021 11th International Conference on Information Science and Technology (ICIST)*.

Yang, Xu, Juan Zou, Shengxiang Yang, Jinhua Zheng, and Yuan Liu. 2021. “A Fuzzy Decision Variables Framework for Large-Scale Multiobjective Optimization.” *IEEE Transactions on Evolutionary Computation* 1–1. doi: 10.1109/TEVC.2021.3118593.

Yasin, Muhammad, Arry Akhmad Arman, Ian Joseph M. Edward, and Wervyan Shalannanda. 2020. “Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ).” Pp. 1–5 in *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*.

Yastrub, Maksym, and Svetlana Kredentsar. 2018. “Enterprise Architecture as a Driver of Transformation in Air Traffic Management.” Pp. 162–65 in *2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*. IEEE.

Yilmaz, Fatih, and Florian Matthes. 2021. “Application of Interorganizational

Business Capability Maps in Different Forms of Horizontal Enterprise Architecture Collaboration." Pp. 82–91 in *2021 IEEE 23rd Conference on Business Informatics (CBI)*. Vol. 1. IEEE.

Zaydi, Mounia, and Bouchaib Nassereddine. 2018. "A New Approach of Information System Security Governance: A Proposition of the Continuous Improvement Process Model of Information System Security Risk Management: 4D-ISS." Pp. 112–18 in *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE.

Zegzhda, Peter D., VG Anisimov, AF Suprun, EG Anisimov, TN Saurenko, and VP Los. 2020. "A Model of Optimal Complexification of Measures Providing Information Security." *Automatic Control and Computer Sciences* 54(8):930–36. doi: 10.3103/S0146411620080374.

Zeng, Wen, and Maciej Koutny. 2019. "Modelling and Analysis of Corporate Efficiency and Productivity Loss Associated with Enterprise Information Security Technologies." *Journal of Information Security and Applications* 49:102385. doi: 10.1016/j.jisa.2019.102385.

Zolfaghari, Samaneh, and Seyed Meysam Mousavi. 2021. "A Novel Mathematical Programming Model for Multi-Mode Project Portfolio Selection and Scheduling with Flexible Resources and Due Dates under Interval-Valued Fuzzy Random Uncertainty." *Expert Systems with Applications* 182:115207. doi: 10.1016/j.eswa.2021.115207.

ANEXOS

Anexo 1: Ranking de evaluación a las entidades públicas del cumplimiento a la calidad de la implementación del EGSI V1.0

RANKING		SIGLAS	NOMBRE DE LA INSTITUCION	CALIFICACIÓN
1	BUENA	SRI	Servicio de Rentas Internas	100,00%
2		CNT EP	Corporación Nacional de Telecomunicaciones	100,00%
3		BDE	Banco de Desarrollo del Ecuador B.P.	99,80%
4		PAM	PETROAMAZONAS EP	99,67%
5		ASTINAVE EP	Astilleros Navales Ecuatorianos	98,67%
6		DIGERCIC	Dirección General de Registro Civil Identificación y Cedulación	98,00%
7		BCE	Banco Central del Ecuador	97,33%
8		CFN	Corporación Financiera Nacional	97,16%
9		PN	Policía Nacional	96,00%
10		PETROECUADOR	Empresa Pública de Hidrocarburos del Ecuador	95,00%
11		MDN	Ministerio de Defensa Nacional	94,33%
12		DINARDAP	Dirección Nacional de Registro de Datos Públicos	94,17%
13		SERCOP	Servicio Nacional de Contratación Pública	93,67%
14		MIES	Ministerio de Inclusión, Económica y Social	93,00%
15		CNII	Consejo Nacional para la Igualdad Intergeneracional	92,33%
16		INEVAL	Instituto Nacional de Evaluación Educativa	91,50%
17		ARCONEL	Agencia de Regulación y Control de Electricidad	91,17%
18		ENAMI	Empresa Nacional Minera del Ecuador	90,50%
19	REGULAR	MREMH	Ministerio de Relaciones Exteriores y Movilidad Humana	88,94%
20		MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información	88,50%
21		PR	Presidencia de la República	88,50%
22		SNGRE	Servicio Nacional de Gestión de Riesgos y Emergencias	87,17%
23		CELEC EP	Corporación Eléctrica del Ecuador	88,17%
24		MSP	Ministerio de Salud Pública	87,10%
25		MT	Ministerio de Turismo	85,67%
26		FEEP	Ferrocarriles del Ecuador Empresa Pública	85.33%
27		IFTH	Instituto de Fomento al Talento Humano	84,67%
28		YACHAY	Empresa Pública YACHAY EP	84,50%
29		MIDUVI	Ministerio de Desarrollo Urbano y Vivienda	84,00%
30		CONADIS	Consejo Nacional de Discapacidades	83,83%
31		STPE	Secretaría Técnica de Planificación	82,33%
32		SENESCYT	Secretaría de Educación Superior, Ciencia y Tecnología	82,08%
33		INEC	Instituto Nacional de Estadísticas y Censos	82,00%
34		MJDHC	Ministerio de Justicia, Derechos Humanos y Cultos	81,90%
35		EEEP	Ecuador Estratégico EP	81,67%

36	EEQ	Empresa Eléctrica de Quito	80,83%
37	CNEL	Corporación Nacional de Electricidad	80,67%
38	SECOB	Servicio de Contratación de Obras	80,67%
39	APM	Autoridad Portuaria de Manta	80,33%
40	MINEDUC	Ministerio de Educación	80,20%
41	CDE EP	Correos del Ecuador Empresa Pública	80,00%
42	ARCH	Agencia de Regulación y Control Hidrocarburífero	80,00%
43	MDT	Ministerio de Trabajo	79,43%
44	ARCSA	Agencia de Regulación y Control Vigilancia Sanitario	79,33%
45	INMOBILIAR	Servicio de Gestión Inmobiliaria del Sector Público	79,33%
46	FLOPEC	Empresa Pública Flota Petrolera Ecuatoriana	79,17%
47	SENAGUA	Secretaría del Agua	78,50%
48	TAME	Empresa Pública Tame - Línea Aérea del Ecuador	77,33%
49	MTOP	Ministerio de Transporte y Obras Públicas	76,83%
50	DGAC	Dirección General de Aviación Civil	75,80%
51	AGROCALIDAD	Agencia Ecuatoriana de Aseguramiento de la Calidad del Agro	75,61%
52	INPC	Instituto Nacional de Patrimonio y Cultura	74,83%
53	IEPS	Instituto Nacional de Economía Popular y Solidaria	73,50%
54	COSEDE	Corporación de Seguro de Depósitos, Fondo de Liquidez y Fondo de Seguros Privados	73,00%
55	APG	Autoridad Portuaria de Guayaquil	72,33%
56	INAE	Instituto Antártico Ecuatoriano	72,17%
57	CONAFIPS	Corporación Nacional de Finanzas Populares y Solidaria	71,17%
58	IGM	Instituto Geográfico Militar	70,30%
59	CONASA	Consejo Nacional de la Salud	70,17%
60	MDG	Ministerio de Gobierno	69,50%
61	MEF	Ministerio de Economía y Finanzas	68,83%
62	SBEP	Santa Bárbara Empresa Pública	68,50%
63	SD	Secretaría del Deporte	68,27%
64	SAE	Servicio de Acreditación Ecuatoriana	66,83%
65	SENADI	Servicio Nacional de Derechos Intelectuales	66,00%
66	VPR	Vicepresidencia de la República	65,50%
67	INIAP	Instituto Nacional de Investigaciones Agropecuarias	65,17%
68	INP	Instituto Nacional de Pesca	65,00%
69	ABG	Agencia de Regulación y Control de la Bioseguridad y Cuarentena	64,17%
70	INAMHI	Instituto Nacional de Meteorología e Hidrología	63,00%
71	STPTV	Secretaría Técnica Plan Toda una Vida	62,50%
72	CACES	Consejo de Aseguramiento de la Calidad de la Educación Superior	62,17%

73		INEN	Servicio Ecuatoriano de Normalización	61,50%
74		ARCP	Agencia de Regulación y Control Postal	61,17%
75		ANT	Agencia Nacional de Tránsito	60,33%
76	MALA	MAE	Ministerio del Ambiente	59,30%
77		MCYP	Ministerio de Cultura y Patrimonio	53,17%
78		SETEC	Secretaría Técnica del Sistema Nacional de Cualificaciones Profesionales	52,33%
79		CTE	Comisión de Tránsito del Ecuador	47,83%
80		SECAP	Servicio Ecuatoriano de Capacitación Profesional	31,17%
81		ICCA	Instituto de Cine y Creación Audiovisual	30,30%
82		INDOT	Instituto Nacional de Donación y Trasplante de Órganos, Tejidos y Células	30,00%

Fuente: MINTEL (2020). Fecha de Corte: septiembre 2020.

Anexo 2: Calculo del %CMSI para los proyectos estratégicos planificados

No.	Tipo de proyecto	Origen incumplimiento	Valoración origen incumplimiento	Clasificación proyecto PDS	Relación ganancia / esfuerzo	Clasificación Tiempo ejecución	Tiempo ejecución (días)	Valoración Tiempo ejecución	Tipo de costo	Costo (USD)	Recursos	Valoración Recursos	Promedio valoraciones	%CMSI
1	Técnico	AU	50.00	PST	50.00	Corto	60.00	100.00	Medio	1,912.00	Externos	50.00	62.50	2.93%
2	Regulatorio	ER	25.00	PSA	75.00	Largo	220.00	50.00	Alto	1,204.00	Internos	100.00	62.50	2.93%
3	Regulatorio	AU	50.00	PFO	100.00	Corto	45.00	100.00	Alto	3,253.00	Internos	100.00	87.50	4.10%
4	Técnico	IS	100.00	PPE	25.00	Largo	260.00	50.00	Medio	3,006.00	Ambos	75.00	62.50	2.93%
5	Técnico	ER	25.00	PSE	90.00	Corto	80.00	100.00	Medio	2,828.00	Ambos	75.00	72.50	3.39%
6	Técnico	ER	25.00	PFO	100.00	Medio	120.00	75.00	Medio	2,143.00	Ambos	75.00	68.75	3.22%
7	Técnico	ES	75.00	PSA	75.00	Largo	200.00	50.00	Alto	1,839.00	Externos	50.00	62.50	2.93%
8	Organizativo	ES	75.00	PSA	75.00	Largo	340.00	50.00	Bajo	5,467.00	Ambos	75.00	68.75	3.22%
9	Organizativo	AU	50.00	PSE	90.00	Corto	60.00	100.00	Bajo	1,712.00	Ambos	75.00	78.75	3.69%
10	Técnico	AU	50.00	PPE	25.00	Largo	240.00	50.00	Alto	5,837.00	Internos	100.00	56.25	2.63%
11	Técnico	ES	75.00	PSE	90.00	Largo	320.00	50.00	Bajo	4,456.00	Externos	50.00	66.25	3.10%
12	Técnico	IS	100.00	PSE	90.00	Medio	160.00	75.00	Alto	1,260.00	Externos	50.00	78.75	3.69%
13	Técnico	ES	75.00	PPE	25.00	Largo	280.00	50.00	Alto	6,489.00	Internos	100.00	62.50	2.93%
14	Técnico	ES	75.00	PFO	100.00	Corto	90.00	100.00	Medio	7,536.00	Externos	50.00	81.25	3.80%
15	Organizativo	IS	100.00	PSE	90.00	Corto	45.00	100.00	Bajo	9,583.00	Ambos	75.00	91.25	4.27%
16	Técnico	IS	100.00	PPE	25.00	Medio	160.00	75.00	Alto	9,812.00	Ambos	75.00	68.75	3.22%
17	Técnico	IS	100.00	PSE	90.00	Medio	140.00	75.00	Alto	14,280.00	Internos	100.00	91.25	4.27%
18	Técnico	AU	50.00	PPE	25.00	Largo	200.00	50.00	Bajo	6,435.00	Ambos	75.00	50.00	2.34%
19	Técnico	ER	25.00	PSA	75.00	Largo	210.00	50.00	Alto	9,258.00	Externos	50.00	50.00	2.34%
20	Técnico	ES	75.00	PPE	25.00	Corto	80.00	100.00	Bajo	14,929.00	Internos	100.00	75.00	3.51%
21	Técnico	ES	75.00	PSA	75.00	Medio	140.00	75.00	Alto	12,874.00	Externos	50.00	68.75	3.22%
22	Técnico	ES	75.00	PST	50.00	Largo	220.00	50.00	Medio	9,612.00	Externos	50.00	56.25	2.63%
23	Regulatorio	ES	75.00	PSE	90.00	Medio	100.00	75.00	Alto	13,360.00	Ambos	75.00	78.75	3.69%
24	Técnico	ER	25.00	PFO	100.00	Largo	320.00	50.00	Alto	10,558.00	Internos	100.00	68.75	3.22%
25	Técnico	AU	50.00	PPE	25.00	Largo	300.00	50.00	Medio	6,107.00	Internos	100.00	56.25	2.63%
26	Organizativo	AU	50.00	PFO	100.00	Largo	340.00	50.00	Bajo	8,616.00	Internos	100.00	75.00	3.51%
27	Organizativo	AU	50.00	PFO	100.00	Medio	120.00	75.00	Bajo	12,925.00	Ambos	75.00	75.00	3.51%
28	Técnico	IS	100.00	PFO	100.00	Corto	70.00	100.00	Medio	37,299.00	Internos	100.00	100.00	4.68%
29	Técnico	AU	50.00	PSE	90.00	Corto	80.00	100.00	Medio	33,211.00	Internos	100.00	85.00	3.98%
30	Organizativo	AU	50.00	PST	50.00	Corto	90.00	100.00	Bajo	25,190.00	Internos	100.00	75.00	3.51%
										282,991.00			2,136.25	100.00%

Anexo 3: Programa base en Python para implementar modelo de optimización

```
# Programa Python para implementar el Modelo de optimización para la gestión de proyectos estratégicos
# para mejorar la seguridad de la información de una Organización Pública en Ecuador.
# Calcula aleatoriamente escenarios de proyectos
# Autor: Richard Romero Izurieta
# Tesis doctoral para optar por el título Doctor en Ciencias con mención en
#  Estadística Matemática Aplicada - Universidad Nacional de Tumbes, Perú.

!pip install deap
```

```
import random
import numpy as np
import matplotlib.pyplot as plt
from deap import base
from deap import creator
from deap import tools
from deap import algorithms

random.seed(42) # ajustamos aquí la semilla para que todos tengamos los mismos valores
CMSI_INF, CMSI_SUP = 1, 100
PRESUPUESTO, OBJETIVO_CMSI = 200000, 80
PORC_PCOSTO_BAJO, PORC_PCOSTO_MEDIO, PORC_PCOSTO_ALTO = 0.40, 0.50, 0.10
TAM_CONJUNTO = 30

#Creamos de forma aleatoria conjunto de costos de proyectos
PCOSTO_BAJO = np.array(random.sample(range(1000, 6000), round(TAM_CONJUNTO*PORC_PCOSTO_BAJO)))
PCOSTO_MEDIO = np.array(random.sample(range(6001, 15000), round(TAM_CONJUNTO*PORC_PCOSTO_MEDIO)))
PCOSTO_ALTO = np.array(random.sample(range(15001, 50000), round(TAM_CONJUNTO*PORC_PCOSTO_ALTO)))
PCOSTO = PCOSTO_BAJO.tolist()
PCOSTO.extend(PCOSTO_MEDIO.tolist())
PCOSTO.extend(PCOSTO_ALTO.tolist())
PCOSTO = np.array(PCOSTO)
print("PCOSTO", PCOSTO)

MAX_CMSI = 100
MAX_COSTO = sum(PCOSTO)
print(MAX_COSTO)
#SUMA_CGSI = sum(CONJUNTO_CGSI)
#CONJUNTO_CGSI = CONJUNTO_CGSI/SUMA_CGSI*100

#Creamos de forma aleatoria conjunto de valoración de origen de proyectos
# ER=25%, AU=50%, ES=75%, IS=100%
PESO_ORIGEN = [25, 50, 75, 100]
PORIGEN = np.random.choice(PESO_ORIGEN, TAM_CONJUNTO)
print("PORIGEN", PORIGEN)

#Creamos de forma aleatoria conjunto de valoración ganancia/esfuerzo de proyectos
# PPE=25%, PST=50%, PSA=75%, PSE=90%, PFO=100%
PESO_GANANCIA = [25, 50, 75, 90, 100]
PGANANCIA = np.random.choice(PESO_GANANCIA, TAM_CONJUNTO)
print("PGANANCIA", PGANANCIA)

#Creamos de forma aleatoria conjunto de valoración por tiempo de ejecución de proyectos
# LARGO=50%, MEDIO=75%, CORTO=100%
PESO_TIEMPO = [50, 75, 100]
PTIEMPO = np.random.choice(PESO_TIEMPO, TAM_CONJUNTO)
print("PTIEMPO", PTIEMPO)
```

```
#Creamos de forma aleatoria conjunto de valoración por tipo de recursos de proyectos
# EXTERNOS=25%, AMBOS=50%, INTERNOS=100%
PESO_RECURSO = [50, 75, 100]
PRECURSO = np.random.choice(PESO_RECURSO, TAM_CONJUNTO)
print("PRECURSO", PRECURSO)

#Calculo el %CMSI
#PCMSI = np.array(PORIGEN, PGANANCIA, PTIEMPO, PRECURSO)
LCMSI = []
LCMSI.append(PORIGEN.tolist())
LCMSI.append(PGANANCIA.tolist())
LCMSI.append(PTIEMPO.tolist())
LCMSI.append(PRECURSO.tolist())
MCMSI = np.array(LCMSI)
print("LCMSI", LCMSI)
print("MCMSI", MCMSI)
MCMSI_PROMEDIO = np.mean(MCMSI, 0)
SUMA_MCMSI_PROMEDIO = sum(MCMSI_PROMEDIO)
print("MCMSI_PROMEDIO", MCMSI_PROMEDIO)
print("SUMA_MCMSI_PROMEDIO", SUMA_MCMSI_PROMEDIO)
PCMSI = (MCMSI_PROMEDIO[:]/SUMA_MCMSI_PROMEDIO)*100
SUMA_PCMSI = sum(PCMSI)
print("PCMSI", PCMSI)
print("SUMA_PCMSI", SUMA_PCMSI)

creator.create("FitnessMulti", base.Fitness, weights=(-1.0, 1.0))
creator.create("Individual", list, fitness=creator.FitnessMulti)
toolbox = base.Toolbox()
def crea_individuo(size):
    return [random.randint(0, 1) for i in range(size)]
toolbox.register("attr", crea_individuo, TAM_CONJUNTO)

#print(toolbox.attr())

toolbox.register("individual", tools.initIterate, creator.Individual, toolbox.attr)
toolbox.register("population", tools.initRepeat, list, toolbox.individual)

ind = toolbox. individual() # creamos un individuo aleatorio
#print(ind)
#print(ind.fitness.values) # en fitness.values se guardará el fitness

#poblacion = []
def funcion_objetivo(individuo, objetivo_cmsi, presupuesto):
    subconjunto = PCMSI[np.array(individuo) == 1]
    suma_subconjunto = np.sum(subconjunto)
    diferencia = objetivo_cmsi - suma_subconjunto
    subconjunto2 = PCOSTO[np.array(individuo) == 1]
    suma_subconjunto2 = np.sum(subconjunto2)
    diferencia2 = presupuesto - suma_subconjunto2
    n_elementos = sum(individuo)
    if diferencia > 0: # nos falta
        return 10000000, -10000000 # pena de muerte
    if diferencia2 > 0: # nos falta
        return 10000000, -10000000 # pena de muerte
    #if n_elementos == 0: # no se selecciona ninguna elemento
        #return -10000, -10000 # pena de muerte
    #poblacion.append(str(individuo) + '\n')
    return suma_subconjunto2, suma_subconjunto
```

```
toolbox.register("mate", tools.cxTwoPoint)
toolbox.register("mutate", tools.mutFlipBit, indpb=0.05)
toolbox.register("select", tools.selNSGA2)
toolbox.register("evaluate", funcion_objetivo, objetivo_cmsi=OBJETIVO_CMSI, presupuesto=PRESUPUESTO)

def plot_frente(pareto):
    lista_fitness1 = list()
    lista_fitness2 = list()
    for ind in pareto: # recorremos los elementos del Pareto
        lista_fitness1.append(ind.fitness.values[0])
        lista_fitness2.append(ind.fitness.values[1])
    plt.scatter(lista_fitness1, lista_fitness2, marker="+", color="b", s=50)
    plt.xlabel("Costo (USD)")
    plt.ylabel("% CMSI Planificado")
    plt.grid(True)
    plt.xlim([PRESUPUESTO, MAX_COSTO+1])
    plt.ylim([OBJETIVO_CMSI, MAX_CMSI+5])
    plt.legend(["Frente de Pareto"], loc="upper right")
    plt.savefig("Pareto_conjunto.eps", dpi = 300)

def main():
    CXPB, MUTPB, NGEN = 0.7, 0.3, 200
    MU, LAMBDA = 300, 300
    pop = toolbox.population(MU)
    stats = tools.Statistics(lambda ind: ind.fitness.values)
    stats.register("avg", np.mean)
    stats.register("std", np.std)
    stats.register("min", np.min)
    stats.register("max", np.max)
    logbook = tools.Logbook()
    pareto = tools.ParetoFront()
    pop, logbook = algorithms.eaMuPlusLambda(pop , toolbox , mu=MU, lambda_=LAMBDA, cxpb=CXPB,
         mutpb=MUTPB, ngen=NGEN, stats=stats, halloffame=pareto,  verbose=True)
    res_individuos = open("individuos_sensores_multi.txt", "a")
    res_fitness = open("fitness_sensores_multi.txt", "a")
    for ide, ind in enumerate(pareto):
        res_individuos.write(str(ide))
        res_individuos.write(",")
        res_individuos.write(str(list(ind)))
        res_individuos.write("\n")
        res_fitness.write(str(ide))
        res_fitness.write(",")
        res_fitness.write(str(ind.fitness.values[0]))
        res_fitness.write(",")
        res_fitness.write(str(ind.fitness.values[1]))
        res_fitness.write("\n")
    res_fitness.close()
    res_individuos.close()
    return pop, logbook, pareto

if __name__ == "__main__":
    pop, log, pareto = main()
    for item in pop:
      subconjunto = PCMSI[np.array(item) == 1]
      suma_subconjunto = round(np.sum(subconjunto),2)
      subconjunto2 = PCOSTO[np.array(item) == 1]
      suma_subconjunto2 = np.sum(subconjunto2)
      n_elementos = sum(item)
      print(str(item)  + " " + str(n_elementos) + " " + str(suma_subconjunto)  + " " + str(suma_subconjunto2))
    print("PCMSI", PCMSI)
    print("PCOSTO", PCOSTO)
    print("Valor máximo que puede tener SUMA_CMSI", round(sum(PCMSI)),2)
    print("Valor máximo que puede tener SUMA_COSTO", sum(PCOSTO))
    print("OBJETIVO_COSTO", PRESUPUESTO)
    print("OBJETIVO_CMSI", OBJETIVO_CMSI)
    plot_frente(pareto)
```

Anexo 4: Corrida de programa en Python del modelo de optimización

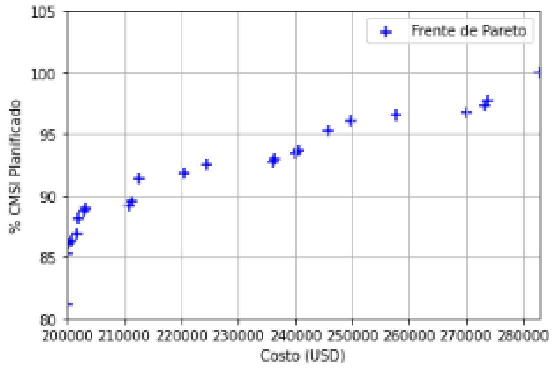
```
Looking in indexes: https://pypi.org/simple, https://us-python.pkg.dev/colab-wheels/public/simple/
Collecting deap
  Downloading deap-1.3.3-cp37-cp37m-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (139 kB)
     |████████████████████████████████| 139 kB 5.1 MB/s
Requirement already satisfied: numpy in /usr/local/lib/python3.7/dist-packages (from deap) (1.21.6)
Installing collected packages: deap
Successfully installed deap-1.3.3
PCOSTO [ 1912  1204  3253  3006  2828  2143  1839  5467  1712  5837  4456  1260
  6489  7536  9583  9812 14280  6435  9258 14929 12874  9612 13360 10558
  6107  8616 12925 37299 33211 25190]
282991
PCMSI [2.92568754 2.92568754 4.09596255 2.92568754 3.39379754 3.21825629
 2.92568754 3.21825629 3.6863663  2.63311878 3.10122879 3.6863663
 2.92568754 3.8033938  4.2715038  3.21825629 4.2715038  2.34055003
 2.34055003 3.51082504 3.21825629 2.63311878 3.6863663  3.21825629
 2.63311878 3.51082504 3.51082504 4.68110006 3.97893505 3.51082504]
SUMA_PCMSI 100.00000000000001
gen     nevals  avg     std     min     max
0       300     0       1e+07   -1e+07  1e+07
1       300     0       1e+07   -1e+07  1e+07
2       300     0       1e+07   -1e+07  1e+07
3       300     0       1e+07   -1e+07  1e+07
4       300     0       1e+07   -1e+07  1e+07
5       300     0       1e+07   -1e+07  1e+07
6       300     0       1e+07   -1e+07  1e+07
7       300     0       1e+07   -1e+07  1e+07
8       300     0       1e+07   -1e+07  1e+07
9       300     0       1e+07   -1e+07  1e+07
10      300     370.914 9.98332e+06     -1e+07  1e+07
11      300     370.914 9.98332e+06     -1e+07  1e+07
12      300     370.914 9.98332e+06     -1e+07  1e+07
13      300     370.914 9.98332e+06     -1e+07  1e+07
14      300     769.172 9.96662e+06     -1e+07  1e+07
15      300     769.172 9.96662e+06     -1e+07  1e+07
16      300     769.172 9.96662e+06     -1e+07  1e+07
17      300     769.172 9.96662e+06     -1e+07  1e+07
18      300     1535.99 9.93313e+06     -1e+07  1e+07
19      300     1931.88 9.91634e+06     -1e+07  1e+07
20      300     1931.88 9.91634e+06     -1e+07  1e+07
21      300     2325.78 9.89952e+06     -1e+07  1e+07
22      300     2325.78 9.89952e+06     -1e+07  1e+07
23      300     2731.28 9.88268e+06     -1e+07  1e+07
24      300     2731.28 9.88268e+06     -1e+07  1e+07
25      300     3109.63 9.8658e+06      -1e+07  1e+07
26      300     3109.63 9.8658e+06      -1e+07  1e+07
27      300     3505.53 9.8489e+06      -1e+07  1e+07
28      300     3505.53 9.8489e+06      -1e+07  1e+07
29      300     4263.41 9.815e+06       -1e+07  1e+07
30      300     4654.12 9.79801e+06     -1e+07  1e+07
31      300     7429.56 9.67824e+06     -1e+07  1e+07
32      300     9371.58 9.59177e+06     -1e+07  1e+07
33      300     11310.5 9.50452e+06     -1e+07  1e+07
34      300     17229   9.23781e+06     -1e+07  1e+07
35      300     20202.7 9.09236e+06     -1e+07  1e+07
36      300     28404.7 8.69899e+06     -1e+07  1e+07
37      300     41652.6 8.02131e+06     -1e+07  1e+07
38      300     65103.5 6.68414e+06     -1e+07  1e+07
39      300     107479  3.00232e+06     -1e+07  1e+07
40      300     116831  117289          80.0468 275529
41      300     116730  117380          80.0468 278535
42      300     116899  117770          80.0468 281787
43      300     118742  119605          80.0468 281787
44      300     118939  119996          80.0468 282991
45      300     118198  119449          80.2224 282991
46      300     121846  123006          80.2224 282991
47      300     121674  122817          80.2224 282991
48      300     126647  127378          81.1001 282991
49      300     129008  129747          81.1001 282991
50      300     131894  132679          81.1001 282991
51      300     135883  136673          81.1001 282991
52      300     137368  138149          81.1001 282991
53      300     136955  137836          81.1001 282991
54      300     136877  137767          81.1001 282991
55      300     136799  137697          81.1001 282991
56      300     136669  137596          81.1001 282991
57      300     136798  137697          81.1001 282991
58      300     136532  137491          81.1001 282991
59      300     136401  137389          81.1001 282991
60      300     136002  137078          81.1001 282991
```

61	300	136002	137078	81.1001	282991
62	300	135733	136869	81.1001	282991
63	300	135458	136655	81.1001	282991
64	300	135458	136655	81.1001	282991
65	300	136108	137169	81.1001	282991
66	300	136443	137445	81.1001	282991
67	300	136443	137445	81.1001	282991
68	300	136325	137350	81.1001	282991
69	300	136190	137245	81.1001	282991
70	300	136190	137245	81.1001	282991
71	300	136598	137559	81.1001	282991
72	300	136598	137559	81.1001	282991
73	300	136461	137454	81.1001	282991
74	300	136339	137357	81.1001	282991
75	300	136339	137357	81.1001	282991
76	300	136339	137357	81.1001	282991
77	300	137350	138151	81.1001	282991
78	300	137350	138151	81.1001	282991
79	300	137350	138151	81.1001	282991
80	300	137350	138151	81.1001	282991
81	300	137350	138151	81.1001	282991
82	300	137350	138151	81.1001	282991
83	300	137216	138049	81.1001	282991
84	300	137216	138049	81.1001	282991
85	300	137216	138049	81.1001	282991
86	300	137216	138049	81.1001	282991
87	300	137216	138049	81.1001	282991
88	300	137216	138049	81.1001	282991
89	300	137216	138049	81.1001	282991
90	300	137216	138049	81.1001	282991
91	300	137216	138049	81.1001	282991
92	300	137216	138049	81.1001	282991
93	300	137083	137947	81.1001	282991
94	300	136950	137844	81.1001	282991
95	300	136950	137844	81.1001	282991
96	300	136950	137844	81.1001	282991
97	300	136950	137844	81.1001	282991
98	300	136950	137844	81.1001	282991
99	300	136950	137844	81.1001	282991
100	300	136950	137844	81.1001	282991
101	300	136950	137844	81.1001	282991
102	300	136950	137844	81.1001	282991
103	300	136950	137844	81.1001	282991
104	300	136950	137844	81.1001	282991
105	300	136950	137844	81.1001	282991
106	300	136950	137844	81.1001	282991
107	300	137637	138364	81.1001	282991
108	300	137499	138260	81.1001	282991
109	300	137499	138260	81.1001	282991
110	300	137499	138260	81.1001	282991
111	300	137499	138260	81.1001	282991
112	300	137499	138260	81.1001	282991
113	300	137499	138260	81.1001	282991
114	300	137499	138260	81.1001	282991
115	300	137499	138260	81.1001	282991
116	300	137499	138260	81.1001	282991
117	300	137499	138260	81.1001	282991
118	300	137499	138260	81.1001	282991
119	300	137499	138260	81.1001	282991
120	300	137499	138260	81.1001	282991
121	300	137499	138260	81.1001	282991
122	300	137499	138260	81.1001	282991
123	300	137499	138260	81.1001	282991
124	300	137499	138260	81.1001	282991
125	300	137499	138260	81.1001	282991
126	300	137365	138158	81.1001	282991
127	300	137365	138158	81.1001	282991
128	300	137365	138158	81.1001	282991
129	300	137365	138158	81.1001	282991
130	300	137231	138056	81.1001	282991
131	300	137231	138056	81.1001	282991
132	300	137231	138056	81.1001	282991
133	300	137231	138056	81.1001	282991
134	300	137231	138056	81.1001	282991
135	300	137370	138160	81.1001	282991
136	300	137370	138160	81.1001	282991
137	300	137370	138160	81.1001	282991
138	300	137370	138160	81.1001	282991
139	300	137370	138160	81.1001	282991
140	300	137231	138056	81.1001	282991

```
141     300     137364  138157          81.1001 282991
142     300     137229  138054          81.1001 282991
143     300     137229  138054          81.1001 282991
144     300     137229  138054          81.1001 282991
145     300     137229  138054          81.1001 282991
146     300     137229  138054          81.1001 282991
147     300     137229  138054          81.1001 282991
148     300     137229  138054          81.1001 282991
149     300     137229  138054          81.1001 282991
150     300     137229  138054          81.1001 282991
151     300     137229  138054          81.1001 282991
152     300     137229  138054          81.1001 282991
153     300     137229  138054          81.1001 282991
154     300     137229  138054          81.1001 282991
155     300     137229  138054          81.1001 282991
156     300     137229  138054          81.1001 282991
157     300     137229  138054          81.1001 282991
158     300     137229  138054          81.1001 282991
159     300     137229  138054          81.1001 282991
160     300     137229  138054          81.1001 282991
161     300     137229  138054          81.1001 282991
162     300     137229  138054          81.1001 282991
163     300     137229  138054          81.1001 282991
164     300     137229  138054          81.1001 282991
165     300     137229  138054          81.1001 282991
166     300     137229  138054          81.1001 282991
167     300     137229  138054          81.1001 282991
168     300     137229  138054          81.1001 282991
169     300     137229  138054          81.1001 282991
170     300     137229  138054          81.1001 282991
171     300     137229  138054          81.1001 282991
172     300     137229  138054          81.1001 282991
173     300     137229  138054          81.1001 282991
174     300     137229  138054          81.1001 282991
175     300     137229  138054          81.1001 282991
176     300     137229  138054          81.1001 282991
177     300     137229  138054          81.1001 282991
178     300     137229  138054          81.1001 282991
179     300     137229  138054          81.1001 282991
180     300     137229  138054          81.1001 282991
181     300     137229  138054          81.1001 282991
182     300     137229  138054          81.1001 282991
183     300     137229  138054          81.1001 282991
184     300     137229  138054          81.1001 282991
185     300     137229  138054          81.1001 282991
186     300     137229  138054          81.1001 282991
187     300     137229  138054          81.1001 282991
188     300     137229  138054          81.1001 282991
189     300     137229  138054          81.1001 282991
190     300     137229  138054          81.1001 282991
191     300     137229  138054          81.1001 282991
192     300     137229  138054          81.1001 282991
193     300     137229  138054          81.1001 282991
194     300     137229  138054          81.1001 282991
195     300     137229  138054          81.1001 282991
196     300     137229  138054          81.1001 282991
197     300     137229  138054          81.1001 282991
198     300     137229  138054          81.1001 282991
199     300     137229  138054          81.1001 282991
200     300     137229  138054          81.1001 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0] 24 81.1 200015
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1] 29 97.66 273733
[1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0] 24 81.1 200015
[1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1] 26 85.31 200041
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1] 29 96.78 270117
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0] 29 96.49 257801
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1] 28 93.68 240522
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1] 29 95.32 245692
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1] 28 92.69 236080
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0] 28 92.51 224590
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0] 29 96.49 257801
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1] 28 91.34 212481
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0] 28 91.81 220502
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1] 29 96.02 249780
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1] 28 91.34 212481
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0] 27 89.47 211244
```

```
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1] 27 89.0 203223
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0] 27 89.17 210890
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1] 29 95.32 245692
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0] 28 92.51 224590
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0] 28 91.81 220502
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1] 29 96.02 249780
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1] 27 88.12 201923
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0] 26 86.83 201632
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1] 29 96.78 270117
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1] 29 97.37 273379
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1] 28 92.98 236434
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1] 28 93.39 240168
[1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1] 26 85.31 200041
[1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1] 26 86.07 200217
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1] 27 88.12 201923
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0] 26 86.83 201632
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0] 26 86.25 200686
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1] 27 88.71 202869
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 29 97.66 273733
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1] 28 93.68 240522
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1] 28 92.69 236080
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0] 27 89.47 211244
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1] 27 89.0 203223
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0] 27 89.17 210890
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1] 29 97.37 273379
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1] 28 92.98 236434
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1] 28 93.39 240168
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1] 27 88.71 202869
[1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1] 26 86.07 200217
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0] 26 86.25 200686
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
```

```
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1] 30 100.0 282991
PCMSI [2.92568754 2.92568754 4.09596255 2.92568754 3.39379754 3.21825629
 2.92568754 3.21825629 3.6863663  2.63311878 3.10122879 3.6863663
 2.92568754 3.8033938  4.2715038  3.21825629 4.2715038  2.34055003
 2.34055003 3.51082504 3.21825629 2.63311878 3.6863663  3.21825629
 2.63311878 3.51082504 3.51082504 4.68110006 3.97893505 3.51082504]
PCOSTO [ 1912  1204  3253  3006  2828  2143  1839  5467  1712  5837  4456  1260
  6489  7536  9583  9812 14280  6435  9258 14929 12874  9612 13360 10558
  6107  8616 12925 37299 33211 25190]
Valor máximo que puede tener SUMA_CMSI 100 2
Valor máximo que puede tener SUMA_COSTO 282991
OBJETIVO_COSTO 200000
OBJETIVO_CMSI 80
WARNING:matplotlib.backends.backend_ps:The PostScript backend does not support transparency; partially trar
WARNING:matplotlib.backends.backend_ps:The PostScript backend does not support transparency; partially trar
```



Anexo 5: Plan de implementación

El plan de implementación del modelo de optimización para la selección de proyectos en ciberseguridad y uso de recursos en una organización pública, deberá contemplar todas las actividades necesarias para su puesta en producción. En todas las etapas es importante el apoyo y compromiso de la Alta gerencia para lograr una implementación exitosa. A continuación, se detallan las etapas para la implementación el modelo de optimización propuesto.

1. Presentación del Proyecto

El Director de TI o el responsable designado deberá presentar el proyecto a la Alta gerencia de la organización para lograr su aprobación. Se deberá definir los objetivos del proyecto, ventajas y beneficios, costos asociados al proyecto, responsabilidades y recursos necesarios.

2. Diagnóstico

Se debe conocer la situación actual de la organización en el tema de ciberseguridad. El director de TI debe nombrar a un equipo evaluador, que mediante una metodología o modelo permita conocer los aspectos a mejorar, para crear los proyectos estratégicos que permitan mejorar la seguridad. Se puede utilizar el modelo para medir la capacidad de gestión de la seguridad de la información presentado en este trabajo, que evalúa 5: 1 Estratégicos, 2 Recursos y Competencias, 3 Organización / Gestión, 4 Mejoramiento Continuo, y 5 Contexto local, nacional e internacional.

3. Planificación

El responsable del proyecto deberá definir detalladamente las actividades a realizar, sus responsables y recursos a utilizar. También se definen los procedimientos de comunicación interna para la implementación del modelo de optimización a implementar.

4. Capacitación

Se debe capacitar a los involucrados en el proyecto a implementar, en los temas relacionados a las responsabilidades, tanto personal técnico, como los usuarios finales.

5. Implementación

Se debe tener la herramienta a utilizar como un producto funcional con la respectiva de la documentación tanto de nivel técnico y operativo que esté al alcance de los

interesados. Además, se debe considerar el hardware y software que requiere la puesta en producción de esta herramienta. También hay que considerar los controles operacionales y de seguridad. Se debe realizar el seguimiento de todo lo planificado, como objetivos y requisitos, para actualizar el avance de implementación del proyecto.

6. Verificación

Debemos establecer los mecanismos de seguimiento y controles operacionales y de seguridad. Se debe realizar el seguimiento de todo lo planificado, como objetivos y requisitos, para actualizar el avance de implementación del proyecto, que debe ser revisado periódicamente por el director de TI y por el equipo de implementación.

7. Mejora Continua

Para asegurar la corrección de errores y no conformidades, se debe implementar un sistema de mejora continua, que permita corregir sistemáticamente considerando la planificación realizada.

Anexo 6: Cronograma de implementación

Descripción		Meses					
Etapas	**Actividades**	**1**	**2**	**3**	**4**	**5**	**6**
1. Presentación del proyecto.	• Estudio preliminar. • Definición de proyecto. • Exposición del proyecto.						
2. Diagnostico.	• Recoger información de los 5 factores. • Aplicar modelo para medir la capacidad de gestión de la seguridad de la información. • Dar a conocer situación actual.						
3. Planificación.	• Desarrollo del Plan de Implementación. • Definición de responsabilidades. • Definición de recursos. • Definición de procedimiento de comunicación interna.						
4. Capacitación.	• Desarrollar plan de capacitación. • Preparación de material. • Capacitación al personal. • Evaluación de las capacitaciones.						
5. Implementación.	• Obtención de herramienta y documentación. • Obtención e implementación de hardware y software. • Organización y Distribución de la documentación. • Puesta en marcha.						
6. Verificación	• Recopilación y análisis de datos. • Seguimiento y supervisión Director TI y equipo de implementación.						
7. Mejora continua.	• Implementación de mejoras, acciones preventivas y correctivas. • Seguimiento a las mejoras y acciones implementadas.						