

ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN



“Diseño de un plan estratégico de tecnologías de información para la Caja Municipal de Ahorro y Créditos de Arequipa 2022 – 2024”

**Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:**

Maestro en
Gestión de Tecnologías de la Información

Autor:

Ing. Abanto Salazar, Benjamín Guillermo

Docente Guía:

Mg. Díaz Zelada, Yvan Francisco

TACNA – PERÚ

2023

Diseño de un plan estratégico de tecnologías de información para la Caja Municipal de Ahorro y Créditos de Arequipa 2022 - 2024

ORIGINALITY REPORT

29%
SIMILARITY INDEX

28%
INTERNET SOURCES

3%
PUBLICATIONS

19%
STUDENT PAPERS

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

Dedicatoria

A mis grandes padres, Flor y Javier; un privilegio de ser su hijo. A mi esposa María Milagros, mi motor y motivo en todos los aspectos de mi vida.
A mis hijos Ariana, Francisco y Micaela, mi gran tarea en este mundo.

Agradecimientos

Al equipo de ciberseguridad de Caja Arequipa que me apoyaron e hicieron posible que este trabajo se realice con éxito.

Índice de Contenido

Dedicatoria	3
Agradecimientos.....	4
Índice de Contenido.....	5
Índice de figuras	9
Resumen	11
Introducción.....	12
Capítulo I. Antecedentes del Estudio.....	15
1.1. Título del Tema	15
1.2. Planteamiento del problema	15
1.3. Objetivos	16
1.3.1. Objetivo general	16
1.3.2. Objetivos específicos.....	16
1.4. Justificación	17
1.4.1. Justificación práctica	17
1.4.2. Justificación metodológica.....	17
1.5. Metodología	17
1.5.1. Tipo y Diseño de Investigación.....	17
1.5.2. Población y Muestra.....	19
1.5.3. Técnicas e instrumentos.....	21
1.5.4. Tratamiento y procesamiento de la información	24
1.6. Alcances y Limitaciones.....	25
1.6.1. Alcance.....	25
1.6.2. Limitaciones	26
Capítulo II. Marco Teórico	27
2.1. Conceptualización de la(s) variable(s) o tópico(s) clave	27
2.1.1. El plan estratégico	27
2.1.2. El Plan estratégico de TI	27
2.1.3. El Plan de Gobierno Digital	31
2.1.4. El Plan estratégico de Ciberseguridad	33
2.1.5. Ciberseguridad vs Seguridad de la Información	34
2.2. Importancia de las variables clave	42
2.2.1. El plan estratégico.....	42
2.2.2. Ciberseguridad	44

2.3. Análisis comparativo	47
2.3.1. Tópico 1: Enfoque estratégico.....	47
2.3.2. Tópico 2: Definir la situación actual.....	47
2.3.3. Tópico 3: Definir los objetivos estratégicos	48
2.3.4. Tópico 4: Elaborar el portafolio de proyectos	49
2.4. Análisis crítico	50
Capítulo III. Marco Referencial	53
3.1. Reseña histórica	53
3.2. Filosofía organizacional	53
3.2.1. Propósito	53
3.2.2. Misión	53
3.2.3. Visión.....	54
3.2.4. Valores	54
3.3. Diseño organizacional.....	55
3.3.1. El Directorio.....	56
3.3.2. La Gerencia Mancomunada	56
3.3.3. Las Gerencia de TI	56
3.3.4. Comités especializados.....	57
3.4. Productos y/o servicios	58
3.4.1. Productos Activos.....	58
3.4.2. Productos Pasivos.....	58
3.5. Diagnóstico organizacional	59
3.5.1. Administración y gerencia	59
3.5.2. Marketing y ventas	60
3.5.3. Operaciones y logística	62
3.5.4. Finanzas y contabilidad.....	63
3.5.5. Recursos humanos.....	65
3.5.6. Sistemas de información y comunicaciones.....	67
3.5.7. Tecnología e investigación	68
3.5.8. Conclusiones del diagnóstico	69
Capítulo IV. Resultados	74
4.1. Entendimiento de la estrategia de negocio	75
4.1.1. Propósito	75
4.1.2. Misión	75
4.1.3. Visión.....	75
4.1.4. Objetivos estratégicos	75

4.2. Diagnóstico de capacidades de ciberseguridad	77
4.2.1. Identificación de requerimientos	79
4.2.2. Definición criterios de evaluación	80
4.2.3. Identificación de controles disponibles	82
4.2.4. Evaluación del cumplimiento de controles disponibles.....	82
4.2.5. Postura actual de ciberseguridad	83
4.2.6. Postura objetivo de ciberseguridad	86
4.2.7. Plan de mejora	86
4.3. Diagnóstico de estructura organizacional de ciberseguridad	87
4.3.1. Estructura organizacional de la Gerencia de TI.....	87
4.3.2. Estructura organizacional de Ciberseguridad y Continuidad Operacional	88
4.3.3. Diagnóstico de estructura organizacional.....	89
4.4. Diseño de la estrategia de SGSI-C	91
4.4.1. Propósito del SGSI-C	92
4.4.2. Misión del SGSI-C	92
4.4.3. Visión del SGSI-C.....	92
4.4.4. Objetivos estratégicos del SGSI-C	92
4.5. Diseñar plan de implantación de estrategias	93
4.5.1. Portafolio de proyectos de ciberseguridad	93
4.5.2. Mapa de ruta	96
4.6. Diseño de Estructura organizacional.....	97
4.6.1. Gobierno y Gestión de Ciberseguridad	98
4.6.2. Identificación de Riesgos.....	98
4.6.3. Protección a Amenazas.....	98
4.6.4. Detección y Respuesta de Incidentes	99
4.6.5. Recuperación de servicios	99
4.7. Diseñar de mecanismos de control.....	100
4.7.1. Matriz de comunicaciones	100
4.7.2. Cronograma de actividades.....	102
4.7.3. Indicadores de los objetivos estratégicos	103
4.7.4. Dashboard de ciberseguridad	105
Capítulo V. Conclusiones y Recomendaciones	107
5.1. Conclusiones	107
5.2. Recomendaciones	111
Capítulo VI. Bibliografía	115
Capítulo VII. Anexos.....	118

7.1. Anexo A: Formulario del Diagnóstico de capacidad de ciberseguridad	118
7.1.1. Requerimientos	118
7.1.2. Criterios de evaluación	119
7.1.3. Controles disponibles	120
7.1.4. Evaluación de controles	121
7.1.5. Efectividad del control	121
7.1.6. Acciones de mejora	122
7.2. Anexo B: Cuestionario del Diagnóstico de la estructura organizacional de Ciberseguridad.....	123

Índice de figuras

Figura 1 Marco de trabajo para crear un Plan IT Agile	28
Figura 2 Las 7 etapas del proceso del Plan de Gobierno Digital” (PGD).....	32
Figura 3 Los 6 pasos de desarrollo y mantenimiento anual para una estrategia de ciberseguridad y resiliencia cibernética.	34
Figura 4 Seguridad de Informacion vs Ciberseguridad.....	38
Figura 5 Diferencias entre seguridad de la información, seguridad informática, y ciberseguridad.	39
Figura 6 Organigrama institucional.....	55
Figura 7 El Departamento de Ciberseguridad y Continuidad Operacional	57
Figura 8 Saldo de colocaciones 2021 de Caja Arequipa	61
Figura 9 Pasivos totales al cierre 2021	62
Figura 10 Cobertura Nacional de Caja Arequipa	63
Figura 11 Estado de Resultados - diciembre 2021	64
Figura 12 Estado de Situación Financiera - Diciembre 2021	65
Figura 13 Gestión del Capital Humano.....	66
Figura 14 Diagrama de Ishikawa del AMOFHIT	70
Figura 15 Mapa Estratégico 2022-2023	76
Figura 16 Etapas del diagnóstico de ciberseguridad	78
Figura 17 Marco de trabajo de ciberseguridad de NIST	79
Figura 18 Ejemplo de Definición de requerimientos	80
Figura 19 Estándar CIS Controls V8	81
Figura 20 Ejemplo de Criterios de evaluación	81
Figura 21 Ejemplo de identificación de controles disponibles	82
Figura 22 Ejemplo de evaluación y efectividad del control	83
Figura 23 Ejemplo de nivel de cumplimiento de funciones NIST-CSF	84
Figura 24 Ejemplo de nivel de cumplimiento de las categorías NIST-CSF	85

Figura 25 Ejemplo del nivel de cumplimiento de CIS Controls	85
Figura 26 Ejemplo de postura objetivo de ciberseguridad y metas anuales	86
Figura 27 Organigrama de la Gerencia de TI	88
Figura 28 Organigrama del departamento de Ciberseguridad y Continuidad Operacional	88
Figura 29 Cumplimiento del marco de trabajo de NICE	90
Figura 30 Cumplimiento de tareas por frente de Ciberseguridad	91
Figura 31 Mapa de ruta de los proyectos estratégicos de ciberseguridad.....	96
Figura 32 Modelo de funciones de Ciberseguridad	97
Figura 33 Estructura organizacional del departamento de Ciberseguridad	100
Figura 34 Ejemplo de cronograma de proyectos del PE SGSI-C	102
Figura 35 Ejemplo de detalle de actividades, tareas, responsables, fechas de proyectos	103
Figura 36 Ejemplo de Dashboard de ciberseguridad.....	106

Resumen

Este trabajo de investigación, titulado “Diseño de un Plan Estratégico de Tecnologías de Información para la Caja Municipal de Ahorro y Crédito de Arequipa 2022-2024”, se ha elaborado con un enfoque de Plan estratégico del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (Plan estratégico del SGSI-C) con el fin de asegurar la visión de la entidad (“liderar la transformación de la industria microfinanciera, y centrado en el uso avanzado de tecnologías digitales e información”), mediante la adecuada gestión riesgos de seguridad de la información y ciberseguridad, que afectan las expectativas de los clientes, los accionistas, y entes reguladores como la Superintendencia de Banca Seguros y AFP (SBS).

Este trabajo propone un método para formular un Plan Estratégico del SGSI-C, a fin de mejorar el nivel de conocimiento de las capacidades actuales de ciberseguridad de la entidad y el alineamiento de las inversiones en ciberseguridad con los objetivos estratégicos del Plan Estratégico Institucional (PEI), así como cumplir con los requerimientos del reglamento SBS-504-2021 de la SBS.

El Plan Estratégico del SGSI, propone un horizonte de planificación de 3 años; y se basa en el estudio completo de las capacidades de ciberseguridad a fin de obtener la postura actual de ciberseguridad de la entidad, basado en el estándar NIST-CSF (por sus siglas en inglés de Cyber Security Framework - CSF del National Institute of Standards and Technology - NIST). También se realizó un diagnóstico de la estructura organizacional de ciberseguridad. Sobre la base de estos diagnósticos se desplegó la etapa de planeamiento estratégico que incluye propósito, misión, visión, objetivos estratégicos, portafolio de proyectos, y un mapa de ruta, así como una propuesta de estructura organizacional de ciberseguridad, y finalmente los instrumentos para las etapas de dirección y control estratégico.

Introducción

Las empresas en general y en especial las del sector financiero como Caja Arequipa, para atender sus objetivos institucionales transformación digital, planes de innovación, planes comerciales y sólida gestión de riesgos, dependen del funcionamiento confiable de las tecnologías digitales, sistemas de información y la infraestructura tecnológica que la soporta. Las amenazas de seguridad de la información y ciberseguridad buscan explotar la mayor diversidad, complejidad y conectividad de los sistemas de información y de la infraestructura tecnológica que la soporta, lo que pone en riesgo la seguridad del negocio, su economía y la seguridad de sus clientes. De manera similar a los riesgos financieros y de reputación, el riesgo de ciberseguridad afecta el resultado final de la entidad; y puede aumentar los costos y afectar los ingresos. Así mismo, puede afectar la capacidad de la entidad para innovar, y aumentar o mantener sus clientes. La ciberseguridad puede ser un componente importante y amplificador de la gestión de riesgos corporativos. (NIST National Institute of Standards and Technology, 2018)

Considerando el contexto anterior, el presente trabajo de investigación tiene el objetivo de abordar esta problemática al proponer un proceso para diseñar un Plan estratégico del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (Plan estratégico del SGSI-C) para la Caja Arequipa, alineado a los requerimientos de la SBS.

La estructura de esta propuesta de Plan estratégico del SGSI-C para la la Caja Arequipa, consta de los siguientes contenidos:

Capítulo I. Antecedentes del Estudio. Se presenta el título del tema, el planteamiento del problema, el objetivo general, los objetivos específicos, la

justificación práctica y justificación metodológica, la metodología de investigación (tipo, diseño, población, muestra, técnicas, instrumentos, procesamientos de información), alcance u limitaciones.

Capítulo II: Marco Teórico. En esta sección se presentan la conceptualización de las variables o tópicos, como plan estratégico, plan estratégico de TI, plan de gobierno digital, plan estratégico de ciberseguridad, y diferencias entre seguridad de la información y ciberseguridad. Asimismo, se sobre estos conceptos se desarrolla un análisis de la importancia, análisis comparativo y finalmente un análisis crítico.

Capítulo III: Marco Referencial. Se presenta información de la Caja Arequipa, se sirve como base para el desarrollo de resultados del Plan Estratégico SGSI-C. Se incluye reseña histórica de la entidad (fundación, número de trabajadores), la filosofía organizacional (propósito, misión, visión, valores), diseño organizacional, productos y servicios, así como un diagnóstico organizacional siguiendo la metodología AMOFHIT, que concluye con un diagrama causa efecto.

Capítulo IV: Resultados. En este capítulo se presentan la estrategia institucional (propósito, misión, visión y objetivos estratégicos), el despliegue del diagnóstico de las capacidades de ciberseguridad basado en NIST-CSF, que concluye con un Postura actual y Postura objetivo de ciberseguridad, y el despliegue del diagnóstico de estructura organizacional de ciberseguridad. Sobre lo anterior se presenta el diseño de la estrategia del SGSI-C (propósito, misión, visión, objetivos estratégicos), el plan de implementación (portafolio de proyectos y mapa de ruta), propuesta de diseño de estructura organizacional, y finalmente mecanismos de control (matriz de comunicaciones, cronograma de actividades, indicadores) como instrumentos para la dirección y control estratégicos.

Capítulo V. Conclusiones y Recomendaciones, Finalmente se redactaron las conclusiones que responden a objetivos de estudio, así como las recomendaciones más importantes para la implementación del Plan estratégico del SGSI-C .

Capítulo VI Bibliografía. Finalmente se adjuntaron las referencias bibliográficas utilizadas en el presente trabajo de investigación, con las fuentes bibliográficas, desde donde se han extraído la información relevante de diversos autores.