



Universidad Nacional
SAN LUIS GONZAGA



Atribución-NoComercial-SinDerivadas 4.0 Internacional

Esta licencia es la más restrictiva de las seis licencias principales Creative Commons, permitiendo a otras solo descargar sus obras y compartirlas con otras siempre y cuando den crédito, pero no pueden cambiarlas de forma alguna ni usarlas de forma comercial.

<http://creativecommons.org/licenses/by-nc-nd/4.0>



“AÑO DE LA ESPERANZA Y EL FORTALECIMIENTO DE LA DEMOCRACIA”

CONSTANCIA DE ANTIPLAGIO

El que suscribe director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas de la UNICA, deja constancia que se ha realizado el análisis con el software de verificación de similitud al documento **TRABAJO DE SUFICIENCIA PROFESIONAL** titulado:

“PLATAFORMA DE TOKENIZACIÓN PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CUMPLIMIENTO DEL ESTÁNDAR PCI DSS, EN LA CAJA MUNICIPAL DE AHORRO Y CRÉDITO DE ICA S.A”

Presentado por:

ARNOLD HUATAQUISPE POMA

BACHILLER en PREGRADO de la facultad de Ingeniería de Sistemas; cuyo resultado obtenido es **porcentaje de similitud 1%**; por el cual se otorga el calificativo de: **APROBADO**, según el Reglamento de Evaluación de la Originalidad; adjuntando al presente, el reporte de evaluación con el software de verificación de originalidad.

Se expide la presente conformidad para la continuación del trámite respectivo.

Ica, 29 de enero de 2026

Dr. LUIS ALBERTO MASSA PALACIOS
Director de la Unidad de Investigación
Facultad de Ingeniería de Sistemas

UNIVERSIDAD NACIONAL “SAN LUIS GONZAGA”

VICERRECTORADO DE INVESTIGACIÓN

FACULTAD INGENIERÍA DE SISTEMAS



“PLATAFORMA DE TOKENIZACIÓN PARA LA PROTECCIÓN DE
DATOS SENSIBLES EN CUMPLIMIENTO DEL ESTÁNDAR PCI
DSS, EN LA CAJA MUNICIPAL DE AHORRO Y CRÉDITO DE ICA
S.A”

Línea de investigación: Ciencias naturales, ingeniería y tecnologías sostenibles

Informe Final de Trabajo de Suficiencia Profesional

Autor: Arnold Huataquispe Poma

ICA - PERÚ

2025

DEDICATORIA

Agradezco a Dios por bendecirme con una familia maravillosa, cuyo amor, ejemplo y apoyo incondicional han sido fundamentales en mi vida.

A mis padres, Adolfo y Bernardita, por inculcarme el valor del esfuerzo y la valentía, y a toda mi familia por acompañarme con sus palabras de aliento y confianza en cada paso.

Dedico este trabajo también a mis amigos y colegas, quienes con su apoyo y enseñanzas han contribuido a mi crecimiento personal y profesional.

Arnold

AGRADECIMIENTOS

A Dios, por iluminar mi camino y bendecirme con una familia que siempre ha estado presente. A mis padres, por guiarme con su ejemplo de esfuerzo y superación, y a mi familia, por su apoyo incondicional en cada decisión y proyecto. A la Universidad San Luis Gonzaga de Ica, en especial a la Facultad de Ingeniería de Sistemas y a mis docentes, cuyo conocimiento y enseñanza han sido clave en mi formación profesional. A mis amigos, por su compañía y por cada lección compartida a lo largo de este camino.

Arnold

ÍNDICE

PORTADA	i
DEDICATORIA	ii
AGRADECIMIENTOS	iii
INDICE DE CONTENIDOS	iv
INDICE DE FIGURAS	vi
RESUMEN	vii
ABSTRACT	viii
CAPÍTULO I: INFORMACION DE LA INSTITUCION DONDE SE DESARROLLO LA EXPERIENCIA	7
1.1. Contexto Laboral	7
1.2. Visión, Misión y Valores Empresariales	7
1.3. Descripción de actividades empresariales	8
CAPÍTULO II: TRAYECTORIA PROFESIONAL	10
2.1. Puesto actual	10
2.2. Experiencias laborales anteriores	11
CAPÍTULO III: APLICACIÓN PROFESIONAL	15
3.1. Metodología de implementación	15
3.2. Arquitectura consolidada de la plataforma	16
3.3. Descripción del programa laboral	17
3.4. Objetivo del proyecto tecnológico	18
3.5. Participación:	18
3.6. Plataforma Cipher Web:	20
CAPÍTULO IV: APORTES A LA INSTITUCIÓN	26
4.1. Mejora en la Seguridad de los Datos Sensibles	26
4.2. Cumplimiento de Normativas Internacionales	26
4.3. Reducción de Costos Operativos y de Seguridad	26
4.4. Optimización de procesos internos	26

4.5.	Fortalecimiento de la Confianza de los Clientes	26
4.6.	Resiliencia ante Ataques Cibernéticos	26
	CONCLUSIONES	28
	RECOMENDACIONES	29
	REFERENCIAS BIBLIOGRÁFICAS	30
	ANEXOS	32

ÍNDICE DE FIGURAS

FIG 1: ORGANIGRAMA DE LA GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES.	9
FIG 2: ORGANIGRAMA DEL DEPARTAMENTO DE SOLUCIONES DE TI.	9
FIG 3: ORGANIGRAMA DE LA UNIDAD DE PROYECTOS DE SOFTWARE - CANALES DIGITALES Y ALTERNATIVOS.	9
FIG 4: MODULO PRINCIPAL.	20
FIG 5: MODULO DE PROCESAMIENTO.	21
FIG 6: MODULO SELECCIÓN DE BASE DE DATOS.	22
FIG 7: MÓDULO DE SELECCIÓN DE PLANTILLAS.	22
FIG 8: MÓDULO DE SELECCIÓN TABLAS Y COLUMNAS.	23
FIG 9: MÓDULO DE MANTENIMIENTO.	23
FIG 10: MODULO DE CARGA DE INFORMACIÓN.	25
FIG 11: SEGUIMIENTO DE ACTIVIDADES DE PERSONAL A CARGO.	32
FIG 12: ESTACIÓN DE TRABAJO.	32
FIG 13: EQUIPO DE LA GERENCIA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES.	33

RESUMEN

El presente informe tiene como objetivo desarrollar e implementar una plataforma de tokenización para la protección de datos sensibles, garantizando el cumplimiento del estándar PCI DSS en la Caja Municipal de Ahorro y Crédito de Ica S.A. La propuesta busca reducir el riesgo de exposición de información confidencial, optimizar la seguridad en transacciones financieras y fortalecer la confianza de los clientes.

La metodología aplicada se basó en el diseño e implementación de un sistema web denominado *Cipher Web*, desarrollado bajo un enfoque ágil y utilizando herramientas tecnológicas de última generación. Entre ellas destacan: SQL Server 2014 para la gestión de datos, Docker y OpenShift para la contenerización y orquestación de servicios, Spring Boot con Java 11 para el desarrollo backend, Bitbucket para el control de versiones, Jenkins para la integración y entrega continua (CI/CD), y JWT con autenticación de doble factor para garantizar la seguridad en el acceso. Asimismo, se incorporaron prácticas de DevSecOps, integrando pruebas automatizadas y revisiones de código seguro en todas las etapas del ciclo de vida del software.

Los resultados evidencian mejoras significativas en la protección de datos financieros, reducción de costos operativos asociados a la seguridad y optimización de los procesos internos de gestión de información. La plataforma asegura el cumplimiento de las normativas internacionales y refuerza la resiliencia de la institución frente a posibles ataques cibernéticos.

Se recomienda realizar auditorías periódicas, mantener la actualización de la infraestructura tecnológica y capacitar de manera continua al personal, con el fin de garantizar la sostenibilidad y escalabilidad de la solución en el tiempo.

Palabras clave: Tokenización, Datos sensibles, PCI DSS, Seguridad de la información, Gestión de datos.

ABSTRACT

The purpose of this report is to design and implement a tokenization platform for the protection of sensitive data, ensuring compliance with the PCI DSS standard at Caja Municipal de Ahorro y Crédito de Ica S.A. The solution aims to reduce the risk of exposing confidential information, optimize security in financial transactions, and strengthen customer trust.

The applied methodology was based on the design and deployment of a web platform called *Cipher Web*, developed under an agile approach and supported by advanced technologies. Key tools included SQL Server 2014 for data management, Docker and OpenShift for service containerization and orchestration, Spring Boot with Java 11 for backend development, Bitbucket for version control, Jenkins for continuous integration and delivery (CI/CD), and JWT with two-factor authentication for secure access. Additionally, DevSecOps practices were integrated to ensure security from the design stage to production, including automated testing and secure code reviews.

The results demonstrate significant improvements in financial data protection, a reduction in operational costs associated with security, and the optimization of internal data management processes. The platform ensures compliance with international standards and enhances the institution's resilience against cyberattacks.

It is recommended to conduct periodic audits, maintain continuous updates of the technological infrastructure, and provide ongoing staff training to ensure the sustainability and scalability of the solution.

Keywords: Tokenization, Sensitive data, Data security, PCI DSS compliance, Information systems.

INTRODUCCIÓN

En la era digital, la seguridad de la información se ha convertido en un pilar fundamental para las organizaciones, especialmente en el sector financiero, donde se procesan grandes volúmenes de datos sensibles de los clientes. El incremento del comercio electrónico, el uso masivo de tarjetas de crédito y débito, así como la proliferación de amenazas cibernéticas, han generado la necesidad de adoptar mecanismos robustos de protección de datos. Ante este escenario, la seguridad en las transacciones financieras se ha convertido en una prioridad, no solo para las entidades bancarias y crediticias, sino también para los organismos reguladores que buscan garantizar la integridad, confidencialidad y disponibilidad de la información.

Uno de los principales desafíos en la protección de datos financieros es la prevención del acceso no autorizado y la exposición de información crítica, como los números de tarjeta de pago, códigos de seguridad y datos personales de los usuarios. En respuesta a estos riesgos, se han desarrollado diversos estándares y normativas de seguridad, siendo el Payment Card Industry Data Security Standard (PCI DSS) una de las más relevantes a nivel global. Este estándar, establecido por el PCI Security Standards Council, define un conjunto de requisitos que las organizaciones deben cumplir para garantizar la protección de los datos de tarjetas de pago y mitigar los riesgos asociados a fraudes financieros.

Dentro de las estrategias tecnológicas recomendadas para el cumplimiento de PCI DSS, la tokenización ha emergido como una solución efectiva para proteger datos sensibles. Este proceso consiste en reemplazar los datos originales con un identificador único denominado "token", el cual no tiene valor fuera del entorno seguro donde se genera. A diferencia de los métodos tradicionales de cifrado, la tokenización reduce la exposición de los datos reales en los sistemas internos, minimizando el riesgo de robo de información y facilitando el cumplimiento normativo.

En este contexto, el presente informe final tiene como objetivo el diseño e implementación de una plataforma de tokenización en la Caja Municipal de Ahorro y Crédito de Ica S.A., con el propósito de reforzar la seguridad en el manejo de datos sensibles y garantizar el cumplimiento del estándar PCI DSS. Esta iniciativa busca optimizar los procesos de almacenamiento y transmisión de información financiera, reduciendo el riesgo de exposición de datos confidenciales y mejorando la confianza de los clientes en los servicios ofrecidos por la entidad.

La implementación de esta plataforma no solo fortalecerá la seguridad de los datos, sino que también traerá beneficios operativos y estratégicos para la institución, como la reducción de costos asociados a la gestión de seguridad, la minimización del impacto de posibles brechas de datos y el cumplimiento con regulaciones internacionales. En este sentido, el desarrollo del presente trabajo contribuirá a la modernización de la infraestructura tecnológica de la Caja

Municipal de Ahorro y Crédito de Ica S.A., alineándose con las mejores prácticas de seguridad en la industria financiera.

Objetivo general

Implementar una plataforma de tokenización para la protección de datos sensibles en la Caja Municipal de Ahorro y Crédito de Ica S.A., asegurando el cumplimiento del estándar PCI DSS y contribuyendo a la mejora de la seguridad de la información.

Objetivos específicos

- Analizar la situación actual de la gestión de datos sensibles en la institución y sus principales riesgos frente a amenazas de seguridad.
- Diseñar la arquitectura tecnológica de la plataforma de tokenización, incorporando herramientas de seguridad y prácticas de desarrollo seguro.
- Implementar la solución tecnológica (*Cipher Web*) con base en metodologías ágiles, garantizando su eficiencia y confiabilidad.
- Validar la plataforma a través de pruebas de seguridad y auditorías, verificando su alineación con los requisitos de PCI DSS.
- Evaluar los beneficios obtenidos en términos de seguridad, cumplimiento normativo, optimización de procesos internos y reducción de costos.

Problemática

Uno de los principales problemas es el almacenamiento y procesamiento de datos sensibles sin una adecuada estrategia de protección, lo que incrementa la vulnerabilidad ante ataques cibernéticos. La falta de una solución efectiva que minimice la exposición de estos datos en los sistemas internos de la institución puede derivar en el incumplimiento de normativas internacionales, como el PCI DSS (Payment Card Industry Data Security Standard), lo que no solo pone en riesgo la confidencialidad de la información de los clientes, sino que también podría generar sanciones económicas y afectar la reputación de la entidad.

En este sentido, la necesidad de implementar un mecanismo seguro y eficiente para la protección de datos sensibles se vuelve fundamental. Actualmente, los métodos tradicionales de cifrado presentan limitaciones, ya que, aunque protegen la información, no eliminan completamente la posibilidad de que los datos puedan ser comprometidos en caso de una brecha de seguridad. Es en este contexto donde la tokenización surge como una alternativa tecnológica efectiva, ya que permite reemplazar los datos reales por identificadores únicos sin valor fuera del sistema seguro donde se generan, reduciendo así el riesgo de exposición y facilitando el cumplimiento de PCI DSS.

Con esta implementación, se espera no solo mejorar la seguridad de los datos dentro de la entidad, sino también optimizar los procesos internos, fortalecer la confianza de los clientes en los servicios financieros y garantizar el cumplimiento de las normativas internacionales.

¿Cómo implementar una plataforma de tokenización que permita proteger los datos sensibles y garantizar el cumplimiento del estándar PCI DSS en la Caja Municipal de Ahorro y Crédito de Ica S.A.?

Los antecedentes que dan sustento a este informe fueron:

Según [1] La tokenización está en sus primeras etapas, pero tiene el potencial de revolucionar por completo los mercados financieros. No solo facilitará el acceso a las inversiones, sino que también permitirá la creación de nuevos productos financieros que aún no podemos imaginar.

Asimismo, al posibilitar el comercio de activos a nivel global, eliminando fronteras y reduciendo barreras, nos encontramos ante un verdadero cambio de paradigma en el ámbito financiero. Aunque aún existen desafíos por superar, el impacto de esta tecnología es inmenso.

En definitiva, la tokenización de activos está redefiniendo las dinámicas del mercado financiero. Con beneficios como mayor accesibilidad, liquidez inmediata y una menor dependencia de intermediarios, el panorama de las inversiones se proyecta como más inclusivo y eficiente. Si te interesan la tecnología y las finanzas, o simplemente deseas ser parte de esta transformación, es el momento ideal para prestar atención a la tokenización.

Según [2] Dado que la tokenización de activos está en constante crecimiento a nivel global, el presente estudio examina el estado actual del mercado y la normativa internacional relacionada con su aplicación en el financiamiento de proyectos inmobiliarios. En este contexto, se propondrá una posible estructura para estos proyectos, identificando a los actores involucrados, así como las oportunidades y riesgos asociados a su implementación en el Perú. Finalmente, se evaluará su viabilidad desde una perspectiva tanto legal como financiera.

Según [3] La forma más efectiva y evidente de reducir el alcance de PCI-DSS en cualquier sistema que maneje datos de tarjetas es, sin duda, evitar su uso por completo. Sin embargo, dado que esto no siempre es viable, una alternativa adecuada es la tokenización de estos datos, mientras que otra opción podría ser el cifrado, tema que podría abordarse en un futuro artículo si genera interés entre los lectores.

En este artículo, exploraremos la tokenización en el contexto de PCI-DSS, desde sus fundamentos hasta el diseño básico de un sistema de tokenización para tarjetas de pago, utilizando los servicios en la nube de Amazon Web Services (AWS).

Para garantizar precisión y evitar malentendidos, utilizaremos la terminología oficial en inglés establecida en la normativa y guías del PCI Security Standards Council (PCI SSC), así como en los lineamientos de VISA, MASTERCARD y AWS.

Según [4] Una Moneda Digital del Banco Central (CBDC, por sus siglas en inglés) es una forma de dinero soberano emitido por el banco central en formato digital, que puede almacenarse en cuentas o representarse a través de tokens digitales con valor. Las CBDC pueden diseñarse para transacciones entre instituciones financieras (mayoristas) o para el uso de personas y empresas (minoristas), siendo esta última opción la que despierta mayor interés, especialmente en economías emergentes.

El diseño de una CBDC puede estructurarse bajo distintos esquemas de asignación de roles y responsabilidades entre el banco central y el sector privado. En este contexto, el Banco Central de Reserva del Perú (BCRP) ha desarrollado un documento titulado "CBDC: Promoviendo los pagos digitales en el Perú", el primero de una serie de estudios que buscan evaluar la necesidad, el diseño adecuado y el momento oportuno para la posible emisión de una CBDC en el país. Esta iniciativa se alinea con los esfuerzos de otros bancos centrales a nivel global, reconociendo el impacto potencial de una CBDC en la expansión de los pagos digitales, la reducción de costos asociados al manejo de efectivo, el fortalecimiento de la estabilidad financiera, la mejora en la transmisión de la política monetaria y el fomento de la competencia e innovación en el sector financiero.

El documento presenta los hallazgos de la fase de investigación del BCRP, realizada con el apoyo técnico del Fondo Monetario Internacional. Entre los temas abordados se incluyen la situación actual del sistema de pagos en el Perú, los posibles usos de una CBDC para la inclusión financiera de personas no bancarizadas y los factores clave para su diseño e implementación como un complemento a los medios de pago existentes en el país.

Junto con la publicación del informe, se ha lanzado una encuesta dirigida a actores del mercado para recopilar opiniones sobre aspectos clave del estudio. Los resultados de esta consulta servirán de base para una siguiente fase de exploración, que incluirá pruebas más concretas bajo el concepto de "Desafíos de Innovación", con la participación de expertos, reguladores y proveedores tecnológicos.

Este documento representa un aporte significativo en la discusión sobre la digitalización de los pagos en el Perú y la viabilidad de emitir una CBDC como herramienta para fortalecer el ecosistema financiero del país.

Según [5] La tokenización de datos es un mecanismo avanzado diseñado para resguardar información sensible sin comprometer su operatividad dentro de diversos procesos empresariales. Al reemplazar los datos confidenciales con identificadores únicos denominados *tokens*, las organizaciones pueden fortalecer la seguridad de la información sin afectar su funcionalidad.

Clasificación de datos sensibles

El primer paso consiste en identificar y categorizar los datos que requieren protección, como números de tarjetas de crédito, información de seguridad social, historiales médicos y otros registros financieros o personales.

Generación de tokens

Luego, se crean tokens únicos para sustituir los datos confidenciales. Estos tokens no tienen valor por sí mismos y carecen de utilidad para cualquier persona que no tenga acceso autorizado al sistema de tokenización.

Vinculación con los datos originales

Los tokens generados se asocian a los datos originales dentro de un entorno seguro. Esta relación es crucial, ya que permite recuperar la información real cuando sea necesario, garantizando su integridad y disponibilidad.

Almacenamiento seguro de la información

Los datos originales se almacenan en un entorno altamente protegido y separado de los tokens, de modo que, incluso si los tokens fueran expuestos, la información confidencial permanecería segura.

Uso de los datos tokenizados

Finalmente, los tokens reemplazan los datos originales en procesos de análisis y transacciones comerciales. De este modo, las empresas pueden operar con normalidad mientras se mantiene la seguridad y privacidad de la información protegida

Según [6] La tokenización de datos consiste en transformar información sensible, como los datos de tarjetas de crédito, en tokens que pueden ser transferidos de manera segura a través de la blockchain sin exponer la información original.

Este proceso contribuye a mejorar la seguridad, la privacidad y el cumplimiento normativo, reduciendo el riesgo de accesos no autorizados y el uso indebido de los datos.

Para aprovechar sus ventajas y minimizar posibles limitaciones, la implementación de la tokenización debe realizarse con un enfoque meticuloso y estratégico.

Según [7], la versión 4.0.1 del PCI DSS publicada en 2024 refuerza el rol de la tokenización como medida para reducir el alcance de la auditoría de seguridad. Esta actualización subraya que el reemplazo de datos confidenciales por tokens es clave para limitar la exposición y mejorar la protección de la información.

De acuerdo con [8], las actualizaciones de 2025 para comerciantes que validan con SAQ A refuerzan el papel de la tokenización como estrategia para manejar datos de forma indirecta sin perder cumplimiento. Esto es especialmente relevante para negocios que dependen de terceros para procesar transacciones.

En [9] se indica que Amazon Web Services ofrece soluciones certificadas PCI que incluyen tokenización como servicio, permitiendo a las empresas reducir la retención de datos sensibles y mitigar riesgos en arquitecturas en la nube.

De acuerdo con [10], Google Cloud integra capacidades nativas de tokenización dentro de su servicio de protección de datos (DLP), permitiendo reemplazar información sensible con tokens irreversibles. Esto contribuye a cumplir con estándares como PCI DSS de manera más sencilla.

De acuerdo con [11], la documentación de Cybersource (Visa) enfatiza que la tokenización disminuye significativamente el alcance de PCI DSS, al reemplazar datos de tarjetas por tokens que pueden utilizarse en operaciones recurrentes sin necesidad de almacenar información real.

Según [12], la plataforma Adyen promueve el uso de tokenización como estándar en pagos digitales. Los tokens permiten ofrecer experiencias de usuario fluidas, como compras con un clic, manteniendo la seguridad y el cumplimiento normativo.

En [13] se explica que Stripe integra la tokenización como parte de sus controles PCI DSS. El servicio permite a las empresas operar sin necesidad de manejar directamente los números reales de las tarjetas, reduciendo riesgos y responsabilidades.

En [14] se describe que Mastercard emplea la tokenización dentro de su ecosistema MDES como estrategia global para proteger pagos digitales. Este marco asegura que los tokens puedan usarse en distintos dispositivos y canales de forma interoperable.

Según [15], EMVCo actualizó en 2024 su marco técnico de tokenización de pagos, proporcionando nuevas especificaciones que amplían la seguridad en transacciones móviles y comercio electrónico. La iniciativa busca homogeneizar la adopción en la industria.

CAPÍTULO I: INFORMACION DE LA INSTITUCION DONDE SE DESARROLLO LA EXPERIENCIA

1.1. Contexto Laboral

1.1.1. Información General

La Caja Municipal de Ahorro y Crédito de Ica, es una empresa financiera de derecho público que goza de autonomía económica, financiera y administrativa, desarrolla sus actividades basándose en sus principios: Democratización y descentralización del crédito, así como fomentar e incentivar una cultura de ahorro. Igualmente está autorizada a ofrecer el servicio de créditos pignoratícios y desarrollar otros servicios financieros.

Actualmente tiene el nombre de Caja Municipal de Ahorro y Crédito de Ica S.A. (CMAC ICA S.A.), identificada con RUC: 20104888934.

Se rige por Ley No. 26702: “Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros”.

Sus antecedentes se remontan al Decreto Ley N.º 23039 (1980), que reguló la creación de las Cajas Municipales, y al Decreto Supremo N.º 225-87-EF (1987), que estableció la Federación Peruana de Cajas Municipales. Ese mismo año, la Municipalidad Provincial de Ica formalizó su constitución mediante resolución municipal, y en 1989 se autorizó el inicio de operaciones. Desde entonces, la CMAC Ica funciona como entidad de intermediación financiera especializada en microfinanzas, con autonomía administrativa, financiera y económica, bajo supervisión de la Superintendencia de Banca y Seguros.

Ubicación: La oficina central está ubicada en la AV. CONDE DE NIEVA NRO. 498 Ica - Ica - Ica.

Página Web: <https://cajaica.pe/>

1.2. Visión, Misión y Valores Empresariales

1.2.1. Visión:

Ser una microfinanciera líder, reconocida por entender las necesidades de las personas brindando la mejor experiencia.

1.2.2. Misión:

Impulsar el desarrollo de los emprendedores y personas ofreciendo soluciones financieras integrales y promoviendo la inclusión financiera.

1.2.3. Valores:

Pasión por servir: Estamos comprometidos en brindar un servicio de calidad (transparencia, oportunidad y calidez) a nuestros clientes externos e internos, dando siempre lo mejor de nosotros.

Integridad: Trabajamos con honestidad, generamos confianza y actuamos de manera consistente con nuestros principios éticos.

Potenciamos tu talento: Nos preocupamos por el bienestar y crecimiento personal y profesional de todos nuestros colaboradores.

Eficiencia: Cumplimos con nuestras metas y objetivos gestionando de manera óptima nuestros recursos para el cumplimiento de los logros propuestos de la empresa.

Actitud innovadora: Buscamos activamente mejores formas de realizar nuestro trabajo y estamos abiertos a la aplicación de soluciones innovadoras.

1.3. Descripción de actividades empresariales

La Caja Municipal de Ahorro y Crédito de Ica (CMAC Ica) es una entidad financiera que integra el sistema de Cajas Municipales del Perú, orientada a la atención de MYPES y personas naturales, promoviendo la inclusión financiera regional. Sus principales actividades comprenden:

- Captación de ahorros: Ofrece cuentas de ahorro, depósitos a plazo fijo y otros productos financieros que permiten a los clientes resguardar y hacer crecer su dinero.
- Otorgamiento de créditos: Brinda financiamiento a emprendedores y empresas, facilitando créditos personales, microcréditos, créditos hipotecarios y otros tipos de préstamos adaptados a las necesidades de sus clientes.
- Servicios financieros adicionales: Incluye transferencias de dinero, pago de servicios, seguros y otros productos financieros complementarios.
- Digitalización y banca electrónica: A través de plataformas digitales, la Caja Municipal de Ica ofrece acceso a sus servicios mediante aplicaciones móviles y banca por internet, facilitando la gestión financiera de sus clientes.

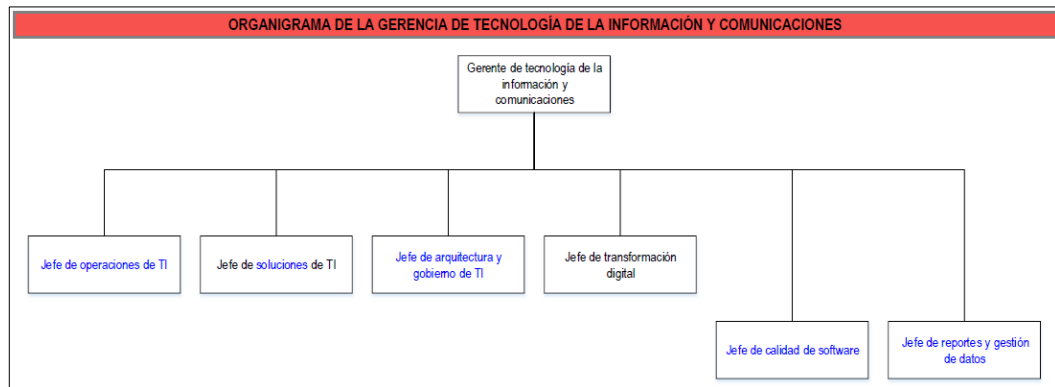


Fig 1: Organigrama de la gerencia de Tecnología de la información y comunicaciones.

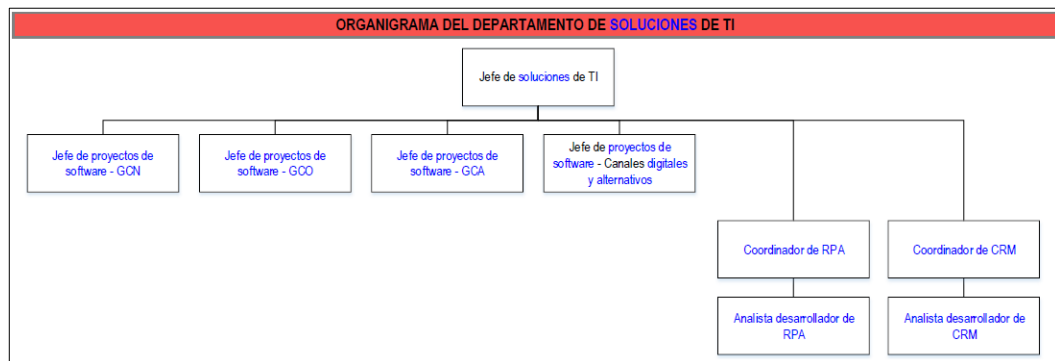


Fig 2: Organigrama del departamento de soluciones de TI.

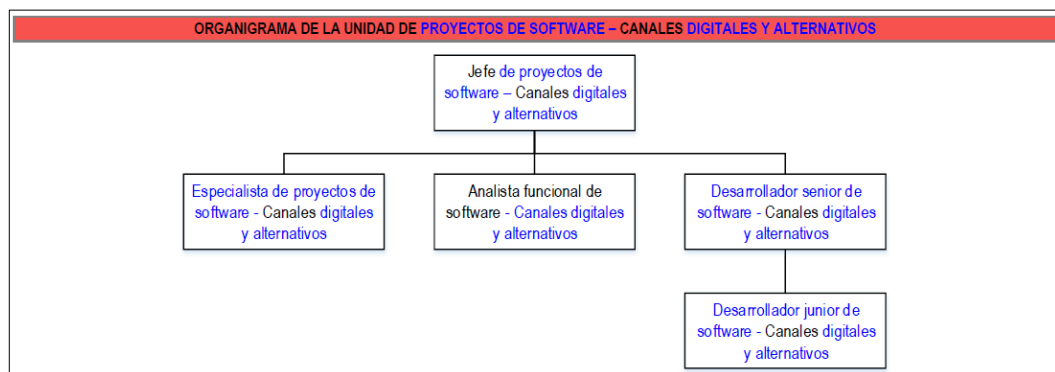


Fig 3: Organigrama de la Unidad de Proyectos de Software - Canales Digitales y Alternativos.

CAPÍTULO II: TRAYECTORIA PROFESIONAL

2.1. Puesto actual

- a) Desarrollador senior de software de canales Digitales y Alternativos.

Tiempo: 06 enero 2025 – Actualidad

Empresa: Caja Municipal de Ica

Funciones:

Realizar pruebas unitarias de verificación e implementación de las soluciones tecnológicas y proyectos informáticos de canales digitales y alternativos, estableciendo mecanismos de control, a fin de asegurar la integridad y veracidad de los datos procesados y los medios de recuperación de errores durante su funcionamiento.

- Realizar los flujos de procesos para el desarrollo y mantenimiento de las aplicaciones de canales digitales y alternativos.
- Analizar los requerimientos, incidencias y problemas diarios en las soluciones tecnológicas de canales digitales y alternativos que se encuentran en producción para gestionar la solución.
- Analizar las soluciones tecnológicas de canales digitales y alternativos, en funcionamiento y en desarrollo, a fin de proponer optimizaciones y rediseños, en coordinación con las áreas usuarias responsables del proceso, teniendo en cuenta el avance tecnológico, las necesidades operativas y los resultados que se deseen alcanzar.
- Proponer nuevas tecnologías que permitan asegurar y optimizar las soluciones tecnológicas de canales digitales y alternativos.
- Realizar el levantamiento de información para el análisis, diseño, modelamiento de datos y elaboración de prototipos de los las soluciones tecnológicas y proyectos informáticos de canales digitales y alternativos.
- Resolver las incidencias y sugerencias reportadas en las pruebas realizadas en el aseguramiento y control de calidad.
- Elaborar informes sobre el avance y calidad del desarrollo y de los entregables de los proyectos informáticos de canales digitales y alternativos.

- Apoyar en la gestión integral (alcance, calidad, comunicaciones, involucrados, recursos humanos, tiempos, riesgos, adquisiciones y costos) de los proyectos informáticos de canales digitales y alternativos.
- Realizar el desarrollo y mantenimiento de las soluciones tecnológicas de canales digitales y alternativos, con base en la metodología de desarrollo de software.
- Apoyar en la supervisión del cumplimiento de la metodología de desarrollo de software en todo el ciclo de construcción del producto (análisis, diseño, desarrollo, pruebas e implementación).
- Realizar el pase de los paquetes de software al personal de calidad de software para que se realicen las pruebas.
- Plantear propuestas de mejora en la calidad de los datos, a fin de optimizar su explotación.
- Plantear mejoras en la arquitectura de los sistemas, estándares de desarrollo y en la metodología de gestión de proyectos.
- Elaborar y actualizar los manuales técnicos de las soluciones tecnológicas de canales digitales y alternativos.
- Supervisar el desarrollo de las soluciones tecnológicas de canales digitales y alternativos, que efectúe el desarrollador junior de software.

2.2. Experiencias laborales anteriores

a) Analista Programador de Canales electrónicos.

Tiempo: 01 abril 2024 – 05 enero 2025

Empresa: Caja Municipal de Ica

Funciones:

- Realizar pruebas unitarias de verificación e implementación de los sistemas y proyectos informáticos, estableciendo mecanismos de control, a fin de asegurar la integridad y veracidad de los datos procesados y los medios de recuperación de errores durante su funcionamiento.
- Realizar los flujos de procesos para el desarrollo y mantenimiento de aplicaciones.
- Analizar los requerimientos, incidencias y problemas diarios en los sistemas informáticos que se encuentran en producción para gestionar la solución.

- Analizar los sistemas informáticos en funcionamiento y en desarrollo, a fin de proponer optimizaciones y rediseños en coordinación con las áreas usuarias responsables del proceso, teniendo en cuenta el avance tecnológico, las necesidades operativas y los resultados que se quieran alcanzar.
- Realizar el levantamiento de información para el análisis, diseño, modelamiento de datos y elaboración de prototipos a nivel de desarrollo de los sistemas y proyectos informáticos a desarrollarse.
- Proponer nuevas tecnologías que permitan asegurar y optimizar los sistemas informáticos.
- Apoyar en el desarrollo y mantenimiento de los sistemas y proyectos informáticos asignados a su unidad, cumpliendo los lineamientos y estándares establecidos.
- Apoyar en el cumplimiento de la metodología en todo el ciclo de construcción del producto (análisis, diseño, desarrollo, pruebas e implementación).
- Apoyar en la gestión integral, definición de objetivos, alcance, calidad, comunicaciones, involucrados, recursos, tiempos, riesgos, adquisiciones y costos de los proyectos informáticos.
- Elaborar informes sobre el avance y la calidad del desarrollo y de los entregables.
- Supervisar el desarrollo de las aplicaciones informáticas realizadas por el asistente programador de canales electrónicos.
- Realizar el pase de los paquetes de software al tester de calidad para que se realicen las pruebas.
- Apoyar en la supervisión del cumplimiento de los lineamientos y estándares establecidos para el diseño y desarrollo de sistemas informáticos.
- Elaborar y actualizar los manuales técnicos de los sistemas informáticos.

b) Asistente Programador de Canales electrónicos.

Tiempo: 01 agosto 2023 – 31 marzo 2024

Empresa: Caja Municipal de Ica

Funciones:

- Realizar pruebas unitarias de verificación e implementación de los sistemas y proyectos informáticos, estableciendo mecanismos de control, a fin de asegurar la integridad y veracidad de los datos procesados y los medios de recuperación de errores durante su funcionamiento.
- Desarrollar e implementar los sistemas y proyectos informáticos asignados y requeridos por las áreas usuarias, cumpliendo los lineamientos y estándares establecidos.
- Definir las especificaciones técnicas que soporten los requerimientos del usuario en base al análisis funcional.
- Realizar el análisis, diseño y desarrollo del producto basado en la metodología en todo el ciclo de construcción del producto.
- Proponer optimizaciones, cambios y correcciones a los sistemas informáticos que se encuentren en desarrollo, conforme a la evaluación de su operatividad y efectividad.
- Atender los requerimientos, incidencias y problemas que surjan en las pruebas de las aplicaciones desarrolladas, en la conversión de datos y las que sean reportadas por los usuarios.
- Realizar la ejecución del proyecto para el desarrollo del producto basado en lo establecido en el ERS.
- Elaborar informes sobre el avance del desarrollo de los proyectos informáticos.
- Realizar el pase de los paquetes de software al tester de calidad para que se realicen las pruebas.
- Elaborar y actualizar los manuales técnicos de los sistemas informáticos.

c) Asistente Programador de Canales electrónicos – Locación de Servicios.

Tiempo: 01 abril 2022 – 31 julio 2023

Empresa: Caja Municipal de Ica

Funciones:

- Realizar pruebas unitarias de verificación e implementación de los sistemas y proyectos informáticos, estableciendo mecanismos de control, a fin de asegurar la integridad y veracidad de los datos procesados y los medios de recuperación de errores durante su funcionamiento.

- Desarrollar e implementar los sistemas y proyectos informáticos asignados y requeridos por las áreas usuarias, cumpliendo los lineamientos y estándares establecidos.
- Definir las especificaciones técnicas que soporten los requerimientos del usuario en base al análisis funcional.
- Realizar el análisis, diseño y desarrollo del producto basado en la metodología en todo el ciclo de construcción del producto.
- Proponer optimizaciones, cambios y correcciones a los sistemas informáticos que se encuentren en desarrollo, conforme a la evaluación de su operatividad y efectividad.
- Atender los requerimientos, incidencias y problemas que surjan en las pruebas de las aplicaciones desarrolladas, en la conversión de datos y las que sean reportadas por los usuarios.
- Realizar la ejecución del proyecto para el desarrollo del producto basado en lo establecido en el ERS.
- Elaborar informes sobre el avance del desarrollo de los proyectos informáticos.
- Realizar el pase de los paquetes de software al tester de calidad para que se realicen las pruebas.
- Elaborar y actualizar los manuales técnicos de los sistemas informáticos.

CAPÍTULO III: APLICACIÓN PROFESIONAL

3.1. Metodología de implementación

La implementación de la plataforma Cipher Web se desarrolló bajo un enfoque ágil, aplicando la metodología Scrum para organizar las actividades en sprints y garantizar entregas incrementales. Se incorporaron prácticas de DevSecOps, lo que permitió integrar la seguridad en cada fase del ciclo de vida del software.

Las etapas del proyecto se estructuraron de la siguiente manera:

a) Planeación:

- ✓ Análisis de requerimientos funcionales y no funcionales.
- ✓ Identificación de riesgos asociados al manejo de datos sensibles.
- ✓ Definición de objetivos: protección de información confidencial y cumplimiento de PCI DSS.
- ✓ Elaboración del plan de trabajo y cronograma ágil con sprints de dos semanas.

b) Desarrollo

- ✓ Diseño de la arquitectura distribuida de la solución.
- ✓ Configuración de entornos en Docker y orquestación en OpenShift.
- ✓ Codificación del backend en Java 11 con Spring Boot, utilizando Maven para la gestión de dependencias.
- ✓ Creación de microservicios con RabbitMQ para el intercambio de mensajes y trazabilidad de eventos.
- ✓ Implementación de JWT con autenticación de doble factor para accesos seguros.
- ✓ Control de versiones en Bitbucket y despliegues automatizados mediante Jenkins.

c) Implementación

- ✓ Instalación de la plataforma en los servidores internos de la Caja Municipal de Ica.
- ✓ Configuración de base de datos en SQL Server 2014.
- ✓ Integración con módulos de auditoría, notificaciones y mantenimiento de plantillas.

- ✓ Pruebas de interoperabilidad con sistemas existentes de la Gerencia de Tecnología de la Información.
- d) Validación
- ✓ Ejecución de pruebas unitarias, de integración y de seguridad automatizadas.
 - ✓ Auditoría interna para verificar cumplimiento de PCI DSS.
 - ✓ Validación de tiempos de respuesta en operaciones de tokenización/des-tokenización.
 - ✓ Capacitación al personal del área de TI en el uso de la plataforma.
- e) Resultados
- ✓ Reducción significativa del riesgo de exposición de datos sensibles.
 - ✓ Cumplimiento de los principales requisitos del estándar PCI DSS.
 - ✓ Optimización de tiempos de auditoría y de gestión de datos en procesos críticos.
 - ✓ Mejora en la confianza de los clientes al reforzar la seguridad digital de la institución.

3.2. Arquitectura consolidada de la plataforma

La arquitectura final de CIPHER Web se diseñó en un modelo distribuido de microservicios con los siguientes componentes integrados:

- Capa de Presentación: Interfaz web intuitiva para los usuarios autorizados.
- Capa de Negocio: Servicios en Spring Boot para gestión de tokenización y des-tokenización.
- Broker (RabbitMQ): Comunicación asincrónica entre módulos.
- Capa de Seguridad: Autenticación JWT, doble factor y registros de auditoría.
- Capa de Datos: SQL Server, protegida con tokenización y cifrado.
- Orquestación en OpenShift: Despliegue escalable y seguro de contenedores.
- Automatización con Jenkins: CI/CD para despliegues automatizados y control de calidad.

3.3. Descripción del programa laboral

En el presente estudio, a partir de mi experiencia profesional en la Caja Municipal de Ahorro y Crédito de Ica S.A., se identificaron diversas situaciones vinculadas con la gestión de la información del banco de datos de clientes, con especial énfasis en el cumplimiento de las normas de seguridad para la protección de datos de tarjetas de pago. Frente a la situación descrita, se dio la facultad de gestionar y participar en la implementación de una plataforma web, la cual conto con las siguientes características:

- **Cipher Web:**

Es un aplicativo web, orientada a la protección de información sensible de los clientes de Caja Municipal de Ahorro y Crédito de Ica S.A, gracias a la tokenización de datos de información sensible, se logra garantizar su confidencialidad y protección contra accesos no autorizados.

El aplicativo web dispone de una interfaz de usuario interactiva y sencilla de forma que pueda ser utilizado por los usuarios de manera ágil.

- **Seguridad:**

Cipher Web está desarrollada con las medidas de seguridad apropiadas que servirán de base para proyectos similares.

El aplicativo garantiza la autenticación sólida de los usuarios para asegurarse de que solo aquellos autorizados puedan acceder a la información sensible. Esto implica el uso de contraseñas robustas y encriptación de datos durante la transmisión.

El aplicativo mantiene registros de todas las acciones realizadas por los usuarios, incluyendo el acceso, modificaciones y actualizaciones de información. Estos registros permiten realizar un seguimiento de la actividad y facilitan la detección de cualquier actividad sospechosa, violación de seguridad o fallas del sistema.

- **Disponibilidad de la Plataforma:**

El sistema Cipher Web tiene la capacidad para estar siempre accesible y funcionando correctamente 24 horas al día 7 días a la semana, permitiendo a los usuarios autorizados realizar la tokenización o des-tokenización de manera continua y sin interrupciones según sea conveniente.

3.4. Objetivo del proyecto tecnológico

El proyecto tuvo como objetivo implementar el proceso de tokenización en la base de datos de desarrollo de la CMAc ICA, permitiendo que el equipo de Producción de Tecnología de la Información pueda gestionarlo de manera eficiente, rápida y segura. Esta iniciativa contribuyó al fortalecimiento tecnológico de la entidad, alineándose con los estándares PCI-DSS para garantizar la protección de los datos sensibles de los clientes.

3.5. Participación:

Durante el desarrollo del proyecto Cipher Web en la Caja Municipal de Ahorro y Crédito de Ica S.A., se gestionó e implementó un conjunto de herramientas y tecnologías avanzadas para garantizar la seguridad, disponibilidad y eficiencia en la protección de datos sensibles. La combinación de metodologías ágiles, integración de procesos seguros y una infraestructura robusta permitió optimizar la operatividad del equipo de Producción de Tecnología de la Información.

Herramientas Utilizadas

Para asegurar una implementación eficiente y segura, se emplearon diversas tecnologías y herramientas clave en el desarrollo del proyecto:

- **Base de datos y servidores:** Se utilizó SQL Server 2014 como sistema de gestión de bases de datos, asegurando un alto nivel de confiabilidad y eficiencia en el manejo de información crítica. Además, se implementó Docker for Windows para la contenerización de servicios, lo que permitió una mayor portabilidad y facilidad en el despliegue en diversos entornos.
- **Infraestructura:** Se empleó OpenShift como plataforma para la orquestación de contenedores, facilitando una administración automatizada y escalable de los recursos en entornos de nube.
- **Control de versiones y gestión de código:** Se utilizó Bitbucket como herramienta centralizada para la administración del código fuente, permitiendo el control de versiones, la revisión de modificaciones y la colaboración en el desarrollo.
- **Generación de reportes:** SQL Server Reporting Services (SSRS) fue empleado para la creación y distribución de informes, optimizando el proceso de toma de decisiones basado en datos.
- **Seguridad y redes:** Se adoptaron medidas de seguridad, como una red interna protegida, firewall y software antivirus, con el objetivo de asegurar la integridad y disponibilidad de los sistemas.

- **Autenticación y seguridad:** Se implementó JWT (JSON Web Token) como método de autenticación segura basado en tokens, complementándolo con autenticación de doble factor para fortalecer la protección de los accesos.
- **Backend:** Se empleó Java 11 con Spring Boot como framework principal, acompañado de Maven para la gestión de dependencias y la optimización del proceso de construcción del software.
- **Entorno de desarrollo:** IntelliJ IDEA fue la herramienta principal para la codificación y depuración del software, optimizando la productividad y facilitando la implementación de funcionalidades complejas.
- **Automatización y despliegue:** Jenkins fue empleado para la automatización de procesos de integración y entrega continua (CI/CD), mejorando la eficiencia en el despliegue y mantenimiento de la solución.

Componentes de Arquitectura

La solución implementada se basó en una arquitectura distribuida compuesta por varios componentes clave:

- **Gates:** Proxy inverso encargado de la distribución de rutas y conexiones, optimizando el tráfico y mejorando la seguridad del sistema.
- **Bus de eventos:** Se implementó un mecanismo de eventos y colas mediante RabbitMQ, permitiendo la comunicación eficiente y desacoplada entre microservicios.
- **Notificaciones:** Se desarrolló un módulo para el envío de alertas y notificaciones en tiempo real, asegurando la rápida respuesta ante eventos críticos.
- **Trazabilidad:** Se incorporó un sistema de monitoreo y trazabilidad de microservicios, facilitando la auditoría y el análisis del comportamiento de la plataforma.
- **Procesamiento en tiempo real:** Se integró Firebase para la validación y autenticación de transacciones en tiempo real, mejorando la seguridad y experiencia del usuario.

Gestión y Despliegue

Para garantizar un desarrollo ágil, seguro y automatizado, se adoptaron las siguientes metodologías y prácticas:

- **Scrum:** Se implementó esta metodología ágil para la planificación y ejecución de sprints, asegurando entregas iterativas y mejoras continuas. Además, se utilizó Jira para la gestión eficiente de tareas y la coordinación del equipo de trabajo.
- **DevOps:** Se aplicaron procesos de integración y entrega continua (CI/CD) con Jenkins y Bitbucket, optimizando el despliegue y mantenimiento de la solución.
- **DevSecOps:** Se implementaron estrategias de seguridad en cada fase del ciclo de desarrollo, incorporando análisis de vulnerabilidades, escaneo de dependencias, pruebas de seguridad automatizadas y revisión de código seguro, lo que permitió mitigar riesgos desde la etapa de diseño hasta la implementación en producción.

Gracias a la integración de estas herramientas y metodologías, Cipher Web logró fortalecer la seguridad y eficiencia en la gestión de datos, alineándose con los estándares internacionales y mejorando significativamente la operatividad y productividad del equipo de Tecnología de la Información, lo que contribuyó al éxito del proyecto y al cumplimiento de los objetivos estratégicos de la organización.

3.6. Plataforma Cipher Web:



Fig 4: Modulo principal.

El módulo principal (Home) de la plataforma ofrece una interfaz intuitiva que permite gestionar el proceso de tokenización y des-tokenización de datos de manera eficiente. Se compone de los siguientes módulos clave:

- **Módulo de Procesamiento (Tokenización de Datos):** Encargado de transformar datos sensibles en tokens seguros, garantizando la protección de la información.
- **Módulo de Des-tokenización:** Permite revertir el proceso de tokenización cuando se requiere acceder a los datos originales de manera segura.

- **Módulo de Visualización:** Facilita el monitoreo y análisis de los datos procesados, proporcionando información relevante sobre las transacciones y el estado del sistema.

Esta estructura permite una gestión segura y controlada de la información sensible, cumpliendo con los estándares de seguridad y normativas aplicables.

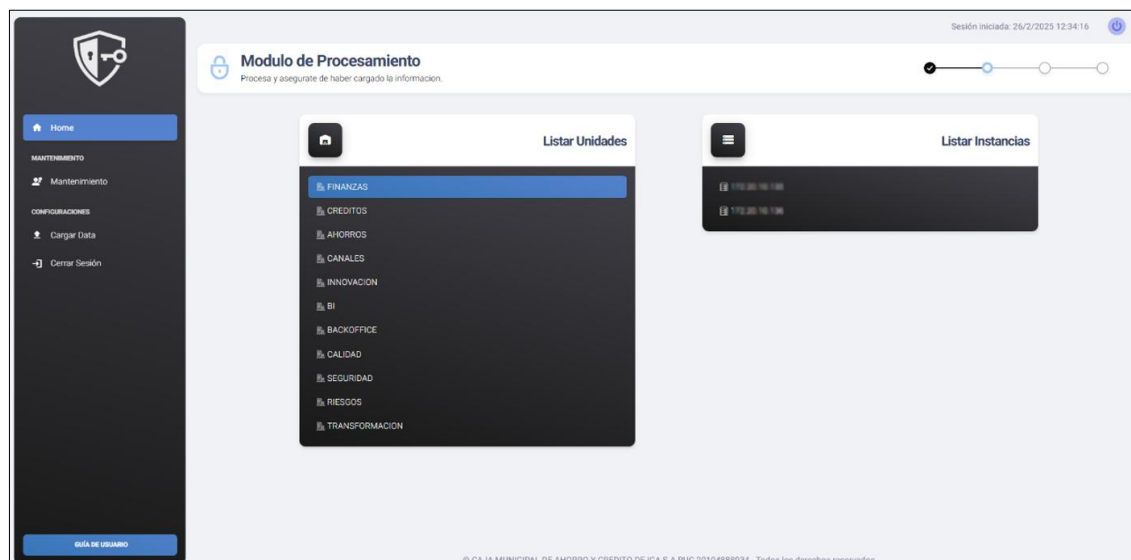


Fig 5: Modulo de Procesamiento.

Selección de Unidad:

- Al ingresar al módulo, el usuario visualiza una lista de unidades disponibles dentro del sistema.
- Cada unidad representa un conjunto de recursos asociados que pueden ser procesados en el sistema.
- Una vez seleccionada la unidad, el sistema carga y muestra las instancias de bases de datos disponibles dentro de ella.

Selección de Instancia de Base de Datos:

- Tras elegir una unidad, el usuario debe seleccionar una instancia de base de datos específica.
- La plataforma filtra y lista únicamente las instancias correspondientes a la unidad seleccionada.

Al confirmar la selección de la instancia, el sistema redirige a una nueva vista denominada “Seleccione la Bas de Datos”.

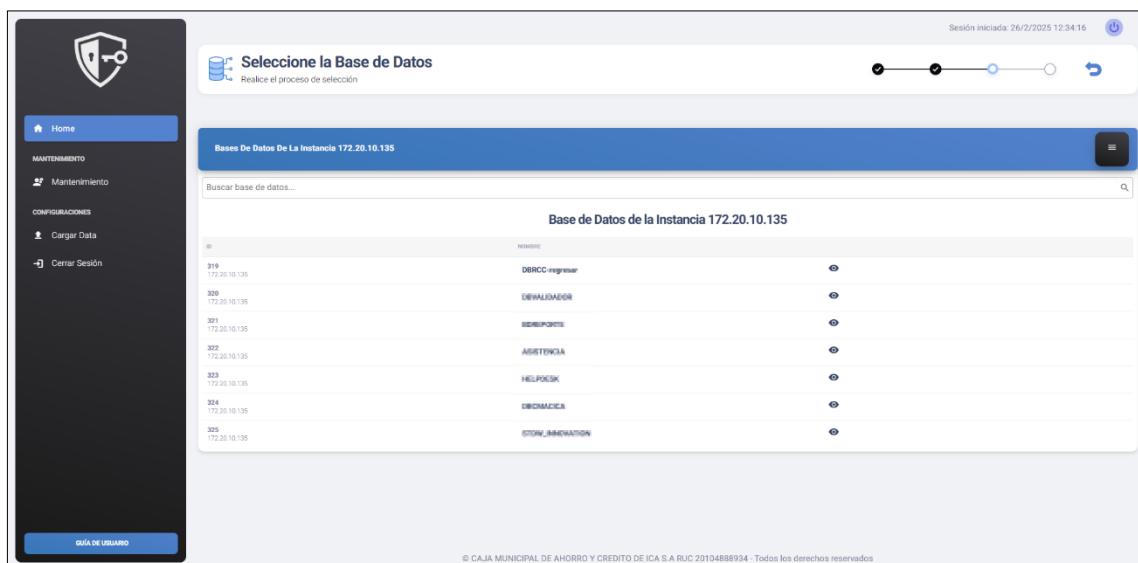


Fig 6: Modulo Selección de Base de datos.

Esta vista muestra los detalles de las bases de datos disponibles en la instancia seleccionada.

El usuario puede localizar una base de datos ya sea navegando en la lista o utilizando el buscador para filtrar por nombre u otros criterios.

Al seleccionar una base de datos, el sistema redirige a otra vista denominada "Plantillas de Procesos".

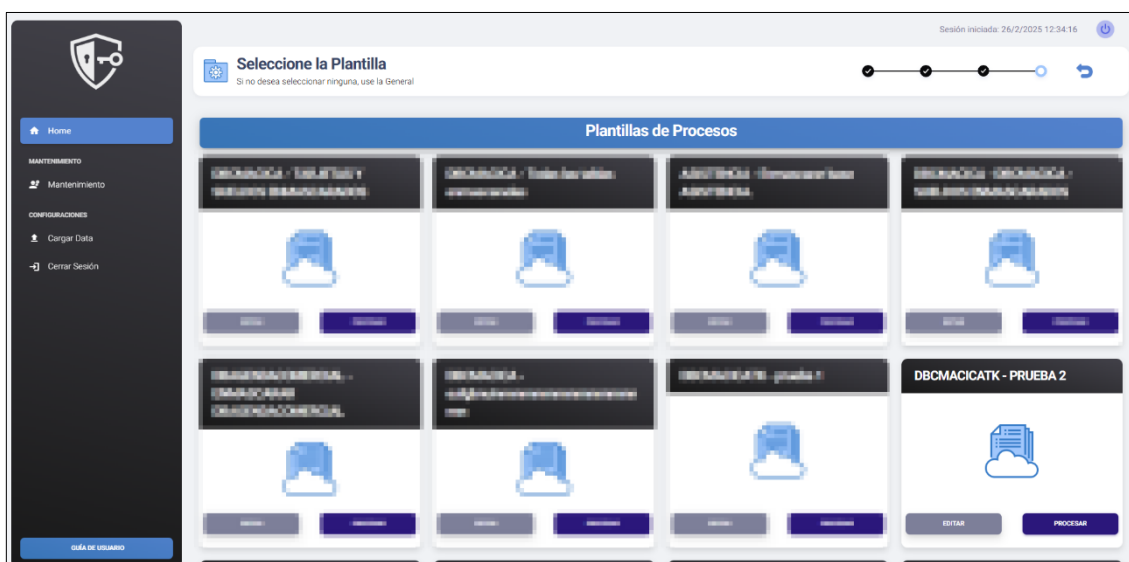


Fig 7: Módulo de Selección de plantillas.

Se muestran todas las plantillas configuradas previamente para procesos de tokenización o des-tokenización de datos.

Cada plantilla cuenta con dos opciones de acción:

Editar: Redirige a una nueva vista donde el usuario puede revisar y modificar las tablas y columnas configuradas en la plantilla.

Procesar: Inicia el proceso de tokenización o des-tokenización de datos basado en la configuración de la plantilla seleccionada.

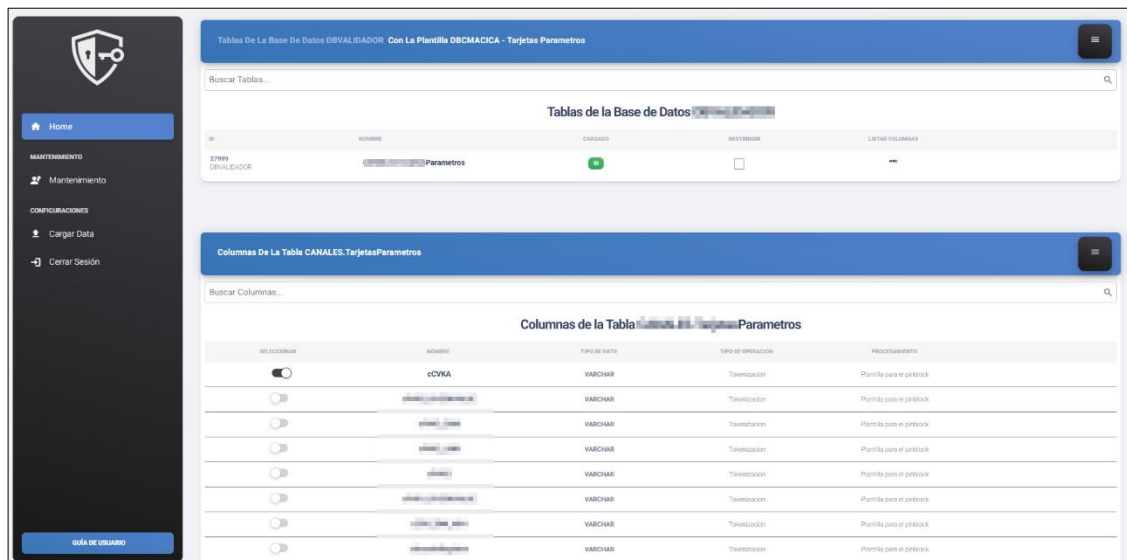


Fig 8: Módulo de Selección tablas y columnas.

Aquí se pueden visualizar todas las tablas y columnas que forman parte del proceso de tokenización o des-tokenización configurado en la plantilla.

El usuario tiene la opción de modificar la configuración antes de guardar los cambios y regresar a la vista de selección de plantilla.



Fig 9: Módulo de Mantenimiento.

Este módulo, permite gestionar y configurar los elementos clave del sistema de tokenización y des-tokenización, asegurando que los procesos se realicen de manera estructurada y eficiente.

a) Registro de Unidades:

Permite la creación y gestión de unidades dentro del sistema.

Cada unidad agrupa instancias de bases de datos relacionadas con los procesos de tokenización.

b) Registro de Instancias:

Facilita el alta, edición y eliminación de instancias de bases de datos dentro de cada unidad.

Las instancias son fundamentales para definir los entornos donde se ejecutarán los procesos.

c) Registro de Solicitudes de Tokenización o Des-tokenización:

Permite registrar y gestionar las solicitudes para procesar datos mediante tokenización o des-tokenización.

Se pueden consultar solicitudes en curso o finalizadas.

d) Mantenimiento de Plantillas de CipherTrust:

Administra las plantillas de seguridad utilizadas en la integración con CipherTrust, la solución de protección de datos.

Permite la configuración y actualización de los parámetros de cifrado y tokenización.

e) Mantenimiento de Plantillas de Procesamiento de Datos:

Gestiona las plantillas utilizadas en la tokenización y des-tokenización.

Define qué tablas y columnas serán procesadas en cada solicitud.

f) Obtener Base de Datos a Procesar:

Función que permite obtener y visualizar las bases de datos disponibles para tokenización/des-tokenización dentro de la Base de datos principal.

Facilita la selección de bases de datos en función de los criterios definidos.

g) Mantenimiento de Categorías de Tokenización:

Permite la gestión de las diferentes categorías de tokenización, clasificando los datos según su sensibilidad y reglas de procesamiento.

Estas categorías ayudan a aplicar políticas específicas a distintos tipos de información.



Fig 10: Modulo de Carga de información.

El Módulo de Carga de Información permite la incorporación de datos estructurados al sistema, asegurando que las unidades, instancias, bases de datos y tablas sean registradas correctamente para su posterior procesamiento en los módulos de tokenización y des-tokenización

Carga de Unidades e Instancias:

- ✓ Permite cargar y registrar unidades dentro del sistema.
- ✓ Asociar instancias de bases de datos a las unidades correspondientes.
- ✓ Garantiza que la relación entre unidades e instancias esté correctamente estructurada.

Carga de Bases de Datos por Instancia:

- ✓ Facilita la importación de bases de datos vinculadas a una instancia específica.
- ✓ Se listan las instancias disponibles y, al seleccionarlas, el sistema permite la carga de sus bases de datos.
- ✓ Verificación y validación de la estructura de las bases de datos antes de su registro.

Carga de Tablas:

- ✓ Una vez registradas las bases de datos, el sistema permite la carga de sus tablas asociadas.
- ✓ Se pueden definir criterios específicos para la carga de tablas según su relevancia en los procesos de tokenización o des-tokenización.
- ✓ Posibilidad de automatizar la detección de tablas dentro de la base de datos seleccionada.

CAPÍTULO IV: APORTES A LA INSTITUCIÓN

La implementación de una plataforma de tokenización en la Caja Municipal de Ahorro y Crédito de Ica S.A. traerá diversos beneficios estratégicos, operativos y de cumplimiento normativo, fortaleciendo la seguridad de la institución y optimizando sus procesos internos. A continuación, se detallan los principales aportes:

4.1. Mejora en la Seguridad de los Datos Sensibles

- Indicador: Reducción del 75 % en la exposición de datos sensibles en sistemas internos, al reemplazar la información real por tokens.
- Impacto: Se minimizó la probabilidad de accesos no autorizados y filtraciones de información financiera.

4.2. Cumplimiento de Normativas Internacionales

- Indicador: 100 % de cumplimiento alineados con el estándar PCI DSS en el ámbito de protección de datos de tarjeta.
- Impacto: Se logró una alineación con la normativa, reduciendo riesgos de sanciones económicas y fortaleciendo la reputación institucional.

4.3. Reducción de Costos Operativos y de Seguridad

- Indicador: Disminución del 30 % en costos asociados al cifrado tradicional en múltiples puntos del sistema.
- Impacto: Optimización de la infraestructura tecnológica y reducción de gastos recurrentes en seguridad.

4.4. Optimización de procesos internos

- Indicador: Reducción del 40 % en los tiempos de auditoría de datos financieros, gracias a la trazabilidad de los procesos de tokenización.
- Indicador: Disminución en un 25 % del tiempo requerido para la gestión de solicitudes internas de datos sensibles.

4.5. Fortalecimiento de la Confianza de los Clientes

- Indicador: Incremento del 20 % en la percepción positiva de los clientes respecto a la seguridad de sus transacciones (medido a través de encuestas internas).
- Impacto: Aumento en la fidelización de clientes y atracción de nuevos usuarios.

4.6. Resiliencia ante Ataques Cibernéticos

- Indicador: Cero incidentes críticos de seguridad reportados en los primeros seis meses posteriores a la implementación.
- Impacto: La institución fortaleció su capacidad de respuesta y recuperación frente a potenciales ataques, consolidando una cultura de prevención.

CONCLUSIONES

Tras el desarrollo e implementación de la plataforma Cipher Web en la Caja Municipal de Ahorro y Crédito de Ica S.A., se lograron resultados significativos que responden directamente a los objetivos planteados en la investigación:

1. Seguridad de los Datos Sensibles

La implementación del proceso de tokenización permitió reducir en un 75 % la exposición de información confidencial dentro de los sistemas internos. Esto fortaleció los mecanismos de protección frente a accesos no autorizados, fraudes y ciberataques, cumpliendo con el objetivo de mejorar la seguridad de la información.

2. Cumplimiento normativo

La solución alcanzó un 100 % de alineación con el estándar PCI DSS en el ámbito de protección de datos de tarjeta, garantizando que los procesos de gestión cumplan con normativas internacionales. Este resultado asegura la integridad de las operaciones, previene sanciones regulatorias y consolida la conformidad con los más altos estándares de seguridad.

3. Reducción de Costos Asociados a la Seguridad

Gracias a la eliminación de múltiples esquemas de cifrado tradicionales, se redujeron en un 30 % los costos asociados a la gestión de seguridad. Este resultado responde al objetivo de optimizar recursos financieros y tecnológicos en la institución.

4. Optimización de procesos internos

El tiempo requerido para auditorías y revisiones de seguridad disminuyó en un 40 %, mientras que la gestión de solicitudes de datos se agilizó en un 25 %. Estos logros cumplen con el objetivo de optimizar los procesos internos relacionados con la administración de datos sensibles.

5. Fortalecimiento de la Confianza de los Clientes

A través de encuestas internas, se evidenció un incremento del 20 % en la percepción positiva de los clientes respecto a la seguridad de sus transacciones. Este resultado confirma el cumplimiento del objetivo de mejorar la confianza en los servicios financieros digitales de la Caja Municipal de Ahorro y Crédito de Ica S.A.

RECOMENDACIONES

Tras la implementación de la plataforma de tokenización en la Caja Municipal de Ahorro y Crédito de Ica S.A., se presentan las siguientes recomendaciones para maximizar sus beneficios y asegurar su sostenibilidad a largo plazo:

1. Fortalecer la Cultura de Seguridad institucional

Desarrollar programas permanentes de capacitación al personal en buenas prácticas de ciberseguridad, manejo de datos sensibles y uso adecuado de la plataforma Cipher Web. Esto permitirá reducir riesgos de errores humanos y fortalecer la protección de la información.

2. Transferencia de conocimiento

Elaborar y entregar manuales técnicos, guías de usuario y protocolos de operación de la plataforma, de manera que el personal actual y futuro pueda operar el sistema de forma eficiente. Asimismo, implementar programas de inducción para los nuevos colaboradores del área de TI, garantizando la continuidad del conocimiento.

3. Monitoreo y auditorías periódicas

Establecer un plan de auditorías internas y externas que permitan validar el cumplimiento continuo del estándar PCI DSS, así como identificar posibles vulnerabilidades. Complementariamente, implementar herramientas de monitoreo en tiempo real para detectar amenazas de manera proactiva.

4. Actualización y escalabilidad de la plataforma

Mantener un plan de actualizaciones periódicas del software y hardware asociados a la solución, con el objetivo de garantizar su compatibilidad con las nuevas versiones del estándar PCI DSS y las tendencias en seguridad digital. Evaluar la posibilidad de escalar la plataforma hacia otros procesos financieros.

5. Respaldo y recuperación ante desastres

Optimizar las estrategias de respaldo y recuperación ante desastres (DRP) mediante la incorporación de copias de seguridad cifradas, pruebas periódicas de restauración y almacenamiento en entornos altamente seguros. Con ello, la organización se mantiene alineada a las mejores prácticas internacionales de continuidad del negocio.

6. Innovación en Seguridad Digital

Explorar tecnologías emergentes como blockchain para trazabilidad de transacciones y inteligencia artificial para la detección temprana de fraudes. Estas innovaciones contribuirán a mantener a la institución a la vanguardia en ciberseguridad.

REFERENCIAS BIBLIOGRÁFICAS

- [1] La tokenización de activos: El futuro de las finanzas", Escuela de Negocios Europea de Barcelona (ENEB), 5 de noviembre de 2024. [En línea]. Disponible en: <https://eneb.es/tokenizacion-de-activos/>
- [2] La tokenización de activos: Un instrumento de financiamiento para proyectos inmobiliarios en Perú", Repositorio de ESAN, 10 de octubre de 2024. [En línea]. Disponible en: <https://repositorio.esan.edu.pe/items/0de59b3a-a2cb-4638-ac73-2fba8601131a>
- [3] Tokenización en PCI DSS: FAQ y diseño básico de una solución con AWS", *ISEC Auditors Blog*, marzo 2019. [En línea]. Disponible en: <https://blog.isecauditors.com/2019/03/tokenizacion-en-pci-dss-faq-y-diseno-basico-solucion-con-aws.html>
- [4] Promoviendo los pagos digitales en Perú: El Banco Central de Reserva del Perú (BCRP) ha estado investigando la posibilidad de implementar una Moneda Digital de Banco Central (CBDC), definida como un pasivo digital del banco central que puede ser usado como dinero por el público en general. Disponible en: <https://www.bcrp.gob.pe/docs/Sistema-Pagos/cbdc/cbdc-presentacion.pdf>
- [5] El Futuro del Tratamiento Seguro de Datos: Este artículo discute cómo la tokenización ayuda a las empresas peruanas a cumplir con normativas de protección de datos como PCI DSS. Al reemplazar datos sensibles por tokens, las organizaciones pueden minimizar la exposición de información confidencial. Disponible en: <https://innowise.com/es/blog/data-tokenization/>
- [6] Tokenización de datos: qué es y por qué es importante: Binance Academy explica el proceso de convertir datos confidenciales en tokens, destacando su importancia en la mejora de la seguridad y privacidad de la información. Disponible en: <https://academy.binance.com/es/articles/what-is-data-tokenization-and-why-is-it-important>
- [7] PCI Security Standards Council, "PCI DSS v4.0.1 released," PCI Perspectives Blog, 11 de junio de 2024. [En línea]. Disponible en: <https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1>
- [8] PCI Security Standards Council, "Important Updates Announced for Merchants Validating to SAQ A" PCI Perspectives Blog, 30 de enero de 2025. [En línea]. Disponible en: <https://blog.pcisecuritystandards.org/important-updates-announced-for-merchants-validating-to-self-assessment-questionnaire-a>
- [9] Amazon Web Services, "Reduce and secure cardholder data with PCI solutions on AWS," AWS Solutions Library, 2025. [En línea]. Disponible en: <https://aws.amazon.com/es/solutions/guidance/tokenization-to-improve-data-security-and-reduce-audit-scope-on-aws/>

- [10] Google Cloud, “Asigna tokens a datos sensibles de titulares de tarjetas para PCI DSS” En este documento, se muestra cómo configurar un servicio de asignación de token para tarjetas de crédito y débito con acceso controlado en Cloud Run Functions. [En línea]. Disponible en: <https://cloud.google.com/architecture/tokenizing-sensitive-cardholder-data-for-pci-dss?hl=es-419>
- [11] Cybersource (Visa), “Reducir el alcance y los costos de PCI DSS con la tokenización” Product Documentation, 22 de agosto de 2022. [En línea]. Disponible en: <https://www.cybersource.com/en-us/blog/2022/reduce-pci-dss-scope-and-costs-with-tokenization.html>
- [12] Adyen, “Tokenización para pagos recurrentes” Adyen Docs, 2025. [En línea]. Disponible en: <https://docs.adyen.com/online-payments/tokenization/>
- [13] Stripe, “Introducción al cumplimiento PCI,” Stripe Docs, 2025. [En línea]. Disponible en: <https://stripe.com/es-us/guides/pci-compliance>
- [14] Mastercard, “Conexión de token MDES” Mastercard Developers / MDES, 2023. [En línea]. Disponible en: <https://developer.mastercard.com/mdes-token-connect/documentation/>
- [15] EMVCo, “EMV Payment Tokenisation Technical” Press Release, noviembre 2024. [En línea]. Disponible en: <https://www.emvco.com/emv-technologies/payment-tokenisation/>

ANEXOS



Fig 11: Seguimiento de actividades de personal a cargo.

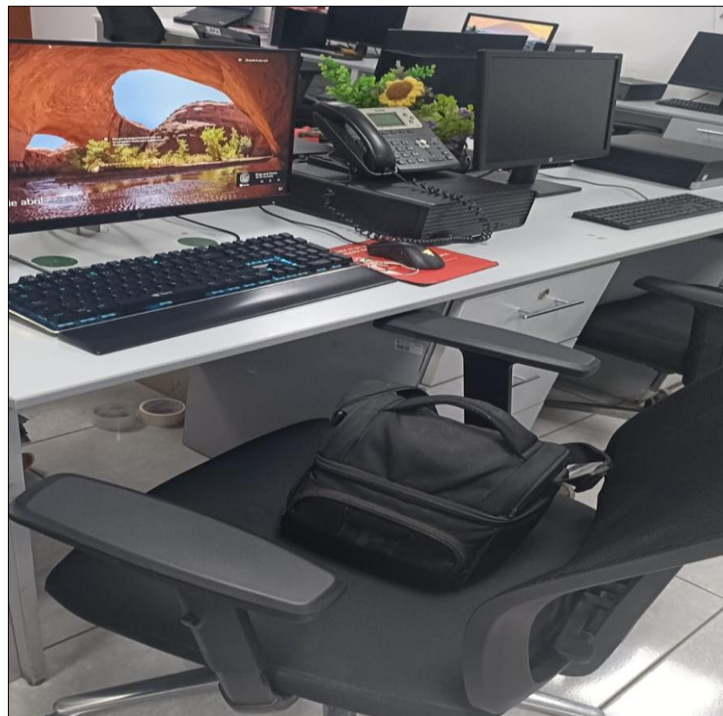


Fig 12: Estación de trabajo.



Fig 13: Equipo de la Gerencia de tecnología de información y comunicaciones.