UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

# Proceso de encriptación para la seguridad de la información en el Comando de Control Aeroespacial basado en ISO 27001

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**

**Ingeniero de Sistemas**


**AUTORES:**

Cabellos Dionicio, Jhojan Enoc (orcid.org/0000-0002-2747-0796)

Oliva Rivera, Mitchael Ever (orcid.org/0000-0002-3880-9433)

**ASESOR:**

Dr. Villaverde Medrado, Hugo (orcid.org/0000-0002-3802-4396)


**LÍNEA DE INVESTIGACIÓN:**

Sistema de Información y Comunicaciones

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2022

**Dedicatoria**

Dedicamos la presente tesis principalmente a Dios, por darnos la fuerza necesaria para culminar esta carrera.

A nuestros padres, por todo su amor y apoyo incondicional para incentivarnos a seguir adelante.

Y, finalmente, a nuestros compañeros que estuvieron constantemente compitiendo sanamente para ser los mejores.

**Agradecimiento**

Quisiéramos agradecer a nuestro asesor, el Dr. Hugo Villaverde Medrado, quien nos supo guiar de principio a fin para desarrollar correctamente el presente trabajo. Sus consejos fueron siempre muy útiles para aclarar las ideas y poder continuar. Muchas gracias por brindarnos su tiempo cuando más lo requeríamos.

También quisiera agradecer a nuestros docentes, su conocimiento y experiencia nos sirvió muchísimo para tener un panorama amplio de la carrera, muchas gracias por su paciencia y dedicación.

Finalmente, a todos nuestros compañeros de clase que día a día, con mucha dedicación y muchas horas sin dormir se esforzaban para continuar y lograr el objetivo principal, culminar nuestra grandiosa carrera.

**Índice de contenidos**

## Índice de tablas

## Índice de figuras

## RESUMEN

Esta investigación tiene como objetivo general determinar en qué medida el proceso de encriptación influye en la seguridad de la información en el comando de control aeroespacial.

Es de tipo aplicado y enfoque cuantitativo, como también de diseño preexperimental. La población contada fue de 56 interacciones y muestra de 49 interacciones, esta muestra se sometió para el recojo de información referido a nuestras variables de investigación mensajes cifrados, porcentaje de disponibilidad de la información y porcentaje de confidencialidad de la información, usando fichas de registro como instrumento para el pre – test y post – test.

En cuanto a los resultados, se aplica la prueba de normalidad Shapiro – Wilk, resultando un valor de significancia de 0.004, 0.002, 0.001 que indica una distribución no normal de los datos de los 3 indicadores respectivamente. De acuerdo a ello se aplica la prueba no paramétrica de Wilcoxon obteniendo un valor de significancia de 0.001 para los 3 indicadores permitiendo así rechazar las Ho y aceptamos las Ha. Teniendo estos resultados se concluye de manera general que el proceso de encriptación tiene una influencia positiva en la seguridad de la información en el comando de control aeroespacial.



Palabras Clave: Proceso de encriptación, seguridad de la información, mensajes cifrados.

## ABSTRACT

The general objective of this investigation is to determine to what extent the encryption process influences the information security in the aerospace control command.

It is of an applied type and a quantitative approach, as well as a pre-experimental design. The counted population was 56 interactions and a sample of 49 interactions, this sample was submitted for the collection of information referring to our research variables encrypted messages, percentage of information availability and percentage of information confidentiality, using registration sheets as instrument for pre-test and post-test.

Regarding the results, the Shapiro - Wilk normality test is applied, resulting in a significance value of 0.004, 0.002, 0.001, which indicates a non-normal distribution of the data of the 3 indicators respectively. Accordingly, the Wilcoxon non-parametric test is applied, obtaining a significance value of 0.001 for the 3 indicators, thus allowing us to reject the Ho and accept the Ha. Having these results, it is generally concluded that the encryption process has a positive influence. in information security at the aerospace control command.



Keywords: Encryption process, information security, encrypted messages.

# I. INTRODUCCIÓN

La demanda de programas informáticos aumentó drásticamente en los últimos años en las instituciones públicas y privadas. Esto ha llevado a un aumento de los requisitos de desarrollo de software, que ahora incluyen otros factores no considerados en los métodos tradicionales, como la entrega temprana, la mejora continua, la flexibilidad y la adaptabilidad al cambio, la medición de la cantidad y la duración de cada proceso y otros. Por ello, en los últimos años, las empresas han adoptado metodologías o marcos ágiles para crear software que produzca resultados inmediatos, con mejor calidad y, lo más importante, que cumpla con los requisitos del cliente, lo que se ha convertido en un factor crítico de éxito para las empresas (Capraro y Tosetti, 2020, p. 6).

El espacio aéreo ha cambiado mucho en los últimos años con la llegada de aviones más potentes y eficaces. El desarrollo de las tecnologías de la información y la comunicación (en adelante TIC) en el ámbito de la seguridad nacional ha obligado a todos los Estados a buscar cada vez más oportunidades para mejorar sus sistemas de defensa y potenciar su ciberseguridad, ya que cuando se trata de problemas con otros Estados, la información significa poder (Muñoz, Díaz y Gallego, 2020, p. 2).

En el caso del Perú, según la Ley Básica de Modernización de las Fuerzas Armadas, Decreto Ley Nº 1142 del 11/12/2012, la modernización consiste en promover la investigación y el desarrollo tecnológico intensivo en las fuerzas armadas y la modernización continua de su logística militar para fortalecer la base científica y tecnológica creando nuevos sistemas y mejorando simultáneamente los existentes de acuerdo a las necesidades de corto, mediano y largo plazo (O'Connor, 2020, p. 78).

Por otro lado, la Ley de la Fuerza Aérea del Perú, según el Decreto Ley Nº 1139 del 09/12/2012, señala que la misión principal de la Fuerza Aérea es desarrollar la investigación académica científica y tecnológica en materia aeroespacial y realizar actividades de capacitación, especialización, perfeccionamiento, mantenimiento y equipamiento del componente aeroespacial de las fuerzas armadas, en concordancia con los objetivos y políticas de seguridad y defensa nacional (Delgado, 2019, párr. 15).

Las organizaciones se esfuerzan constantemente por mejorar la calidad del software introduciendo nuevos métodos de trabajo para aumentar la eficacia del ciclo de vida del software. En este contexto, Gaete et al. (2021, p. 288) sostienen que los métodos ágiles producen buenos resultados debido a su flexibilidad ante los requisitos y las decisiones que surgen durante el proceso de desarrollo de software, ya que pueden cambiar o evolucionar con el tiempo en función de las necesidades del proyecto. También destaca el método Scrum como uno de los más útiles.

Por otro lado, Ozdenizci (2021, p. 6) sostiene que las organizaciones utilizan enfoques rápidos en el proceso de desarrollo de software para garantizar la entrega incremental de versiones de programas consistentes, la entrega de características precisas y menos fallos en el proyecto. Las principales razones para utilizar métodos ágiles son acelerar el despliegue de software, mejorar la capacidad de hacer frente a los cambios de prioridades y aumentar la productividad. En ese escenario, en la fuerza aérea del Perú se ha detectado que los sistemas de comunicación e información pueden ser mejorados para facilitar la comunicación entre los distintos departamentos, asimismo se debe reforzar con nuevos protocolos de seguridad estas comunicaciones.

La seguridad de la información (SI) ya no es un tema reservado para audiencias técnicas, sino que se llegó a convertir en uno de los principales desafíos de gestión de la década actual. La aceleración de un primer enfoque digital a raíz de la COVID-19 ha aumentado aún más la necesidad de una mejor comprensión por parte de los tomadores de decisiones comerciales. Esto también se refleja en el creciente interés en el estándar de gestión de seguridad de la información ISO/IEC 27001 tanto en la academia como en la práctica. (Podrecca et al., 2020, p. 1).

Por ello, es necesario responder el siguiente problema general: ¿En qué medida el proceso de encriptación influye en la seguridad de la información en el Comando de Control Aeroespacial? De igual manera, tenemos las siguientes preguntas específicas: ¿En qué medida el proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial?, ¿En qué medida el proceso de encriptación incrementa la disponibilidad de la información en el comando de control aeroespacial?, ¿En qué medida el proceso de encriptación

incrementa la confidencialidad de la información en el comando de control aeroespacial?

Respecto a la perspectiva teórica la investigación se justifica debido a que la misma recabará conocimientos sobre la aplicación de la metodología SCRUM en sistemas de comunicación en entidades gubernamentales. Esto servirá a los futuros investigadores a tener un soporte teórico para la implementación de un nuevo sistema de comunicación, así como también mantener registros de esta metodología SCRUM. Desde el punto de vista metodológico es justificable porque proporciona herramientas y procedimientos efectivos y confiables para que los usen otros investigadores y sirve como precedente para nuevas direcciones de investigación. Desde el punto de vista práctico, ayudará a mejorar un sistema de comunicación que en algunos componentes de las fuerzas de seguridad del estado pueden estar fallando y de forma específica ayudará a la fuerza aérea, donde se sigue utilizando, protocolos desactualizados, por lo cual permitirá mejorar la comunicación y seguridad del sistema.

Según Mlkva (2016, p. 330), una de las herramientas que se puede aplicar a la mejora continua en una organización es la estandarización de procesos. Mejorar los esfuerzos de estandarización es un proceso interminable que reduce la variabilidad del proceso y mejora la calidad del producto y del proceso.

Las empresas necesitan este enfoque. La implementación de métodos ágiles es una de las principales tendencias en la reingeniería de procesos (Rasnacis & Berzisa, 2016, p. 44). Esto se debe principalmente a la facilidad de administrar la sobrecarga, es decir, el enfoque iterativo simplifica el proceso de entrega y validación y, además, permite la obtención inmediata de cambios dentro del alcance del proyecto.

Para la Fuerza Aérea del Perú, adoptar un enfoque ágil brindó la oportunidad de mejorar la calidad del proyecto, reducir los tiempos de entrega, optimizar los recursos y mejorar la motivación de la fuerza laboral.

Asimismo, este proyecto de investigación es de interés para el departamento, el cual se hace factible debido a:

Factibilidad Técnica:

El proyecto es técnicamente factible porque cuenta con los necesarios recursos técnicos, referentes a infraestructura, herramientas técnicas o software, acceso a datos e información necesaria. Además de la participación directa de técnicos en el campo de los sistemas, contribuirán activamente al desarrollo del proyecto.

Factibilidad Operativa:

El proyecto es operativamente viable gracias al apoyo de la comunidad informática y SINFA. Asimismo, el proyecto va a contar con la participación de muchas unidades operativas, para lo cual el sector de tecnologías de la información deberá brindar soluciones a la medida de sus necesidades. Por lo tanto, también va a permitir la apertura con el personal de dichas unidades para obtener la información necesaria y asegurar que los resultados de este proyecto tengan un nivel de calidad mínimamente aceptable.

Factibilidad Económica:

Económicamente el proyecto es factible porque la inversión que genera la implementación de un sistema por parte de una empresa de desarrollo asciende a $ 1770.00, explicado en el anexo 6, pero en este caso esa inversión económica se reduciría a 0 porque el personal encargado del proyecto con apoyo del área de informática del Comando de Control Aeroespacial realizará dicho trabajo y gracias a ello el presupuesto anual de la institución no se vería afectado.

Por otro lado, se tendrá como objetivo general: Determinar en qué medida el proceso de encriptación influye en la seguridad de la información en el comando de control aeroespacial. Asimismo, se tienen los siguientes objetivos específicos: Determinar en qué medida el proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial, determinar en qué medida el proceso de encriptación incrementa la disponibilidad de la información en el comando de control aeroespacial, determinar en qué medida el proceso de encriptación incrementa la confidencialidad de la información en el comando de control aeroespacial.

Finalmente, como hipótesis general: El proceso de encriptación influirá de manera positiva en la seguridad de la información en el comando de control aeroespacial. Asimismo, se tienen las siguientes hipótesis específicas: El proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial, el proceso de encriptación incrementará la disponibilidad de la información en el comando de control aeroespacial, el proceso de encriptación incrementará la confidencialidad de la información en el comando de control aeroespacial.

## II. MARCO TEÓRICO

Para elaborar esta investigación se procedió a tomar en cuenta investigaciones previas que sirvan como soporte o guía para realizar el estudio. En términos internacionales se tuvo a An (2022, p. 1) que en su artículo propone un sistema de comunicación de extremo a extremo con cifrado simétrico basado en redes antagónicas generativas convolucionales profundas para resolver el problema de seguridad de la transmisión en sistemas de comunicación inalámbricos basados en el aprendizaje de extremo a extremo. El sistema genera una clave mediante una red antagónica generativa convolucional profunda y la comparte con el transmisor y el receptor. Tanto el transmisor como el receptor están representados por redes neuronales convolucionales. Proponemos usar redes neuronales como puente para hacer una relación de mapeo irreversible entre el mensaje y la clave. El método propuesto logra una transmisión de mensajes más segura que los sistemas de comunicación de extremo a extremo con cifrado simétrico que utilizan claves generadas aleatoriamente. Las partes legítimas pueden establecer una transmisión segura en esta configuración, y el intruso ilegal no puede decodificar con precisión sin la clave.

Almomani (2022, p. 1) realizó un artículo indicando que las redes privadas virtuales (VPN) son un ejemplo de los servicios de comunicación encriptados que se usan comúnmente para eludir la censura y acceder a servicios bloqueados geográficamente. Este estudio realizó análisis de tráfico VPN y no VPN y desarrolló un sistema de clasificación basado en las nuevas técnicas de clasificadores de aprendizaje automático conocidas como aprendizaje de conjuntos de apilamiento. Los métodos utilizados para la clasificación de VPN y no VPN utilizan tres técnicas de aprendizaje automático: bosque aleatorio, red neuronal y máquina de vectores de soporte. Para evaluar el rendimiento del método propuesto, lo probó en un conjunto de datos que contenía 61 características. Los resultados del experimento prueban con precisión que los clasificadores del estudio diferencian entre tráfico VPN y no VPN. El nivel de precisión fue de aproximadamente 99% en la fase de entrenamiento y prueba.

Zawislak (2022, p. 128) en su artículo propone nuevos algoritmos de criptografía simétrica del Sistema Numérico de Residuos y su Forma Perfecta Modificada. De

acuerdo con el primer método, el texto cifrado se considera como un conjunto de residuos de los correspondientes conjuntos de módulos y el descifrado o la recuperación de números decimales a partir de sus residuos se lleva a cabo de acuerdo con el Teorema del Resto Chino. En este algoritmo, el bloque de texto plano se divide en sub-bloques que son más pequeños que el módulo correspondiente y sirven como restos al dividir algún número, que es un texto cifrado, por estos módulos. La recuperación de texto sin formato se basa en encontrar los restos de texto cifrado en los módulos correspondientes. Se investiga qué bitness y una cantidad de módulos se requieren para los sistemas de seguridad simétricos desarrollados para garantizar el mismo nivel de seguridad que la clave de mayor longitud del algoritmo AES. Se muestra que, con el aumento de los parámetros especificados, también aumenta la seguridad de los métodos desarrollados.

Del Pozo (2015, p. 533) en su artículo propuso un nuevo algoritmo de cifrado de baja complejidad para la comunicación de dispositivos móviles. A través del estudio, pruebas e implementación realizada, parece que el algoritmo de encriptación es óptimo para el servicio de mensajería instantánea. Indica que un método de encriptación para dispositivos móviles debe realizarse en una complejidad baja, el método propuesto realiza la tarea de cifrado y descifrado en poco tiempo, lo que optimiza la duración de la batería., también llega a un compromiso entre robustez y baja complejidad. El algoritmo se ejecuta en una complejidad polinómica cuadrática. Además, al cifrar el mensaje de texto en una línea plana de números, es más difícil adivinar el número que representa el carácter o cuántos dígitos tendrá cada carácter, por lo tanto, la longitud total del mensaje. En el caso de que un ataque intercepte el mensaje, será difícil que el ataque encuentre una aproximación al algoritmo, debido a todas las implementaciones y seguridades del algoritmo matemático.

Alsaber et al. (2021, p. 360), realizó un artículo que tuvo como objetivo determinar si los desarrolladores de software comprenden las reglas de scrum. El estudio indicó que adaptar las necesidades de los usuarios para cumplir con sus requisitos y entregar los productos a tiempo dentro del coste previsto, es una cuestión crítica que todos los directores de proyectos de software buscan desempeñar y colocan la

máxima prioridad para ello, teniendo en cuenta la satisfacción de los usuarios. La metodología ágil es una de las soluciones aportadas por los ingenieros de software para involucrar a los clientes en el ciclo de vida de desarrollo del sistema y evitar el riesgo de incumplimiento. Los resultados apuntaron a que estas metodologías siguen enfrentándose a los costes de no conformidad y a los cambios dinámicos, y no se registra la causa raíz del problema para encontrar una solución. Además, vislumbraron cómo afecta este conocimiento al éxito de los proyectos de software desde la perspectiva de la gestión de proyectos. También se estudió el compromiso y el impacto de la falta de conocimientos suficientes sobre el tema para la entrega del proyecto. Concluyeron que los datos recogidos a partir de los métodos cualitativos y cuantitativos, que se llevaron a cabo con equipos de scrum y trabajaron en el sistema de información sanitaria, soluciones educativas y soluciones gubernamentales, mostraron desviaciones en las prácticas organizativas y en los conflictos, la competencia y la presión del equipo, así como una disminución de la calidad del producto.

La revista Dilemas Contemporáneos: Educación, Política y Valores en el estado de México publicó un artículo escrito por Martínez Delgado et al. (2018, p. 1) expone los resultados fundamentales de una investigación que con un enfoque teórico-práctico revisa los conceptos en torno a la gestión de la información con el fin de lograr una integración armoniosa de los sistemas de información relacionados en unidades de diversas entidades del país que gestionan información de interés del gobierno, Se propuso un procedimiento de mejora que se aplicó a un grupo de ministerios y organismos priorizados, mostró efectividad, facilitando la toma de decisiones oportunas a nivel gubernamental y empresarial, y sentando las bases para el establecimiento del e-gobierno.

Mashal y Rozilawati (2018, p. 2315) realizaron un estudio que pretendió mostrar cómo se forma el método Scrumban basado en una combinación de los métodos Kanban y Scrum. Scrumban es una combinación de prácticas de Kanban y Scrum para gestionar el desarrollo de software basado en diferentes situaciones del proyecto. Sin embargo, ya que cada método tiene sus propios pros y contras, la formación inadecuada de las prácticas Scrumban puede conducir a un aumento de los residuos y el tiempo de desarrollo, y la disminución de la calidad, que, a su vez,

afectan a las organizaciones ágiles y causan un desarrollo ineficiente e ineficaz. Los practicantes de Kanban y Scrum están convencidos de que una combinación de ambos métodos es mejor que el uso de uno solo y, por lo tanto, los practicantes deben ser guiados en su toma de decisiones. La formación de Scrumban y la identificación de los factores que ayudan a la combinación de Kanban y Scrum se llevaron a cabo a través de una revisión de los trabajos anteriores y entrevistas semi-estructuradas con 7 expertos ágiles, después de lo cual, se realizó un análisis de contenido para analizar los datos recogidos. Diferentes factores, la prescripción del método, las funciones y responsabilidades, el tiempo de adopción, el tamaño del equipo, el tamaño del lote, la priorización de los requisitos, el tamaño de las características, el tiempo de entrega, las prácticas técnicas, el coste y la calidad, ayudan a los miembros del equipo Ágil en la formación de Scrumban mediante la combinación de las prácticas apropiadas de Kanban y Scrum. Además, se descubrió que Scrumban es más apropiado que Scrum o Kanban para ahorrar tiempo, mejorar la calidad y minimizar los residuos.

Por otro lado, en Madrid se publicó un artículo de la revista de la Sociedad Española de Farmacia Hospitalaria escrito por Santolaya-Perrin et al. (2020, p. 1) donde indica que la pandemia de COVID 19 ha limitado enormemente la capacidad de respuesta del sistema médico y a sus especialistas. Los servicios de urgencias fueron los primeros en afrontar este reto junto con los farmacéuticos pertenecientes a estas unidades médicas, que han precedido a los del resto de las áreas del servicio de farmacia. Facilitar la comunicación dentro del pro pio servicio y en emergencias es una de las tantas estrategias clave impulsadas durante esta pandemia. La cooperación multidisciplinaria y la coordinación de la información junto con un sistema informático bien desarrollado como elemento importante de la seguridad del proceso de reciclaje de medicamentos, son siempre la base de un trabajo eficiente y de alta calidad. Los avances de las TIC durante las pandemias permitirán nuevos modelos de atención farmacéutica, esto no reemplazará el trabajo personal del farmacéutico en la sala de emergencias que es esencial.

En el ámbito nacional, Vallejos (2021, p. 5) en su estudio tiene como objetivo comparar el rendimiento del intercambio de datos JSON cifrados sobre una plataforma web, configurando escenarios para probar sobre una plataforma web

desarrollada en Node y JS, donde se pueden cifrar los datos, además de generar claves y realizar cifrado, monitorear el cifrado y descifrado de los paquetes enviados, también se estima el rendimiento del intercambio de datos según el grado de seguridad, la fortaleza de la clave y la velocidad del tiempo en el cifrado y descifrado, definiendo el tamaño y la generación de claves. Finalmente, se compara el rendimiento de la estructura del algoritmo Json cifrado por Json y RSA, y se determina que el Json cifrado por RSA tiene mayor seguridad y mayor fortaleza de clave, pero el tiempo de ejecución del cifrado es mayor.

Chuco (2013) en su proyecto de investigación utiliza el cifrado RSA, un método alternativo que va permitir la prevención de ataque como también de vulnerabilidades contra los activos de información de la empresa ELECTROPERÚ S.A. Ampliamente utilizado en protocolo de comercio electrónico, en correo electrónico, en transmisión de datos y otros campos. Considerado como uno de los más seguros los algoritmos asimétricos, con longitudes de clave RSA de 1024-2048 bits, la seguridad está basado en la inexistencia de una forma concreta de descomponer como dos grandes primos, que en conclusión tienen un alto impacto en la confiabilidad y mejoran la confiabilidad de las transferencias de archivos de texto en la sede de ELECTROPERÚ S.A realizado en la investigación.

Enciso (2022, p. 5) realizó un artículo que estuvo centrado en la exploración de la transformación digital y la aplicación del modelo Scrum. También se examinó la relación entre la transformación digital y la aplicación de la metodología Scrum en el ámbito tecnológico de un banco peruano. Investigación de enfoque cuantitativo, descriptivo-correlacional, no experimental y transversal. El estudio se realizó sobre una muestra de 119 trabajadores del sector tecnológico mediante un método de encuesta. Los resultados obtenidos se observaron mediante la prueba estadística de Spearman con un valor rho de 0,693, lo que indica una correlación positiva de nivel medio a un nivel de significación inferior a 0,05, lo que sugiere una relación directa entre la transformación digital y el Marco Scrum en el ámbito tecnológico del banco.

Abanto y Ibañez (2021, p. 1) destinaron sus esfuerzos investigativos a introducir métodos ágiles de desarrollo empresarial. La metodología de la investigación fue aplicada y preexperimental y el estudio se centró en los usuarios finales de los

servicios de mantenimiento general o de los servicios relacionados con las reparaciones, las renovaciones y el mantenimiento de las viviendas y las empresas de la ciudad. Se utilizaron las herramientas Lean Startup y Scrum para implementar el proyecto. Como resultado, se estableció una cuota de mercado del 0,5% para el producto mínimamente viable 1, correspondiente a S23 590,93 en el primer año, y una cuota de mercado del 0,1% para el producto mínimamente viable 2, correspondiente a S37 080,00 en el primer año. Se identificaron cinco procesos para el desarrollo del proyecto: en primer lugar, el proceso de conceptualización de la idea de negocio, la formulación de un modelo a seguir, el desarrollo de un modelo de negocio, el desarrollo de un prototipo y, por último, la prueba y el desarrollo de un producto mínimo viable. Por último, el proyecto se ejecutó con métodos ágiles, en un plazo breve y en tres iteraciones, lo que permitió probar el modelo de negocio con los clientes.

Ayaipoma (2018, p. 6) estudió el problema del servicio de atención al cliente en COT 101, que no disponían de una herramienta adecuada para desarrollar sus operaciones y obligaba a los usuarios a utilizar métodos manuales y archivos de Excel, que servían como única herramienta para gestionar los tickets. Como no era posible basarse en informes automatizados para determinar el número de solicitudes pendientes, completadas y cerradas, así como el número de solicitudes gestionadas por cada miembro del personal, era difícil tomar decisiones en cada nivel organizativo, de tal manera que el proceso de atención al cliente presentaba varias anomalías en su evolución, lo que provocaba la insatisfacción de los clientes. Por todo ello, la solución del problema se planificó utilizando la metodología SCRUM, basada en un entorno flexible y ágil que permitió maximizar el retorno de la inversión a través de la aportación continua para obtener la funcionalidad del software en poco tiempo, de forma que pueda adaptarse fácilmente y de manera continua a las nuevas características. Concluyó que el proceso de atención al cliente mejoró notablemente, ya que los indicadores de eficiencia del proceso de atención al cliente aumentaron positivamente: mayor número de pedidos procesados, menor tiempo de tramitación de pedidos, automatización de procesos y creación de información más accesible, completa y fiable.

Los siguientes párrafos presentan las teorías y conceptos importantes para la comprensión de este estudio. En torno a ello, el componente de información y comunicación se refiere a los métodos, procesos, canales, medios y actividades que garantizan que la información fluya en todas las direcciones, con calidad suficiente y en el momento oportuno, utilizándola de forma sistemática y regular. De esta manera, se puede cumplir con la responsabilidad (Ayaipoma, 2018, p. 33).

Los recursos de las tecnologías de la información y la comunicación establecen espacios formativos y creativos fomentando el trabajo colaborativo, usa herramientas como blogs, webinars, wikis, redes sociales y entornos para crear, almacenar y publicar de contenidos. Para facilitar el poder desarrollar y generar el conocimiento colaborativamente entre discentes y docentes es necesario los recursos de aprendizaje, emplean herramientas educativas online y sistemas de gestión y evaluación del aprendizaje (Fernández et al, 2022, p. 28).

En cuanto a la funcionalidad, el sistema tiene como elemento fundamental la información, por lo que su finalidad es gestionar, almacenar y proporcionar datos e información que puedan dar soporte a los procesos y funciones que se realizan en la empresa, y subvencionar la toma de decisiones (Vértiz et al., 2019, p. 152). De igual manera, el cliente es una parte fundamental porque es la persona que utilizará el sistema, por lo que una estrategia de comunicación con el cliente es una guía que expresa cómo se planea entregar un determinado mensaje al público objetivo a través de diferentes canales para satisfacer los requerimientos de los clientes (Vértiz, 2018, p. 152).

La definición de seguridad de la información indica que es un conjunto de medidas técnicas, legales y organizativas que van a permitir a las organizaciones garantizar su integridad , su confidencialidad y su disponibilidad de los sistemas de la información. La definición del estándar ISO/IEC 27001 incluye mantener su integridad, su confidencialidad y su disponibilidad de la información; están involucradas también otras más características como lo es responsabilidad, autenticidad, confiabilidad y no repudio (Calderón, 2016, p. 2).

Según Rodríguez et al (2020), para que la ISO 27001 impacte en nuestra empresa, se deben definir los objetivos de seguridad de la información junto con el método

de evaluación de riesgos, habiendo pensado en la estrategia de seguridad, el siguiente paso que debemos dar es identificar los riesgos. que puede enfrentar la empresa, quién será el responsable de gestionar estos riesgos, cuál es la vulnerabilidad de la empresa. Una vez que finaliza la fase de planificación, es hora de implementar nuevas tecnologías y prácticas para ayudar a lograr los objetivos establecidos y hacer cumplir los controles de seguridad. Luego, es fundamental capacitar a los empleados sobre las nuevas tecnologías que se aplican y los nuevos protocolos que se han establecido. Velaremos por la eficacia de los procesos ya implantados en la empresa, invirtiendo tiempo en medir, controlar y revisar cómo funciona el sistema y si permite la consecución de los objetivos planteados.

La seguridad de la información se relaciona con la propia información, como el activo clave de una organización. En ese marco, una herramienta que permite mejorar los desarrollos de gestión de la información en una organización son los conocidos como TICs. Actúa sobre esta información para que tome las decisiones correctas comerciales en una organización moderna (Valencia et al , 2017, p. 74).

Basim et al. (2021, p. 347) indica que la seguridad de la información se utiliza para evitar el acceso no autorizado a la información y realizar diversas operaciones en dicha información, como el uso, divulgación, inhabilitación, destrucción o modificación de dicha información. SI tiene muchos objetivos en relación con la protección de la información contra los riesgos a los que dicha información puede estar expuesta. El tipo de riesgo al que están expuestos los datos varía según la aplicación.

Inthrani et al. (2020, p. 1820) en su artículo indica que los centros de datos son principalmente los principales objetivos de los ciberdelincuentes y las amenazas de seguridad, ya que albergan varios servicios críticos de tecnología de la información y la comunicación (TIC). La identificación de las amenazas y la gestión de los riesgos asociados con los centros de datos se han convertido en un gran desafío, ya que esto permitirá a las organizaciones optimizar sus recursos para centrarse en las amenazas más peligrosas para prevenir los riesgos y daños potenciales.

Nguyen Van Tanh et al (2021, p. 1727) indica que el desarrollo de Internet de las cosas (IoT) ha traído al mundo de las redes muchas innovaciones con nuevos

protocolos. Junto con eso, está la complejidad de los problemas de seguridad que afectan en gran medida a los datos personales y los recursos limitados en el desarrollo y las aplicaciones de tecnología de la información.

Pronika, SS Tyagui (2021, p. 1030) en su artículo indica que en este tumultuoso siglo XXI, estamos rodeados de muchas aplicaciones, como sitios web de redes sociales en Internet, o esta era también puede definirse como la era digital en la que todo es accesible a través de Internet. Hay miles de millones de usuarios de Internet en todo el mundo y comparten su información a través del mismo y, debido a esto, muchas personas intentan robar intencionalmente los datos confidenciales de otras personas, por lo que siempre es recomendable compartir y almacenar datos en forma encriptada.

Jomar L. et al (2022, p. 922) indica que se debe cifrar la información para fortalecer la seguridad de los datos dentro de la aplicación para que incluso los atacantes potenciales obtengan acceso a la base de datos de la aplicación; no pueden obtener información valiosa porque está codificada e ilegible.

Encriptar o cifrar se trata de envolver un mensaje utilizando un algoritmo matemático para que solo un destinatario legítimo pueda abrirlo y obtener su contenido mediante el uso de una clave única o clave que desenvuelve el mensaje. El propósito del cifrado es hacer que sea difícil de entender el mensaje a ojos de terceros ajenos a la comunicación (Valenzuela, 2019, p. 243).

El cifrado constituye el más importante avance tecnológico de los últimos dos milenios, pero es un arma de doble filo, es la mejor de las tecnología existentes y la peor al mismo tiempo. Puede detener el crimen y crear otros nuevos. De esta forma, se pueden identificar tensiones no resueltas entre las funciones que cumple la encriptación de las comunicaciones privadas como medio tecnológico de profundización en el ejercicio de la inviolabilidad de las comunicaciones, derecho a la privacidad y la seguridad pública (Valenzuela, 2019, p. 249).

Criptografía es una palabra del griego Kryptos (oculto) y graphos (escribir). Literalmente significa "texto oculto", mantener secreto codificando el mensaje los hace ilegibles, por lo que solo ese destinatario puede verlo como el remitente quiere, es una rama de las matemáticas que brinda herramientas ideales para

resolver problemas relacionados con la autenticidad y confiabilidad enfocándose en el mundo de la información digital. Los problemas de confidencialidad generalmente están relacionados con una técnica llamada "cifrado", mientras que la autenticidad está relacionada con una técnica llamada "firmas digitales", aunque en la práctica la solución a ambos se reduce a la aplicación de procedimientos criptográficos para el cifrado y descifrado. Las terminaciones indican que el texto original tiene por nombre texto claro, el texto codificado se denomina texto cifrado, la conversión de texto claro a texto cifrado es llamado cifrado y el proceso de recuperación del texto claro se llama descifrado (Volodymyr et al, 2022, p. 55).

Conocida también como una clave privada la criptografía simétrica tiene una característica significativa que es la de llevar una clave secreta para las acciones de cifrado como también para el descifrado, para este método de cifrado usa operaciones matemáticas y puede programarse con ciertos algoritmos informáticos que pueden ser simples pero muy rápidos. Este cifrado se divide en dos tipos como lo son el cifrado de bloque y de flujo, el primero va utilizar grupos de bits que también son llamados bloques, que se van a procesar muchas veces y la clave que se dio para este mismo es única para cada ronda, el segundo va dividir los datos en diminutos bits y va realizar siguiendo el cifrado (Volodymyr et al, 2022, p .55).

En cuanto al proceso son las acciones que buscan cumplir con los requerimientos del usuario,en otras palabras, son los pasos que debe seguir un sistema para mantener su eficacia y anticiparse a posibles problemas y limitaciones. Desde el punto de vista de la experiencia del usuario, si la calidad del producto no satisface sus expectativas, el producto no funcionará (Gracia, 2020, p. 289).

En cuanto a  metodologías ágiles o "ligeras" se obtiene que son un nuevo enfoque para el desarrollo de software que es mejor aceptado por los desarrolladores de proyectos informáticos que las metodologías tradicionales debido a sus principios y prácticas simples, el énfasis en equipos pequeños de desarrolladores, la flexibilidad al cambio y la ideología de la colaboración (Arias y Alvear, 2022, p. 11).

Según Cababie (2021, p. 5) las lista de elementos que se necesitan para la implementación de la metodología Scrum son: Backlog del producto, trata sobre la descripción de los requerimientos, elementos y enumera todas las funciones

deseadas del producto, ademas, clasifica según su prioridad. Backlog del Sprint, trata sobre la enumeración y contenidos de los sprint. Incrementos de funcionalidad del producto, verificar las versiones factibles y utilizables despues de cada final de iteración. Equipo de desarrollo, son personas que se unen formando un grupo para realizar un producto con los requitos propuestos por el dueño, estas personas deben contar con las habilidades necesarias para el mismo. Scrum Master, persona responsable para garantizar los objetivos y principios de scrum sean entendidos y usados por el equipo.

Scrum tiene un ciclo de vida que empieza con la vision del Product owner hacia el producto que se va crear y de acuerdo a ello se realizara una lista priorizada que va contener las características del producto denominada Product Backlog. Luego, se comienza con la planificacion del sprint y sprint backlog, estas incluyen las actividades que va realizar el equipo. En sprint planning el quipo elige una tarea del product backlog, creyendo que se puede completar en el intervalo de un ciclo de Sprint. A continuación viene sprint backlog donde la tarea se divide en unidades que llevara adelante el equipo y dentro de cada ciclo de sprint determina la mejor manera de lograr el objetivo. Tambien se realizan reuniones de scrum, aquí se obtiene progreso y dirección de nuestro proyecto, estas tienen una duración normal de 15 minutos (Tabares et al , 2017, p. 2).

Asimismo, este método se utiliza en planes que requieren resultados a corto plazo, así como en situaciones con incertidumbre y actividades dispersas. La novedad, la eficiencia, la competitividad y la flexibilidad son cruciales para el éxito del proyecto. Scrum es un modelo que define un conjunto de prácticas y roles que pueden servir como punto de partida para definir el proceso de desarrollo en un proyecto. Los roles más importantes en Scrum son el Scrum Master, el Product Owner y el Equipo Scrum (Kuz et al., 2018, p. 5).

Definir qué se quiere conseguir, lo primero que debe hacer es una lista de todo lo que el cliente quiere de su producto o desarrollo: características, funciones o requisitos. Esta información es base para realizar el backlog del producto (Gonçalves, 2018).

Establecer prioridades, dado que SCRUM está diseñado para simplificar el desarrollo en proyectos pequeños, es importante trazar el viaje de desarrollo del producto en sprints o iteraciones. Una vez hecho esto, se debe convocar el primer acto (Kadenic, Koumaditis y Junker, 2022, p. 2).

Para un sistema web general, se consideran las siguientes características: accesibilidad porque el sistema brinda acceso web compatible con diferentes navegadores web, dispositivos terminales y sistemas operativos, y no requiere complementos ni fallas ni problemas de actualización causados por complementos como Flash Player, disponibilidad porque el sistema está disponible las 24 horas del día, los 7 días de la semana, al que se puede acceder en cualquier momento desde cualquier lugar, siempre que haya Internet disponible, universalidad porque el sistema brinda servicios para diferentes usuarios en todo el mundo, independientemente de sus idiomas, antecedentes y otros, escalabilidad porque el sistema admite la integración de diferentes tipos de bancos de pruebas, controladores, etc., y la implementación de nuevas funcionalidades. Un diseño modular mejoraría la escalabilidad de un sistema (ZHONGCHENG, 2022, p. 2).

En cuanto al lenguaje de programación se utilizará PHP, como uno de los lenguajes dinámicos más populares, actualmente funciona en casi el 80% de los sitios web, PHP fue creado originalmente por Rasmus Lerdorf como un lenguaje de plantillas para páginas HTML renderizadas del lado del servidor. Gracias a su simplicidad y facilidad de uso, su popularidad y conjunto de características han crecido rápidamente, de manera similar a otros lenguajes dinámicos, PHP también permite ejecutar código generado dinámicamente, ya sea pasándolo directamente a la función o escribiéndolo en un archivo y luego incluyéndolo, esta característica ciertamente debe abordarse en cualquier compilador, porque contrasta fuertemente con la forma en que normalmente funcionan los lenguajes compilados. Sin embargo, dado que la ejecución de código generado dinámicamente puede causar imprevisibilidad y problemas de seguridad, generalmente se limita a casos de uso específicos en proyectos de la vida real (Husák et al, 2022, p. 2).

De igual manera se usó MySQL como la base de datos de descarga gratuita más famosa del mundo, MySQL tiene muchos atractivos como ser pequeño, rápido y de bajo precio, es una base de datos relacional convencional y las operaciones que se

enumeran aquí con estas dos bases de datos son CREAR, SELECCIONAR, INSERTAR, ELIMINAR e IMPORTAR. Aquí, se realiza un conjunto de experimentos mediante la ejecución de diferentes consultas y comandos. Son consultas SELECCIONAR con y sin usar funciones agregadas, comandos INSERTAR y ACTUALIZAR, la consulta SELECT se ejecuta para un caso simple y también para una condición (Benymol y Sajimon, 2020, p. 2037).

# III. METODOLOGÍA

## 3.1. Tipo y diseño de investigación

Tipo de investigación

Desde una perspectiva cuantitativa, se desarrollará el estudio siguiendo el método científico y caracterizándolo, en primer lugar, como descriptivo, por cuanto estos tipos de investigación hacen hincapié en la descripción de los hechos que son observables desde la realidad sobre la cual se desenvuelven para poder procesar los datos recabados de manera estadística y proceder a realizar inferencias sobre los mismos (Hernández y Mendoza, 2018, p. 40).

En ese mismo orden, el tipo de investigación es aplicado, por cuanto el autor del estudio pondrá en práctica los conocimientos, las herramientas y los aspectos profesionales adquiridos durante su formación profesional con el propósito de brindar una solución a un problema real (Baena, 2017, p. 42).

Diseño de investigación

En este sentido, se enmarcará en un pre-experimental. Según Hernández y Mendoza (2018, p. 42), un diseño preexperimental se caracteriza por una intervención consciente por parte del investigador, analizando los elementos que componen la unidad de análisis, con el fin de publicar una posición final o desarrollar un plan de acción a favor de su corrección o mejora.

En el mismo eje, el alcance de la investigación será transversal, ya que los datos se tomarán una sola vez en el tiempo, seguido de la publicación de conclusiones o el desarrollo de mejoras y/o acciones correctivas (Carrasco, 2019, p. 46).

### 3.2. Variables y operacionalización

**Variable 1:** Proceso de encriptación

- **Definición conceptual:** Se trata de envolver un mensaje utilizando un algoritmo matemático para que solo un destinatario legítimo pueda abrirlo y obtener su contenido mediante el uso de una clave única o clave que desenvuelve el mensaje. El propósito del cifrado es hacer que sea difícil de entender el mensaje a ojos de terceros ajenos a la comunicación (Valenzuela, 2019, p. 243)
- **Dimensiones:** Información.
- **Indicadores:** Mensajes cifrados.
- **Escala de medición:** razón.

**Variable 2:** Seguridad de la información

- **Definición conceptual:** Incluye mantener su integridad, su confidencialidad y su disponibilidad de la información; están involucradas también otras más características como lo es responsabilidad, autenticidad, confiabilidad y no repudio (Calderón, 2016, p. 1)
- **Dimensiones:** Rendimiento.
- **Indicadores:** Porcentaje de disponibilidad de la información dentro de la institución, porcentaje de confidencialidad de la información dentro de la institución.
- **Escala de medición:** razón.

La matriz de operacionalización se podrá ver en el anexo 1.

### 3.3. Población, muestra y muestreo

**Población**

Es considerada como el conjunto o universo de elementos que interactúan entre sí y comparten características de interés de estudio para el investigador (Hernández y Mendoza, 2018, p. 195). En ese orden, se tomará como población las interacciones del sistema en el periodo de una semana.

**Tabla 1 :** *Población.*

| TIEMPO | REGISTRO DIARIO | TOTAL | UNIDAD |
|---|---|---|---|
| 1 semana | 8 | 56 | interacción |

Fuente: Elaboración propia

**Muestra**

La muestra es una fracción de la población con el fin de extraer información para dar respuesta a las preguntas de investigación (Hernández y Mendoza, 2018, p. 196).

Para hallar las muestras se usará una fórmula:

$$n = \frac{N*z^2*p*q}{(N-1)*e^2+z^2]*p*q}.$$

Dónde:

n = Población: Tamaño de la muestra

z = 1.96: Nivel de Confianza (95%)

p = 0.5: Probabilidad de éxito

q = 0.5: Probabilidad de fracaso

e = 0.05: Error máximo de tolerancia (5%)

Reemplazando:

$$n = \frac{56 *(1.96)^2*0.5*0.5}{(56 -1)*0.05^2+1.96^2*0.5*0.5} = 48.99$$

Muestra = n = 49 interacciones

**Muestreo**

Se aplicará un muestreo de tipo probabilístico y al azar simple. En estos tipos de muestreo, la probabilidad de que los elementos sean seleccionados es la misma. (Hernández y Mendoza, 2018, p. 197).

## 3.4. Técnicas e instrumentos de recolección de datos

### Técnicas de recolección de datos

La recolección de datos indica que se va usar distintos instrumentos que sirvan de medición para recopilar los datos de las variables que tengamos en la investigación. Los datos que se obtengan serán la base del estudio., sin datos no puede haber investigación. Este proceso lleva por consecuencia elaborar un cronograma de procedimientos para el fin que es la recolección de información con un propósito establecido (Hernández y Mendoza, 2018, p. 228).

### Instrumentos de recolección de datos

Como complemento de la técnica a emplear, se suscita la necesidad de diseñar un instrumento. En este caso será una ficha de registro que detalla los 3 indicadores en las 49 interacciones que tendrá la muestra.

**Tabla 2 :** *Instrumento.*

| N° Interacción | Indicador |
|---|---|
| Técnica | |

Fuente: Elaboración propia

## 3.5. Procedimientos

Primero, se realizará la solicitud de acceso a la institución en mención. Luego se realizará el formulario para el registro de información que arroje el sistema, estos datos serán necesarios para los indicadores de la investigación (mensajes cifrados, porcentaje de disponibilidad de la información y porcentaje de confidencialidad de la información).

Posteriormente a la recaudación de la información, se realizará el traslado de los datos al programa estadístico SPSS, el cual permitirá observar de manera objetiva la información a través de tablas y figuras.

## 3.6. Método de análisis de datos

En este caso se hará uso de la estadística descriptiva e inferencial como también del programa informático SPSS para analizar los datos recolectados.

### 3.7. Aspectos éticos

- **Autonomía:** Los miembros pueden participar o retirarse de la investigación en cualquier momento a petición propia.
- **Competencia profesional y científica:** Cuando los estudiantes alcanzaron el nivel suficiente de formación para realizar una investigación, la precisión científica está garantizado por todo el tiempo que dure el estudio, hasta su publicación
- **Objetividad:** Su significancia es mostrar la realidad tal y como es. Por ende, esta investigación se va basar en estándares técnicos e imparciales de análisis de todos las variables y factores y estará respaldada por diversos estudios e investigaciones que serán de fuentes ya confiables.
- **Respeto a los derechos de propiedad intelectual:** Indica la característica de un estudio de no ser copia o imitación. Por ende, las referencias otorgadas corresponden a fuentes confiables y están marcadas justamente para evitar plagios.
- **Transparencia:** Es una característica de la autenticidad, lo que significa que toda la información que se presenta es verdadera porque la autoridad u organismo se utiliza como fuente bibliográfica o en caso de no estar disponible, se cita correctamente la fuente.
- **Libertad:** Esta investigación se realizará sin perjuicio y sin consideración de intereses económicos, políticos, religiosos o de otra índole.

## IV. RESULTADOS

Este capítulo tendrá como objetivo mostrar resultados obtenidos al desarrollar el sistema lo cual se aplicó al centro de comando aeroespacial. Se inició desarrollando pruebas previas sin el sistema y también una prueba posterior cuando el sistema estuvo terminado. Se utilizó el software IBM SPSS Statics versión 27 para los resultados de estadística confiables.

**Tabla 3 :** *Resultados de Pre - test y Post - test para indicadores.*

| N° Interacción | Indicador 1: Mensajes cifrados | | Indicador 2: Porcentaje de disponibilidad de la información (%) | | Indicador 3: Porcentaje de confidencialidad de la información (%) | |
|---|---|---|---|---|---|---|
| | Pre - test | Post - test | Pre - test | Post - test | Pre - test | Post - test |
| 1 | 0 | 30 | 53 | 100 | 0 | 100 |
| 2 | 0 | 15 | 59 | 100 | 0 | 100 |
| 3 | 0 | 26 | 27 | 100 | 0 | 100 |
| 4 | 0 | 10 | 52 | 100 | 0 | 100 |
| 5 | 0 | 15 | 49 | 100 | 0 | 100 |
| 6 | 0 | 30 | 45 | 100 | 0 | 100 |
| 7 | 0 | 5 | 20 | 100 | 0 | 100 |
| 8 | 0 | 33 | 41 | 100 | 0 | 100 |
| 9 | 0 | 26 | 33 | 100 | 0 | 100 |
| 10 | 0 | 15 | 54 | 100 | 0 | 100 |
| 11 | 0 | 26 | 36 | 100 | 0 | 100 |
| 12 | 0 | 30 | 36 | 100 | 0 | 100 |
| 13 | 0 | 10 | 45 | 100 | 0 | 100 |
| 14 | 0 | 32 | 60 | 100 | 0 | 100 |
| 15 | 0 | 13 | 40 | 100 | 0 | 100 |
| 16 | 0 | 30 | 54 | 100 | 0 | 100 |
| 17 | 0 | 26 | 38 | 100 | 0 | 100 |
| 18 | 0 | 30 | 35 | 100 | 0 | 100 |
| 19 | 0 | 10 | 26 | 100 | 0 | 100 |
| 20 | 0 | 16 | 24 | 100 | 0 | 100 |
| 21 | 0 | 26 | 24 | 100 | 0 | 100 |
| 22 | 0 | 17 | 42 | 100 | 0 | 100 |
| 23 | 0 | 30 | 20 | 100 | 0 | 100 |
| 24 | 0 | 5 | 30 | 100 | 0 | 100 |
| 25 | 0 | 15 | 27 | 100 | 0 | 100 |
| 26 | 0 | 18 | 38 | 100 | 0 | 100 |
| 27 | 0 | 30 | 60 | 100 | 0 | 100 |
| 28 | 0 | 17 | 55 | 100 | 0 | 100 |
| 29 | 0 | 26 | 49 | 100 | 0 | 100 |
| 30 | 0 | 10 | 57 | 100 | 0 | 100 |
| 31 | 0 | 40 | 20 | 100 | 0 | 100 |
| 32 | 0 | 30 | 26 | 100 | 0 | 100 |
| 33 | 0 | 11 | 58 | 100 | 0 | 100 |
| 34 | 0 | 15 | 52 | 100 | 0 | 100 |
| 35 | 0 | 46 | 36 | 100 | 0 | 100 |
| 36 | 0 | 5 | 27 | 100 | 0 | 100 |
| 37 | 0 | 16 | 37 | 100 | 0 | 100 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 38 | 0 | 30 | 60 | 100 | 0 | 100 |
| 39 | 0 | 12 | 29 | 100 | 0 | 100 |
| 40 | 0 | 5 | 34 | 100 | 0 | 100 |
| 41 | 0 | 53 | 29 | 100 | 0 | 100 |
| 42 | 0 | 10 | 55 | 100 | 0 | 100 |
| 43 | 0 | 15 | 57 | 100 | 0 | 100 |
| 44 | 0 | 16 | 55 | 100 | 0 | 100 |
| 45 | 0 | 4 | 28 | 100 | 0 | 100 |
| 46 | 0 | 30 | 24 | 100 | 0 | 100 |
| 47 | 0 | 16 | 30 | 100 | 0 | 100 |
| 48 | 0 | 10 | 52 | 100 | 0 | 100 |
| 49 | 0 | 30 | 58 | 100 | 0 | 100 |

Fuente: Elaboración propia

### 4.1 Análisis descriptivo

**Tabla 4 :** *Medias de los indicadores para la pre - test y post – test.*

| Indicadores | Pre - test (media) | Post - test (media) |
|---|---|---|
| Cantidad de mensajes cifrados | 0 | 20,73 |
| Porcentaje de disponibilidad de la información dentro de la institución (%). | 40,73 | 100 |
| Porcentaje de confidencialidad de la información dentro de la institución (%). | 0 | 100 |

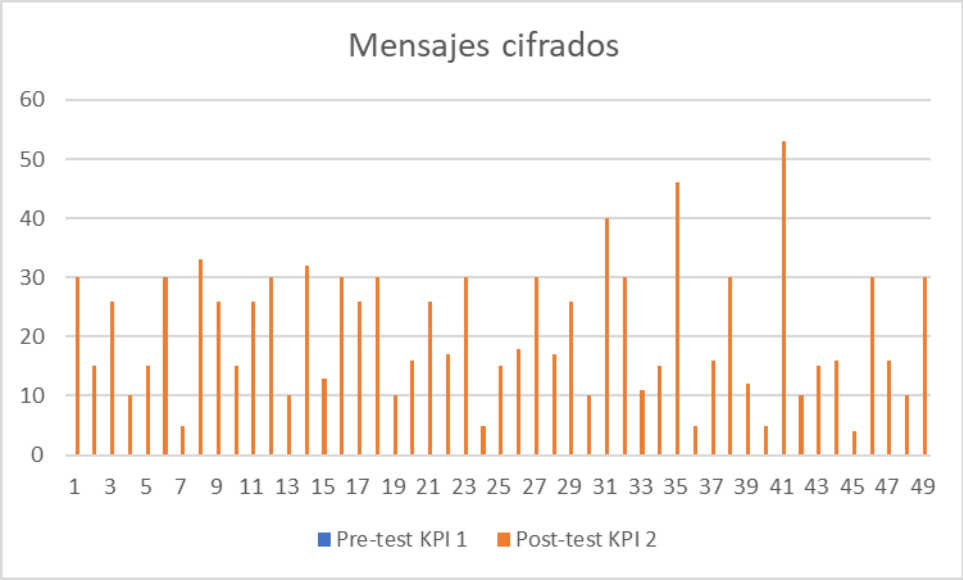
Fuente: Elaboración propia

Interpretación

Como se muestra en la tabla 3, se puede ver que el número promedio de los mensajes cifrados (indicador 1) aumentó luego de la implementación del sistema de comunicación, de igual manera el promedio del porcentaje de disponibilidad de la información aumentó después de la implementación del sistema, como también aumentó el porcentaje medio de la confidencialidad de la información. Se realiza el análisis detallado de los indicadores presentados a continuación.

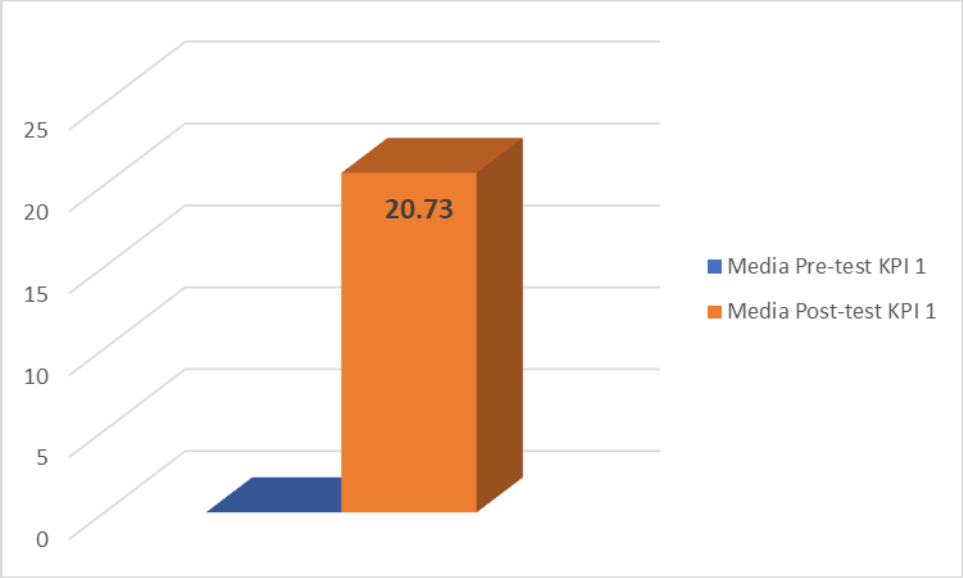
### 4.1.1 Indicador 1: Mensajes cifrados

*Figura 1:* Resultados de Pre - test y Post - test para el primer indicador.




*Fuente*: Elaboración propia

*Figura 2:* Media de resultados de Pre - test y Post - test para el primer indicador.



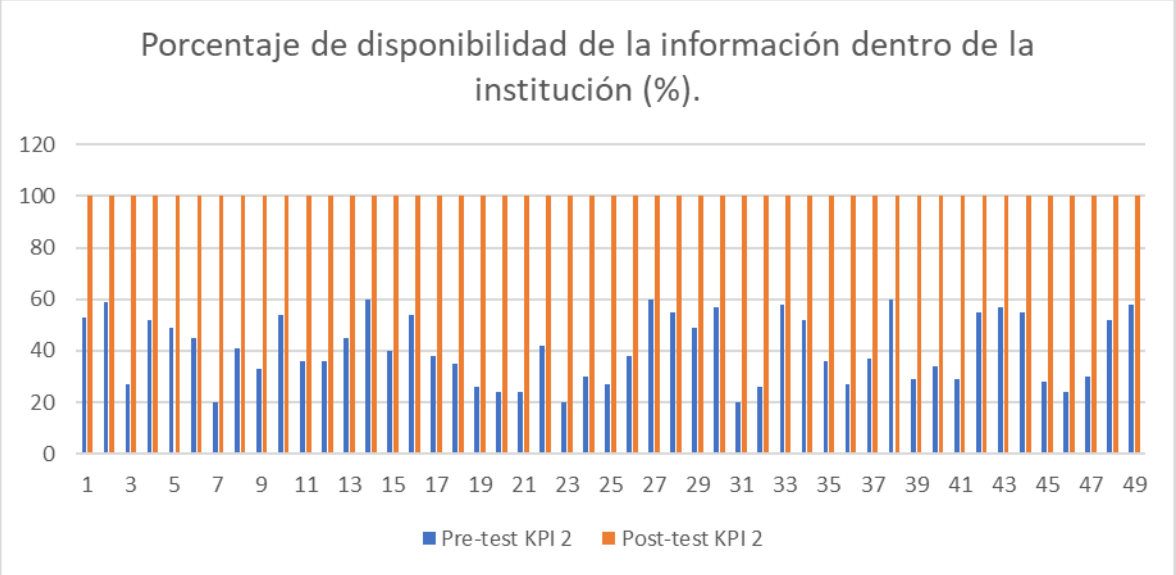

*Fuente*: Elaboración propia

Interpretación

En la figura 2 se observa que la media de los mensajes cifrados de todas las interacciones es de 20.73 luego de implementar el sistema de comunicación, por lo tanto, tenemos un incremento del 100%.

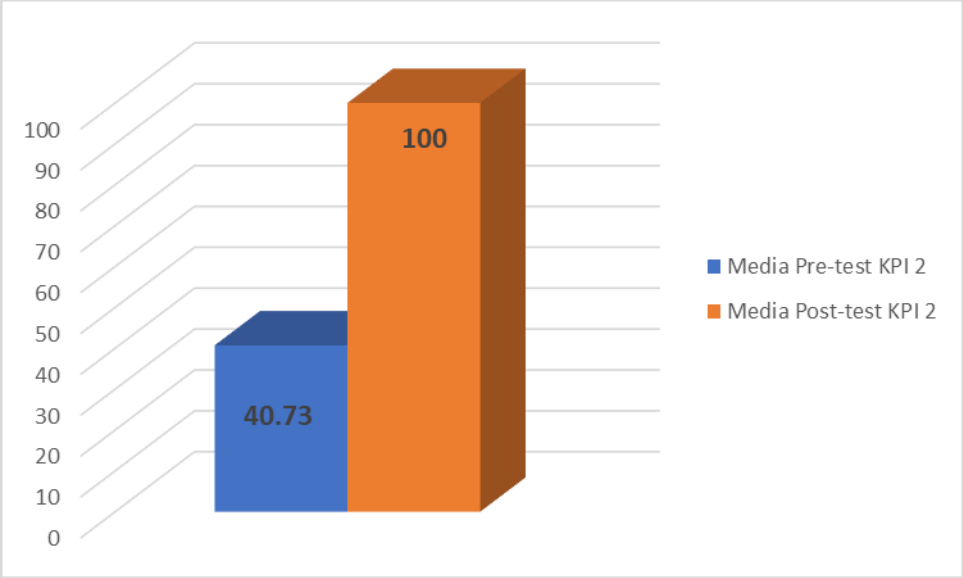
### 4.1.2 Indicador 2: Porcentaje de disponibilidad de la información dentro de la institución (%).

*Figura 3:* Resultados de Pre - test y Post - test para el segundo indicador.




*Fuente*: Elaboración propia

*Figura 4:* Media de resultados de Pre - test y Post - test para el segundo indicador.



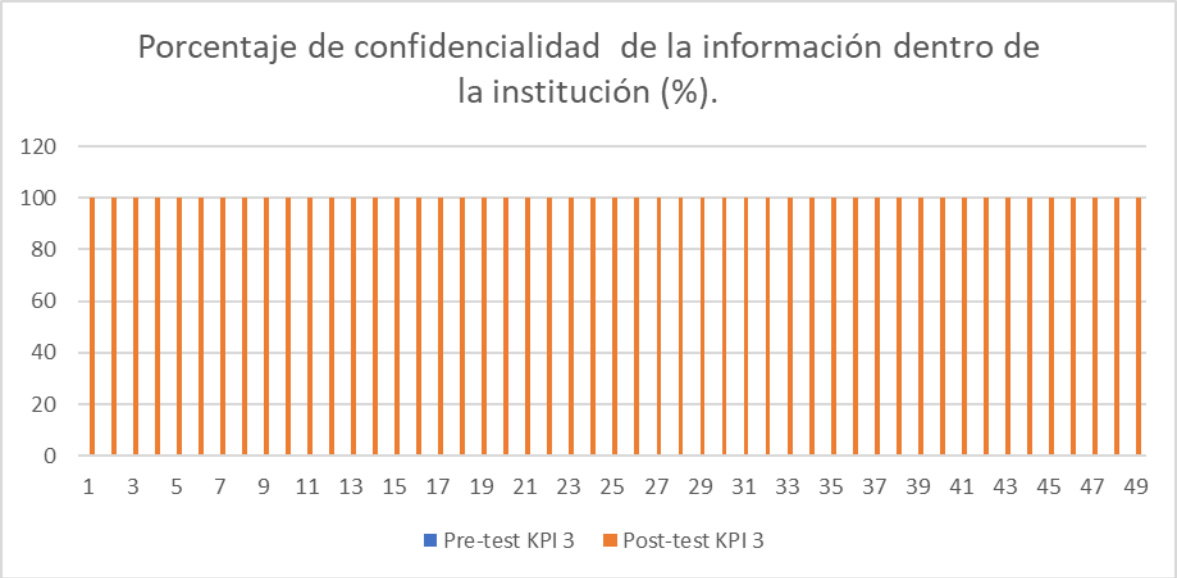

*Fuente*: Elaboración propia

Interpretación

La figura 4 muestra que la media del porcentaje de disponibilidad de la información es de 40.73 % antes de implementar el sistema de comunicación, realizado la implementación el porcentaje de disponibilidad es del 100%, obteniendo un incremento de 59.27%.

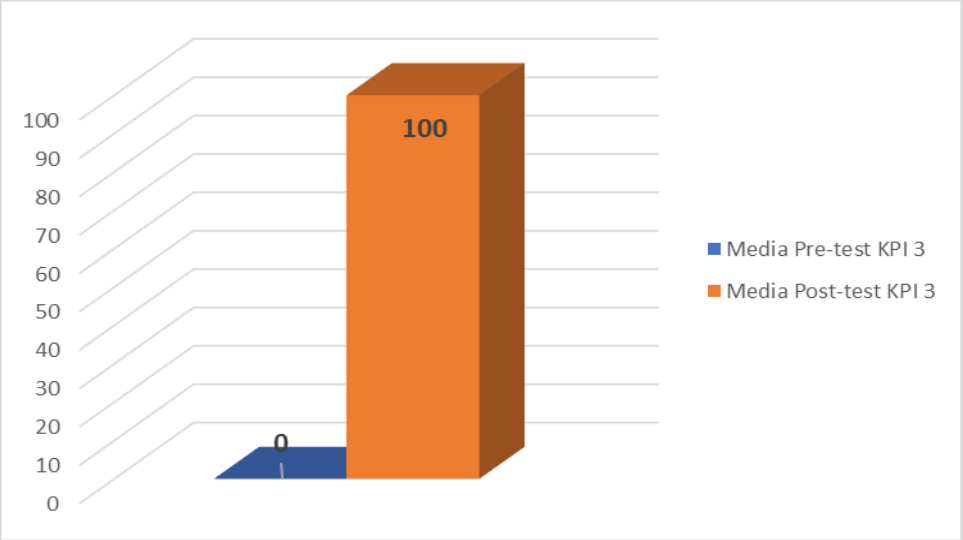
### 4.1.3 Indicador 3: Porcentaje de confidencialidad de la información dentro de la institución (%).

*Figura 5:* Resultados de Pre - test y Post - test para el tercer indicador.




*Fuente*: Elaboración propia

*Figura 6:* Media de resultados de Pre - test y Post - test para el tercer indicador.




*Fuente*: Elaboración propia

Interpretación

En la figura 6 se observa que con la utilización del sistema de comunicación se pudo incrementar al 100% el porcentaje de confidencialidad de la información en el centro de comando aeroespacial.

## 4.2 Análisis inferencial

### 4.2.1 Nivel de confianza y grado de significancia

Los siguientes parámetros se utilizaron para la prueba de hipótesis de los datos recopilados:

El nivel de confianza es del 95%

El nivel de significancia es del 5%

### 4.2.2 Contrastación de para el indicador 1: Seguridad

4.2.2.1 Prueba de normalidad

Para seleccionar nuestra prueba de hipótesis de la investigación, los datos se sometieron a comprobar su distribución, de manera específica si los datos de seguridad (número de mensajes de encriptados) contaban con una distribución normal, como la muestra era menor de 50, se aplicó la prueba de Shapiro-Wilk a las métricas.

Si:

Sig. < 0.05 Adopta una distribución no normal.

Sig. ≥ 0.05 Adopta una distribución normal

**Tabla 5 :** *Prueba de normalidad del primer indicador.*

| Prueba | | Shapiro - Wilk | | |
|---|---|---|---|---|
| | | Estadístico | Gl | Sig. |
| Pre - test | Seguridad | ,000 | 49 | ,000 |
| Post - test | Seguridad | ,926 | 49 | ,004 |

Fuente: Elaboración propia

Según la tabla 4 el resultado arroja que el Sig. Del indicador 1 antes fue de ,000 y ,004 después en donde el valor es menor a 0.05 en ambos test indicando por consiguiente una distribución no normal y se va usar la prueba de Wilcoxon, utilizado para probar hipótesis.

Hipótesis nula

El proceso de encriptación disminuye los mensajes cifrados en el sistema del comando de control aeroespacial.

Hipótesis alterna

El proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial.

**Tabla 6 :** *Prueba de Wilcoxon al primer indicador.*

| | Seguridad (Pre - test) - Seguridad (Post - test) |
|---|---|
| Z | -6,106[b] |
| Sig. asintótica (bilateral) | ,001 |

Fuente: Elaboración propia

La siguiente prueba de Wilcoxon, aplicado porque los datos tienen una distribución no normal, arroja un resultado demostrando que, el nivel de significancia es 0.001, viendo que es menor que 0.05, se procede a rechazar la hipótesis nula y aceptamos la hipótesis alterna, el cual es que el proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial.

### 4.2.3 Contrastación de para el indicador 2: Porcentaje de disponibilidad de la información dentro de la institución

4.2.3.1 Prueba de normalidad

Para seleccionar nuestra prueba de hipótesis de la investigación, los datos se sometieron a comprobar su distribución, de manera específica si los datos del porcentaje de disponibilidad de la información dentro de la institución contaban con una distribución normal, como la muestra era menor de 50, se aplicó la prueba de Shapiro-Wilk a las métricas.

Si:

Sig. < 0.05 Adopta una distribución no normal.

Sig. ≥ 0.05 Adopta una distribución normal

**Tabla 7 :** *Prueba de normalidad del segundo indicador.*

| Prueba | | Shapiro - Wilk | | |
|---|---|---|---|---|
| | | Estadístico | Gl | Sig. |
| Pre - test | Seguridad | ,917 | 49 | ,002 |
| Post - test | Seguridad | ,000 | 49 | ,000 |

Fuente: Elaboración propia

Según la tabla 6 el resultado arroja que el Sig. Del indicador 2 antes fue de ,002 y ,000 después en donde el valor es menor a 0.05 en ambos test indicando por consiguiente una distribución no normal y se va usar la prueba de Wilcoxon, utilizado para probar hipótesis.

Hipótesis nula

El proceso de encriptación disminuye la disponibilidad de la información en el comando de control aeroespacial.

Hipótesis alterna

El proceso de encriptación incrementa la disponibilidad de la información en el comando de control aeroespacial.

**Tabla 8 :** *Prueba de Wilcoxon al segundo indicador.*

| | Seguridad (Pre - test) - Seguridad (Post - test) |
|---|---|
| Z | -6,094[b] |
| Sig. asintótica (bilateral) | ,001 |

Fuente: Elaboración propia

La siguiente prueba de Wilcoxon, aplicado porque los datos tienen una distribución no normal, arroja un resultado demostrando que, el nivel de significancia es 0.001 la cual es menor a 0.05, se procede a rechazar la hipótesis nula y aceptamos la hipótesis alterna, el cual es que el proceso de encriptación incrementa la disponibilidad de la información en el comando de control aeroespacial.

### 4.2.4 Contrastación de para el indicador 3: Porcentaje de confidencialidad de la información dentro de la institución

4.2.4.1 Prueba de normalidad

Para seleccionar nuestra prueba de hipótesis de la investigación, los datos se sometieron a comprobar su distribución, de manera específica si los datos del porcentaje de confidencialidad de la información dentro de la institución contaban con una distribución normal, como la muestra era menor de 50, se aplicó la prueba de Shapiro-Wilk a las métricas.

Si:

Sig. < 0.05 Adopta una distribución no normal.

Sig. ≥ 0.05 Adopta una distribución normal

**Tabla 9 :** *Prueba de normalidad del tercer indicador.*

| Prueba | | Shapiro - Wilk | | |
|---|---|---|---|---|
| | | Estadístico | Gl | Sig. |
| Pre - test | Seguridad | ,000 | 49 | ,000 |
| Post - test | Seguridad | ,000 | 49 | ,000 |

Fuente: Elaboración propia

Según la tabla 6 el resultado arroja que el Sig. Del indicador 2 antes fue de ,000 y ,000 después en donde el valor es menor a 0.05 en ambos test indicando por consiguiente una distribución no normal y se va usar la prueba de Wilcoxon, utilizado para probar hipótesis.

Hipótesis nula

El proceso de encriptación disminuye la confidencialidad de la información en el comando de control aeroespacial.

Hipótesis alterna

El proceso de encriptación incrementa la confidencialidad de la información en el comando de control aeroespacial.

**Tabla 10 :** *Prueba de Wilcoxon al tercer indicador.*

| | Seguridad (Pre - test) - Seguridad (Post - test) |
|---|---|
| Z | -7,000[b] |
| Sig. asintótica (bilateral) | ,001 |

Fuente: Elaboración propia

La siguiente prueba de Wilcoxon, aplicado porque los datos tienen una distribución no normal, arroja un resultado demostrando que, el nivel de significancia es 0.001 la cual es menor a 0.05, se procede a rechazar la hipótesis nula y aceptamos la hipótesis alterna, el cual es que el proceso de encriptación incrementa la confidencialidad de la información en el comando de control aeroespacial.

## V. DISCUSIÓN

Respecto a la información que se extrajo de la prueba de Wilcoxon, logramos aceptar todas las hipótesis alternas de cada hipótesis de investigación planeada, para la primera prueba se obtiene como resultado un valor de 0.01 de significancia bilateral, lo cual es menor a 0.05, por ello se acepta la hipótesis alterna, en donde nos indica que el proceso de encriptación incrementa los mensajes cifrados en el sistema del Comando de Control Aeroespacial, esto también significó una mejora del 100% en los mensajes cifrados porque previo a la implementación del sistema no existía mensajes cifrados. Esta mejora concuerda con lo demostrado en el artículo realizado por Torroba y Barrera (2016, p. 55) que lleva a cabo una implementación de un sistema de protección de los datos, esto estuvo fundado en un procesamiento óptico y analizó la exactitud de los datos recuperados si se producen pérdidas durante la transmisión. Se encripta la información usando una técnica de codificación llamada doble máscara de fase, entonces se determina que la información o datos encriptados aumentaron, además se recupera satisfactoriamente dicha información cuando el usuario autorizado posee la clave, de esta manera no se puede obtener mediante la interceptación del mismo.

En cuanto a la segunda hipótesis alterna, obtenemos un resultado de 0.01 de significancia bilateral, gracias a la prueba de Wilcoxon, que de igual forma es menor a 0.05, esto nos lleva a aceptar la hipótesis alterna, lo cual nos indica que el proceso de encriptación incrementa la disponibilidad de la información en el Comando de Control Aeroespacial, significando también una mejora del 59.27%. en cuanto a la disponibilidad de la información luego de implementar el sistema. Esta mejora concuerda con lo demostrado en la tesis realizada por Sarmiento y Gonzales (2019, p. 108) que luego de una implementación de la NTP/ISO 27001, logró tener una mejora significativa de la disponibilidad de la información, la cual aumentó de 30.6 % a 78.6 % utilizando un procedimiento de riesgo de disponibilidad de la información.

Referente a la tercera hipótesis alterna, obtenemos un resultado de 0.01 de significancia bilateral gracias a la prueba de Wilcoxon, que de igual forma es menor a 0.05, esto nos lleva a aceptar la hipótesis alterna, lo cual nos indica que el proceso de encriptación incrementa la confidencialidad de la información en el Comando de

Control Aeroespacial, significando también una mejora del 100%. en cuanto a la confidencialidad de la información luego de implementar el sistema, que ahora cuenta con la encriptación de los mensajes que anteriormente no tenía. Esta mejora concuerda con lo demostrado en el artículo realizado por Alves et al (2021, p. 1237) que tuvo como objetivo demostrar que los desarrolladores de IoT, siempre que necesiten realizar operaciones en archivos (crear, escribir, leer, adjuntar y eliminar) con datos encriptados, no tengan necesidad de conocer o estudiar diversas áreas y la complejidad del cifrado, concluyendo que el aumento de confidencialidad se dará sin importar tener un marco como este, en donde los desarrolladores ya no necesiten replicar todo el proceso criptográfico en todos los proyectos, pudiendo así centrarse sobre otros aspectos de los proyectos. Se observa en la fase de análisis de cifrados que no existe un cifrado ideal, cada cifrado trae consigo características que se pueden utilizar, la posibilidad de elegir el cifrado cambiando solo 2 parámetros de API, hace que el desarrollador elija un cifrado que corresponda con lo que desea del archivo.

Al implementar este sistema se mejora notablemente la seguridad de la información desde las contraseñas por cada usuario hasta los mismos mensajes, que es lo más importante dentro de la organización, infiriendo así que el proceso de encriptación influye de manera positiva en la seguridad de la información en el Comando de Control Aeroespacial.

Con relación a la metodología Scrum Endres, Bican y Wollner (2022, p. 8) en su artículo indican como ventaja que, mediante el uso de un backlog priorizado, los equipos pueden cambiar el enfoque para desarrollar las funciones principales desde el punto de vista de un cliente o usuario, esas características pueden luego presentarse en intervalos frecuentes a las partes interesadas respectivas, quienes pueden proporcionar comentarios para futuras mejoras. Por lo tanto, las soluciones se desarrollan hasta que son lo suficientemente buenas desde la perspectiva de las partes interesadas. Debido a las frecuentes sesiones de retroalimentación, los encuestados también consideraron que Scrum es un marco de apoyo para desarrollar soluciones fáciles de usar. Sin embargo, como desventaja, para desarrollar una solución fácil de usar y de calidad adecuada, se requiere la retroalimentación de los usuarios reales. La inclusión de la perspectiva del usuario

no está prescrita en Scrum, en algunos proyectos se vio que invitaban formal y regularmente a los usuarios a las reuniones de revisión; muchas veces estos mismos usuarios dijeron que incluyen su perspectiva solo de manera irregular.

En cuanto a la relevancia de la norma ISO 27001 aplicada a la investigación se realizaron las siguientes tareas como análisis de casos en el Comando de Control Aeroespacial, comparación y selección de métodos de seguridad de la información y desarrollo del proceso de seguridad de la información. En la primera tarea se diagnosticó la problemática en la unidad y como era de esperar, el problema más apremiante es una violación de la seguridad de la información, tales como:

- La divulgación de información a terceros puede ocurrir por incompetencia de los empleados que no están cumpliendo con las normas de protección de la información, puede transmitirse a través de comunicación, publicación, reenvío, pérdida, medios de comunicación, correspondencia, conferencias, reuniones personales, etc.
- Acceso no autorizado a la información, por ejemplo, la transferencia de información confidencial a personas que no tienen derecho a acceder a ella; pueden considerarse condiciones propicias para la incautación de información: soborno, bajo desempeño de los empleados, bajos salarios, falta de disciplina, etc.
- Bajo nivel de implementación de las metas establecidas para la creación de un sistema de comunicación e información.
- Falta de comprensión entre los empleados sobre la importancia de realizar trabajos para proteger la información; el personal no está suficientemente informado sobre los fines y objetivos de la empresa y no comprende la importancia de proteger los datos confidenciales.

Con respecto a la segunda tarea, se realizó la comparación y elección de métodos de seguridad de la información, tales como: métodos criptográficos; registro y creación de copias de seguridad del sistema, análisis de las ventajas y desventajas de cada método y la posibilidad de su aplicación en las condiciones de la unidad.

Se han desarrollado reglas de protección de la información para garantizar la dirección de la gestión de la protección de la información y respaldar la protección

de la misma de acuerdo con los requisitos comerciales y las leyes y reglamentos aplicables. A través de estas reglas de seguridad de la información, la dirección de la unidad demuestra el apoyo a la protección de la información y la obligación de protegerla.

Esta investigación tiene una relevancia importante en cuanto a la seguridad de la información porque se implementaron en el sistema un conjunto recomendado de medidas para garantizar lo anterior mencionado dentro de la unidad, estas incluyen medidas organizacionales tales como: restringir el acceso a las secciones en las que se lleva a cabo el procesamiento y transferencia de información confidencial sólo a trabajadores verificados; la exclusión de la visualización por parte de personas ajenas al contenido de los materiales procesados a través de la pantalla, uso de códigos criptográficos para la transmisión de información valiosa a través de canales de comunicación; destrucción de papel y otros materiales que contengan fragmentos de información valiosa.

Respecto a las medidas recomendadas para garantizar la seguridad de la información del Comando de Control Aeroespacial, se incluyen métodos especiales como la protección criptográfica de la información, como "firma electrónica" con la transferencia de información confidencial a través de canales de comunicación con la autenticación de mensajes transmitidos, almacenamiento de información (bases de datos) en medios en forma encriptada.

Verificando así que se garantice la disponibilidad de datos para usuarios autorizados: la capacidad de obtener rápidamente servicios de información y de igual manera garantizar la confidencialidad de la información en el Comando de Control Aeroespacial.

## VI. CONCLUSIONES

La primera conclusión es que el proceso de encriptación incrementa los mensajes cifrados en el sistema del Comando de Control Aeroespacial que posterior a la implementación del sistema se obtuvo un 100% de incremento con respecto al pre test realizado, esto a consecuencia de que el sistema cuenta con un algoritmo de encriptado de mensajes que utiliza una clave secreta para la realización de su función.

Como segunda conclusión el proceso de encriptación incrementa la disponibilidad de la información en el Comando de Control Aeroespacial, esto debido a que el promedio del pre test realizado fue de 40.73% y el post test fue del 100% en cuanto a disponibilidad de la información, llevando así a una mejora del 59.27% gracias a que el sistema cuenta a su vez con el algoritmo de descifrado para mostrar a la persona autorizada los mensajes que él mismo crea conveniente.

Como tercera conclusión el proceso de encriptación incrementa la confidencialidad de la información en el comando de control aeroespacial que posterior a la implementación del sistema se obtuvo un 100% de incremento con respecto al pre test realizado, debido a que para el descifrado de los mensajes es necesario la clave secreta aparte del algoritmo utilizado para atentar contra la seguridad y/o confidencialidad de los mismos.

Finalmente, como cuarta conclusión el proceso de encriptación influye de manera positiva en la seguridad de la información en el comando de control aeroespacial, esto basado en los resultados obtenidos ya que ahora el sistema brinda el cifrado de las contraseñas por cada usuario, contraseñas por cada sala de chat y también de los mensajes dentro de ellos, permitiendo así que la información esté completamente segura.

## VII RECOMENDACIONES

Como primera recomendación se podría implementar un nuevo algoritmo de encriptado de datos que sea de forma asimétrica en cuanto los usuarios se encuentren a mayor distancia entre ellos ya que esta criptografía es la ideal para esos casos.

Como segunda recomendación, se debería realizar la coordinación necesaria con el ámbito de sistemas para implementar o ampliar el acceso al sistema con nuevos perfiles de acuerdo a la categoría o grados dentro del centro de comando aeroespacial.

Como tercera recomendación, se deben incluir copias de seguridad automáticas de las bases de datos cada año, sobre todo de las tablas donde se mantienen los mensajes cifrados por un tema de auditoría, así como el mantenimiento regular de la información almacenada para contener solo la información relevante y necesaria y evitar la ralentización del procesamiento del sistema debido al almacenamiento de datos históricos, esto se coordina con las áreas del sistema para evitar la indisponibilidad de los datos que dichas áreas necesitan para realizar sus validaciones.

**REFERENCIAS**

ABANTO, H., IBAÑEZ, N. Implementación de las metodologías ágiles para el desarrollo del emprendimiento empresarial Comodin Perú SAC en la ciudad de Trujillo. Tesis de pregrado. Trujillo: Universidad Nacional de Trujillo, 2021.

Disponibel en: https://dspace.unitru.edu.pe/handle/UNITRU/18163

ALMOMANI, Ammar. Classification of Virtual Private networks encrypted traffic using ensemble learning algorithms. Egyptian Informatics Journal [en línea]. Julio 2022. [Fecha de consulta: 07 de junio de 2022].

Disponible en: https://doi.org/10.1016/j.eij.2022.06.006

ALSABER, L., AL ELSHEIKH, E., & ALJUMAH, S. Perspectives on the adherance to scrum rules in software project management. Indonesian Journal of Electrical Engineering and Computer Science [en línea]. Enero 2021. [Fecha de consulta: 12 de junio de 2022].

Disponible en: http://doi.org/10.11591/ijeecs.v21.i1.pp360-366

ALVES, Filipe, MATHEUS, Nuno, CRUZ, Manuela. Encryption File System Framework - Proof of Concept. Procedia Computer Science 181 [en línea]. 2021. [Fecha de consulta: 07 de noviembre de 2022].

Disponible en: https://doi.org/10.1016/j.procs.2021.01.322

AN, Yongli [et al.]. DCGAN-based symmetric encryption end-to-end communication systems. AEU - International Journal of Electronics and Communications [en línea]. Setiembre 2022. [Fecha de consulta: 02 de agosto de 2022].

Disponible en: https://doi.org/10.1016/j.aeue.2022.154297

ARIAS, B., ALVEAR, O. Análisis del resultado de la implementación de SCRUM, LEAN Y BSC en el proceso de desarrollo de software en la industria del Retail. Perspectivas [en línea]. Febrero 2022. [Fecha de consulta: 02 de julio de 2022].

Disponible en: https://doi.org/10.47187/perspectivas.4.1.116

AYAIPOMA, A. Implementación de una aplicación web para optimizar el proceso de atención a clientes en el área COT 101 de telefónica del Perú basado en la

metodología Scrum. Tesis de pregrado. Huancayo: Universidad Nacional del Centro del Perú, 2018.

Disponible en: https://repositorio.uncp.edu.pe/handle/20.500.12894/4822

BAENA, G. Metodología de la investigación. [en línea]. Azcapotzalco: Grupo editorial Patria, 2017. [Fecha de consulta: 06 de mayo de 2022].

Disponible en: http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

BENAVIDES, J. Modernización de las Tecnologías de la Información y su incidencia en la Seguridad Informática de la Fuerza Aérea del Perú – 2018. Tesis de maestría. Lima: Fuerza aérea del Perú, 2018.

Disponible en: http://repositorio.fap.mil.pe/handle/fap/65

BENIMOL, Jose, SAJIMON, Abraham. Performance analysis of NoSQL and relational databases with MongoDB and MySQL. Materials Today: Proceedings 24 [en línea]. 2020. [Fecha de consulta: 02 de noviembre de 2022].

Disponible en: https://doi.org/10.1016/j.matpr.2020.03.634

CABABIE, Pablo, TROILO, Fernando. Metodologías ágiles en equipos de operaciones del área de tecnología de la información (TI) [en línea]. Marzo 2021. [Fecha de consulta: 05 de mayo de 2022].

Disponible en: https://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=149445440&lang=es&site=eds-live

ISSN: 1668-4575

CALDERON, Laura. Seguridad informática y seguridad de la información. Universidad Piloto de Colombia [en línea]. Setiembre 2016. [Fecha de consulta: 06 julio 2022].

Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2821

CAMILO Salazar, J., TOVAR, Á., CARLOS Linares, J., LOZANO, A. y VALBUENA, L. Scrum contra XP: similitudes y diferencias. TIA [en línea]. Diciembre 2018. [Fecha de consulta: 12 de junio 2022].

Disponible en: https://revistas.udistrital.edu.co/index.php/tia/article/view/10496

ISSN: 2344-8288.

CAPRARO, F. y TOSETTI, S. Modern precision irrigation management tools based on electronic devices, computer programs and automatic control techniques. [en línea]. Marzo 2020. [Fecha de consulta: 04 de junio 2022].

Disponible en: https://publicaciones.sadio.org.ar/index.php/EJS/article/view/154.

CARRASCO, S. Metodología de la investigación científica. Décimo novena ed. Lima: San Marcos E I R, 2019. 476 pp.

ISBN: 978-9972-38-344-1

CHUCO, Marlon. Sistema de encriptación RSA para la fiabilidad de transmisión de archivos de texto en la sede campo armiño de Electroperú S.A. Tesis (Ingeniero de sistemas). Huancayo – Perú: Universidad nacional del centro del Perú, 2013.

Disponible en: https://repositorio.uncp.edu.pe/handle/20.500.12894/1426

DELGADO, C. Bicameralidad - modernización del estado y las TIC (caso peruano). Revista Caribeña de Ciencias Sociales [en línea]. Junio 2019. [Fecha de consulta: 13 de mayo 2022].

Disponible en: https://www.eumed.net/rev/caribe/2019/06/bicameralidad-tic.html

ISSN: 2254-7630

DEL POZO, Ivan. CI: A New Encryption Mechanism for Instant Messaging in Mobile Devices. Procedia Computer Science [en línea]. 2015. [Fecha de consulta: 14 junio 2022].

Disponible en: https://doi.org/10.1016/j.procs.2015.08.381

ENCISO, C. Transformación digital y uso de marco Scrum en el área de tecnología de un banco en Perú, 2021. Tesis de maestría. Lima: Universidad Cesar Vallejo, 2022.

Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/86350

ENDRES, Miro, BICAN, Peter, WOLLNER, Theresa. Sustainability meets agile: Using Scrum to develop frugal innovations. Journal of Cleaner Production [en línea]. Mayo 2022. [Fecha de consulta: 16 de noviembre de 2022].

Disponible en: https://doi.org/10.1016/j.jclepro.2022.130871

FERNÁNDEZ, Ana Martína, REYES, María Jódar, VALENZUELA López, Isabel. Tecnologías de la información y comunicación (TIC) en formación y docencia [en línea]. Marzo 2022. [Fecha de consulta: 05 de mayo de 2022].

Disponible en: https://doi.org/10.1016/j.fmc.2022.03.004

GRACIA, X. Uso de sistemas domóticos aplicados a la ingeniería eléctrica. Dominio de las ciencias [en línea]. Septiembre 2020. [Fecha de consulta: 16 de julio 2022].

Disponible en:
https://www.dominiodelasciencias.com/ojs/index.php/es/article/view/1398/0

GAETE, J., VILLARROEL, R., FIGUEROA, I., CORNIDE, H., & MUÑOZ, R. Enfoque de aplicación ágil con Scrum, Lean y Kanban. Ingeniare. Revista chilena de ingeniería [en línea]. 2021. [Fecha de consulta: 14 de junio 2022].

Disponible en: https://scielo.conicyt.cl/pdf/ingeniare/v29n1/0718-3305-ingeniare-29-01-141.pdf

GONÇALVES, L. The methodology to become more agile. Controlling & Management Review [en línea]. 2018.[Fecha de consulta: 04 de junio 2022].

Disponible en: https://sci-hubtw.hkvisa.net/10.1007/s12176-018-0020-3.

HERNÁNDEZ Sampieri, R., MENDOZA, C. Metodología de la investigación. [en línea]. D.F México: McGraw-Hill, 2018. [Fecha de consulta: 07 de mayo de 2022].

Disponible en:

http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

ISBN: 978-1-4562-6096-5

HUSÁK, Robert [et al.]. PeachPie: Mature PHP to CLI compiler. Journal of Computer Languages Volume 73 [en línea]. 2022 [Fecha de consulta: 10 de octubre de 2022].

Disponible en: https://doi.org/10.1016/j.cola.2022.101152

KADENIC, Maja Due, KOUMADITIS, Konstantinos y JUNKER, Louis. Mastering scrum with a focus on team maturity and key components of scrum. Department of Business Development and Technology, Aarhus University [en línea]. Abril 2022. [Fecha de consulta: 10 de octubre 2022].

Disponible en: https://doi.org/10.1016/j.infsof.2022.107079

Kuz, A., Falco, M., & Giandini, R. Comprendiendo la Aplicabilidad de Scrum en el Aula: Herramientas y Ejemplos. Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología [en línea], 2018. [Fecha de consulta: 20 de agosto 2022].

Disponible en: http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1850-99592018000100008

MARTÍNEZ Delgado, E., ROSARIO Garza Ríos, D., ACEVEDO, I., DALESSANDRO, E. y CÉSPEDES Valdivia, E. TITLE: Procedure for improving information systems for the establishment of a government information system. [en línea]. 2018. [Fecha de consulta: 26 de abril 2022].

Disponible en: https://search.ebscohost.com/login.aspx?direct=true&db=eue&AN=127823806&lang=es&site=eds-live.

MARTÍNEZ, P. La capacitación en Doctrina Operacional y las Competencias de los Oficiales Pilotos en un Componente Aéreo en el año 2020. Tesis de maestría. Lima: Fuerza aérea del Perú, 2021

Obtenido de: http://repositorio.fap.mil.pe/handle/fap/236

MASHAL, A., ROZILAWATI, R. An Empirical Study of Scrumban Formation based on the Selection of Scrum and Kanban Practices. International Journal on Advanced

Science, Engineering and Information Technology [en línea], 2018. [Fecha de consulta: 29 de junio 2022].

Disponible en: http://www.insightsociety.org/ojaseit/index.php/ijaseit/article/view/6566

MĹKVA, M., PRAJOVÁ, V., YAKIMOVICH, B., KORSHUNOV, A. y TYURIN, I. Standardization-one of the tools of continuous improvement. *Procedia Engineering* [en línea]. 2016. [Fecha de consulta: 06 de mayo 2022].

Disponible en: https://doi.org/10.1016/j.proeng.2016.06.674

MUÑOZ, L., Díaz, E., GALLEGO, S. The responsibilities arising from the use of information and communication technologies in health professional practice. Anales de Pediatría [en línea]. Mayo 2020. [Fecha de consulta: 17 de agosto 2022].

Disponible en : https://doi.org/10.1016/j.anpedi.2020.03.003

O'CONNOR, L. Modernización de Las Fuerzas Armadas del Perú: Organización y Diseño de la Fuerza Modernization of the Peruvian Armed Forces: Organization and Design of the Force. [en línea]. 2017 [Fecha de consulta: 04 de junio 2022].

Disponible en: https://www.recide.caen.edu.pe/index.php/recide/article/view/33.

OZDENIZCI, B. (2021). Business process management approach for improving agile software process and agile maturity. Journal of Software: Evolution and Process [en línea]. 2021. [Fecha de consulta: 10 de agosto 2022].

Disponible en: https://sci-hub.se/10.1002/smr.2331

PODRECCA [et al.]. Seguridad de la información y creación de valor: las implicaciones de rendimiento de ISO/IEC 27001. Departamento Politécnico de Ingeniería y Arquitectura, Universidad de Udine [en línea]. Noviembre 2022. [Fecha de consulta: 12 de agosto 2022].

Disponible en: https://doi.org/10.1016/j.compind.2022.103744

QUIROGA Pérez, N. Uso de los tics en el área de matemáticas de la Carrera. Fides Et Ratio [en línea]. 2018.[Fecha de consulta: 4 junio 2022].

Disponible en: http://www.scielo.org.bo/pdf/rfer/v15n15/v15n15_a09.pdf

Rasnacis, A., & Berzisa, S. Method for Adaptation and Implementation of Agile Project Management Methodology. Procedia Computer Science [en línea]. 2017. [Fecha de consulta: 21 de mayo 2022].

Disponible en: https://doi.org/10.1016/j.procs.2017.01.055

RODRIGUEZ [et al]. Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. Propósitos y representaciones [en línea]. Agosto 2020. [Fecha de consulta: 05 de diciembre 2022].

Disponible en: http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf

Santolaya-Perrin, R., García-Martín, Á., Carrero-Fernández, A. y Torres-Santos-Olmo, R. Experiencias del farmacéutico de hospital en el equipo pluridisciplinar en unidades especiales. Farmacia hospitalaria: órgano oficial de expresión científica de la Sociedad Española de Farmacia Hospitalaria [en línea]. 2020. [Fecha de consulta: 26 de abril 2022].

Disponible en: http://dx.doi.org/10.7399%2Ffh.11512

ISSN 21718695.

SARMIENTO, Gustavo, GONZALES, Richard. Implementación de la NTP/ISO 27001 para mejorar el proceso de seguridad de información en el departamento telemática de la oficina de economía del ejército del Perú. Tesis (Ingeniero de sistemas). Lima: Universidad Autónoma del Perú, 2019.

Disponible en: https://repositorio.autonoma.edu.pe/handle/20.500.13067/1039

TABARES, Breno G., DA SILVA Eduardo, Carlos, DE SOUZA, Adler. Risk management in scrum projects: A bibliometric study [en línea]. 2017. [Fecha de consulta: 05 de mayo de 2022].

Obtenido de: http://dx.doi.org/10.24138/jcomss.v13i1.241

ISSN: 18456421

TORROBA, Roberto, BARRERA, John. Protección de datos usando un sistema experimental de encriptación de correlador de transformada conjunta. Rev. Acad.

Colomb. Cienc. Ex. Fis. Nat. 39 [en línea]. Noviembre 2016. [Fecha de consulta: 07 de noviembre 2022].

Disponible en: http://dx.doi.org/10.18257/raccefyn.263

VALENCIA, Francisco., OROZCO, Mauricio. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Universidad Nacional de Colombia – Sede Manizales - Departamento de Informática y Computación [en línea]. Mayo 2017. [Fecha de consulta: 07 de agosto 2022].

Disponible en: https://scielo.pt/pdf/rist/n22/n22a06.pdf

ISSN: 1696-9895

VALENZUELA, Daniel. Algunos aspectos jurídicos del cifrado de comunicaciones. Universidad de Chile (Chile) [en línea]. 2019. [Fecha de consulta: 03 de julio 2022].

Disponible en: https://doi.org/10.18800/derechopucp.201902.008

VALLEJOS, Larry. Comparación de rendimiento de intercambio de datos con json encriptado. Tesis (Ingeniería de sistemas). Pimentel – Perú: Universidad Señor de Sipán, 2021.

Disponible en: https://repositorio.uss.edu.pe/handle/20.500.12802/9210

VELÁSQUEZ Restrepo, M., VAHOS Montoya, D., GÓMEZ Adasme, E., PINO Martínez, A., RESTREPO Zapata, J. y LONDOÑO Marín, S. Una revisión comparativa de la literatura acerca de metodologías tradicionales y modernas de desarrollo de software A comparative review about traditional and modern software development methodologies. Medellín-Colombia Revista CINTEX [en línea]. Diciembre 2019. [Fecha de consulta: 04 de junio 2022].

Disponible en: https://doi.org/10.33131/24222208.334

VÉRTIZ Osores, R.I., PÉREZ Saavedra, S., FAUSTINO Sánchez, M.A., VÉRTIZ-Osores, J.J. y Alain, L. Tecnología de la Información y Comunicación en estudiantes del nivel primario en el marco de la educación inclusiva en un Centro de Educación Básica Especial. Propósitos y Representaciones [en línea]. 2019. [Fecha de consulta: 04 de junio 2022].

Disponible en: http://dx.doi.org/10.20511/pyr2019.v7n1.266

VOLODYMYR, Rudnytskyi [et al]. Cryptographic encoding in modern symmetric and asymmetric encryption. University of Bielsko-Biala [en línea]. 2022, [Fecha de consulta: 08 noviembre 2022].

Disponible en: https://doi.org/10.1016/j.procs.2022.09.037

ZAWISLAK, Stanislaw [et al.]. Methods of crypto-stable symmetric encryption in the residual number system. Procedia Computer Science [en linea]. 2022. [Fecha de consulta: 05 de junio de 2022].

Disponible en: https://doi.org/10.1016/j.procs.2022.09.045

ZHONGCHENG, Lei [et al.]. Toward an international platform: A web-based multi-language system for remote and virtual laboratories using react framework. Department of Artificial Intelligence and Automation, Wuhan University, Wuhan [en linea]. Octubre 2022. [Fecha de consulta: 05 de noviembre de 2022].

Disponible en: https://doi.org/10.1016/j.heliyon.2022.e10780

BASIM, Abood [et al]. Data transmitted encryption for clustering protocol in heterogeneous wireless sensor networks. College of Computer Science and Information Technology, University of Sumer, Al-Rifai, Iraq [en linea]. Noviembre 2021 [Fecha de consulta: 28 de noviembre del 2022].

Disponible en: http://doi.org/10.11591/ijeecs.v25.i1.pp347-357

INTHRANI, Shammugam [et al]. Information security threats encountered by Malaysian public sector data centers. Razak Faculty of Technology and Informatics, UniversitiTeknologi Malaysia, Malaysia [en linea]. Diciembre 2020 [Fecha de consulta: 28 de noviembre del 2022].

Disponible en: http://doi.org/10.11591/ijeecs.v21.i3.pp1820-1829

NGUYEN, Van Tanh [et al]. The solution to improve information security for IoT networks by combining lightweight encryption protocols. International School-Vietnam National University, Hanoi, Vietnam [en linea]. Agosto 2021 [Fecha de consulta: 28 de noviembre del 2022].

Disponible en: http://doi.org/10.11591/ijeecs.v23.i3.pp1727-1735

PRONIKA, S. S. Tyagi. Performance analysis of encryption and decryption algorithm. Department of Computer Science & Engineering, Faculty of Engineering and Technology, Manav Rachna International Institute of Research & Studies, Haryana, India [en linea]. Julio 2021 [Fecha de consulta: 28 de noviembre del 2022].

Disponible en: http://doi.org/10.11591/ijeecs.v23.i2.pp1030-1038

JOMAR, L. [et al]. Application of advanced encryption standard in the computer or handheld online year-round registration system. Instruction Department, Southern Isabela College of Arts and Trades, Isabela, Philippines [en linea]. Junio 2022 [Fecha de consulta: 28 de noviembre del 2022].

Disponible en: http://doi.org/10.11591/ijeecs.v27.i2.pp922-935

## ANEXOS

### Anexo 1. Matriz de operacionalización

| Problema | Variables | Definición conceptual | Dimensión | Indicador | Índice | Escala |
|---|---|---|---|---|---|---|
| General:<br><br>¿En qué medida el proceso de encriptación influye en la seguridad de la información en el comando de control aeroespacial? | Proceso de encriptación | Se trata de envolver un mensaje utilizando un algoritmo matemático para que solo un destinatario legítimo pueda abrirlo y obtener su contenido mediante el uso de una clave única o clave que desenvuelve el mensaje. El propósito del cifrado es hacer que sea difícil de entender el mensaje a ojos de terceros ajenos a la comunicación (Valenzuela,2019). | Información | Mensajes cifrados Zawislak (2022, p. 5). | $\text{CME} = \sum_{i=1}^{n}$<br><br>CME: Cantidad de mensajes encriptados<br>n: mensajes | Razón |

| | | | | | | |
|---|---|---|---|---|---|---|
| Específico:<br>¿En qué medida el proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial?<br><br>¿En qué medida el proceso de encriptación incrementa la disponibilidad de la información en el comando de control aeroespacial?<br><br>¿En qué medida el proceso de encriptación incrementa la confidencialidad de la información en el comando de control aeroespacial? | Seguridad de la información | Incluye mantener su integridad, su confidencialidad y su disponibilidad de la información; están involucradas también otras más características como lo es responsabilidad, autenticidad, confiabilidad y no repudio (Calderón, 2016). | Rendimiento | Porcentaje de disponibilidad de la información dentro de la institución Sarmiento y Gonzales (2019, p. 11).<br><br>Porcentaje de confidencialidad de la información dentro de la institución Sarmiento y Gonzales (2019, p. 11). | [47-89] % | Razón |

**Anexo 2: Matriz de consistencia**

| Problema | Objetivos | Hipótesis | Variables | Metodología | Población y muestra |
|---|---|---|---|---|---|
| General:<br>¿En qué medida el proceso de encriptación influye en la seguridad de la información en el comando de control aeroespacial? | General:<br>Determinar en qué medida el proceso de encriptación influye en la seguridad de la información en el comando de control aeroespacial. | General:<br>El proceso de encriptación influirá de manera positiva en la seguridad de la información en el comando de control aeroespacial. | Independiente:<br>Proceso de encriptación | Tipo de investigación:<br>Aplicado | Población:<br>56 interacciones |
| PE1: ¿En qué medida el proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial? | OE1: Determinar en qué medida el proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial. | HE1: El proceso de encriptación incrementa los mensajes cifrados en el sistema del comando de control aeroespacial. | | | |
| PE2: ¿En qué medida el proceso de encriptación incrementa la disponibilidad de la | OE2: Determinar en qué medida el proceso de encriptación incrementa la disponibilidad de la | HE2: El proceso de encriptación incrementará la disponibilidad de la | | | |

| | | | | | |
|---|---|---|---|---|---|
| información en el comando de control aeroespacial? | información en el comando de control aeroespacial. | información en el comando de control aeroespacial. | | | |
| PE3: ¿En qué medida el proceso de encriptación incrementa la confidencialidad de la información en el comando de control aeroespacial? | OE3: Determinar en qué medida el proceso de encriptación incrementa la confidencialidad de la información en el comando de control aeroespacial. | HE3: El proceso de encriptación incrementará la confidencialidad de la información en el comando de control aeroespacial. | Dependiente: Seguridad de la información | Diseño de investigación: pre-experimental | Muestra: 49 interacciones |

**Anexo 3. Recolección de datos Pre – test**

Ficha de registro Pre – test para el indicador “Seguridad”

| | |
|---|---|
| N° de ficha de registro | 1 |
| Institución donde se investiga | COMANDO DE CONTROL AEROESPACIAL |
| Dirección | AVENIDA PERUANIDAD S/N JESÚS MARÍA |
| Proceso de observación | - Mensajes cifrados<br>- Porcentaje de disponibilidad de la información dentro de la institución<br>- Porcentaje de confidencialidad de la información dentro de la institución. |

| N° Interacción | Indicador 1: Mensajes cifrados | Indicador 2: Porcentaje de disponibilidad de la información (%) | Indicador 3: Porcentaje de confidencialidad de la información (%) |
|---|---|---|---|
| 1 | 0 | 53 | 0 |
| 2 | 0 | 59 | 0 |
| 3 | 0 | 27 | 0 |
| 4 | 0 | 52 | 0 |
| 5 | 0 | 49 | 0 |
| 6 | 0 | 45 | 0 |
| 7 | 0 | 20 | 0 |
| 8 | 0 | 41 | 0 |
| 9 | 0 | 33 | 0 |
| 10 | 0 | 54 | 0 |
| 11 | 0 | 36 | 0 |
| 12 | 0 | 36 | 0 |
| 13 | 0 | 45 | 0 |
| 14 | 0 | 60 | 0 |
| 15 | 0 | 40 | 0 |
| 16 | 0 | 54 | 0 |
| 17 | 0 | 38 | 0 |
| 18 | 0 | 35 | 0 |
| 19 | 0 | 26 | 0 |
| 20 | 0 | 24 | 0 |

| | | | |
|---|---|---|---|
| 21 | 0 | 24 | 0 |
| 22 | 0 | 42 | 0 |
| 23 | 0 | 20 | 0 |
| 24 | 0 | 30 | 0 |
| 25 | 0 | 27 | 0 |
| 26 | 0 | 38 | 0 |
| 27 | 0 | 60 | 0 |
| 28 | 0 | 55 | 0 |
| 29 | 0 | 49 | 0 |
| 30 | 0 | 57 | 0 |
| 31 | 0 | 20 | 0 |
| 32 | 0 | 26 | 0 |
| 33 | 0 | 58 | 0 |
| 34 | 0 | 52 | 0 |
| 35 | 0 | 36 | 0 |
| 36 | 0 | 27 | 0 |
| 37 | 0 | 37 | 0 |
| 38 | 0 | 60 | 0 |
| 39 | 0 | 29 | 0 |
| 40 | 0 | 34 | 0 |
| 41 | 0 | 29 | 0 |
| 42 | 0 | 55 | 0 |
| 43 | 0 | 57 | 0 |
| 44 | 0 | 55 | 0 |
| 45 | 0 | 28 | 0 |
| 46 | 0 | 24 | 0 |
| 47 | 0 | 30 | 0 |
| 48 | 0 | 52 | 0 |
| 49 | 0 | 58 | 0 |

ALEMAN SANTANA, JORGE ANTONIO

---

JEFE DE INFORMÁTICA

**Anexo 4. Recolección de datos Post – test**

Ficha de registro Post – test para el indicador “Seguridad”

| | |
|---|---|
| N° de ficha de registro | 1 |
| Institución donde se investiga | COMANDO DE CONTROL AEROESPACIAL |
| Dirección | AVENIDA PERUANIDAD S/N JESÚS MARÍA |
| Proceso de observación | - Mensajes cifrados<br>- Porcentaje de disponibilidad de la información dentro de la institución<br>- Porcentaje de confidencialidad de la información dentro de la institución. |

| N° Interacción | Indicador 1: Mensajes cifrados | Indicador 2: Porcentaje de disponibilidad de la información (%) | Indicador 3: Porcentaje de confidencialidad de la información (%) |
|---|---|---|---|
| 1 | 30 | 100 | 100 |
| 2 | 15 | 100 | 100 |
| 3 | 26 | 100 | 100 |
| 4 | 10 | 100 | 100 |
| 5 | 15 | 100 | 100 |
| 6 | 30 | 100 | 100 |
| 7 | 5 | 100 | 100 |
| 8 | 33 | 100 | 100 |
| 9 | 26 | 100 | 100 |
| 10 | 15 | 100 | 100 |
| 11 | 26 | 100 | 100 |
| 12 | 30 | 100 | 100 |
| 13 | 10 | 100 | 100 |
| 14 | 32 | 100 | 100 |
| 15 | 13 | 100 | 100 |
| 16 | 30 | 100 | 100 |
| 17 | 26 | 100 | 100 |
| 18 | 30 | 100 | 100 |
| 19 | 10 | 100 | 100 |
| 20 | 16 | 100 | 100 |
| 21 | 26 | 100 | 100 |

| | | | |
|---|---|---|---|
| 22 | 17 | 100 | 100 |
| 23 | 30 | 100 | 100 |
| 24 | 5 | 100 | 100 |
| 25 | 15 | 100 | 100 |
| 26 | 18 | 100 | 100 |
| 27 | 30 | 100 | 100 |
| 28 | 17 | 100 | 100 |
| 29 | 26 | 100 | 100 |
| 30 | 10 | 100 | 100 |
| 31 | 40 | 100 | 100 |
| 32 | 30 | 100 | 100 |
| 33 | 11 | 100 | 100 |
| 34 | 15 | 100 | 100 |
| 35 | 46 | 100 | 100 |
| 36 | 5 | 100 | 100 |
| 37 | 16 | 100 | 100 |
| 38 | 30 | 100 | 100 |
| 39 | 12 | 100 | 100 |
| 40 | 5 | 100 | 100 |
| 41 | 53 | 100 | 100 |
| 42 | 10 | 100 | 100 |
| 43 | 15 | 100 | 100 |
| 44 | 16 | 100 | 100 |
| 45 | 4 | 100 | 100 |
| 46 | 30 | 100 | 100 |
| 47 | 16 | 100 | 100 |
| 48 | 10 | 100 | 100 |
| 49 | 30 | 100 | 100 |

ALEMAN SANTANA, JORGE ANTONIO

---

JEFE DE INFORMÁTICA

## Anexo 5. Metodología scrum

### Acta de constitución del proyecto

Nombre del proyecto:

PROCESO DE ENCRIPTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL COMANDO DE CONTROL AEROESPACIAL BASADO EN ISO 27001

Información del proyecto:

| | |
|---|---|
| Nombre del proyecto | PROCESO DE ENCRIPTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL COMANDO DE CONTROL AEROESPACIAL BASADO EN ISO 27001 |
| Fecha de elaboración | 03 / 09 / 22 |
| Cliente | Fuerza Aérea del Perú |
| Patrocinador principal | |
| Director o jefe del proyecto | Aleman Santana Jorge Antonio |

### Descripción del proyecto

Desarrollar un sistema web donde se pueda realizar intercambio de comunicación entre los integrantes del COMCA (Comando de control aeroespacial), el detalle que contará es que los mensajes recibidos y enviados estarán cifrados evitando así la baja seguridad.

### Presupuesto estimado

| Concepto | Unidad | Cantidad | Costo por unidad | Costo Total |
|---|---|---|---|---|
| *Recursos humanos* | | | | |
| Asesor metodólogo | Servicio | 1 | S/0.00 | S/0.00 |
| **Sub-Total recursos humanos** | | | | **S/0.00** |

| | | | | |
|---|---|---|---|---|
| *Equipos y bienes duraderos* | | | | |
| Laptop | Unidad | 1 | S/1900.00 | S/1900.00 |
| Impresoras | Unidad | 1 | S/180.00 | S/180.00 |
| **Sub-total materiales** | | | | **S/2080.00** |
| *Materiales e insumos* | | | | |
| Lapicero | Paquete | 1 | S/12.00 | S/12.00 |
| Hojas blancas | Paquete | 1 | S/15.00 | S/15.00 |
| Pendrive | Unidad | 1 | S/40.00 | S/40.00 |
| **Sub-total materiales** | | | | **S/67.00** |
| *Gastos operativos* | | | | |
| Transporte | Servicio | 4 | S/30.00 | S/120.00 |
| Fotocopias | Unidad | 50 | S/0.10 | S/5.00 |
| Servidor Host | Unidad | 1 | S/160.00 | S/160.00 |
| **Sub-total materiales** | | | | **S/285.00** |
| **Total** | | | | **S/2432.00** |

## Diagrama de Gantt

*Figura 7:* Diagrama de Gantt de la tesis.

| | | | | |
|---|---|---|---|---|
| **PROCESO DE ENCRIPTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN EN EL COMANDO DE CONTROL AEROESPACIAL DE LA FUERZA AEREA DEL PERÚ BASADO EN ISO 27001** | **85 días** | **sáb 3/09/22** | **sáb 10/12/22** | |
| Realización de Pre-test | 2 días | sáb 3/09/22 | lun 5/09/22 | |
| **Fase inicial** | **7 días** | **lun 5/09/22** | **lun 12/09/22** | **2** |
| Recopilación de requerimientos | 3 días | lun 5/09/22 | mié 7/09/22 | |
| Análisis de requerimientos | 3 días | jue 8/09/22 | sáb 10/09/22 | 4 |
| Definición de funcionamiento | 1 día | lun 12/09/22 | lun 12/09/22 | 5 |
| **Diseño** | **20 días** | **mar 13/09/22** | **mié 5/10/22** | **3** |
| Diagrama de casos de uso | 2 días | mar 13/09/22 | mié 14/09/22 | |
| Modelado de Base de Datos | 12 días | jue 15/09/22 | mié 28/09/22 | |
| Realización de prototipo | 6 días | jue 29/09/22 | mié 5/10/22 | 9 |
| **Ejecución** | **49 días** | **jue 6/10/22** | **jue 1/12/22** | **7** |
| Creación de tablas de la base de datos | 5 días | jue 6/10/22 | mar 11/10/22 | |
| **Codificación del sistema** | **44 días** | **mié 12/10/22** | **jue 1/12/22** | **12** |
| **Definición del primer sprint** | **15 días** | **mié 12/10/22** | **vie 28/10/22** | |
| Avance del sprint | 11 días | mié 12/10/22 | lun 24/10/22 | |
| Presentación y/o aceptación | 1 día | mar 25/10/22 | mar 25/10/22 | 15 |
| Levantamiento de observaciones | 2 días | mié 26/10/22 | jue 27/10/22 | 16 |
| Cierre de sprint | 1 día | vie 28/10/22 | vie 28/10/22 | 17 |
| **Definición del segundo sprint** | **15 días** | **sáb 29/10/22** | **mar 15/11/22** | **14** |
| Avance del sprint | 11 días | sáb 29/10/22 | jue 10/11/22 | |
| Presentación y/o aceptación | 1 día | vie 11/11/22 | vie 11/11/22 | 20 |
| Levantamiento de observaciones | 2 días | sáb 12/11/22 | lun 14/11/22 | 21 |

| | | | | |
|---|---|---|---|---|
| Cierre de sprint | 1 día | mar 15/11/22 | mar 15/11/22 | 22 |
| **Definición del tercer sprint** | **14 días** | **mié 16/11/22** | **jue 1/12/22** | **19** |
| Avance del sprint | 10 días | mié 16/11/22 | sáb 26/11/22 | |
| Presentación y/o aceptación | 1 día | lun 28/11/22 | lun 28/11/22 | 25 |
| Levantamiento de observaciones | 2 días | mar 29/11/22 | mié 30/11/22 | 26 |
| Cierre de sprint | 1 día | jue 1/12/22 | jue 1/12/22 | 27 |
| **Pruebas** | **5 días** | **vie 2/12/22** | **mié 7/12/22** | **11** |
| Ejecución de plan de pruebas según los requisitos del sistema | 4 días | vie 2/12/22 | mar 6/12/22 | |
| Realización de Post-test | 1 día | jue 8/12/22 | jue 8/12/22 | 29 |
| Implementación | 2 días | vie 9/12/22 | sáb 10/12/22 | 31 |
| **Cierre del proyecto** | **1 día** | **sáb 10/12/22** | **sáb 10/12/22** | **32** |
| Finalización del desarrollo del proyecto de investigación | 1 día | sáb 10/12/22 | sáb 10/12/22 | |

*Fuente*: Elaboración propia

## EJECUCIÓN DEL PROYECTO

La ejecución del proyecto se llevó a cabo mediante la metodología ágil Scrum, aprovechando su enfoque dinámico al momento de realizar un proyecto, centrándose en iteraciones rápidas satisfaciendo al cliente con entregas tempranas y continuas del producto con valor, evitando resultados finales insatisfactorios.

| ROL | PERSONAL A CARGO | DESCRIPCIÓN |
|---|---|---|
| Control de calidad | Alemán Santana Jorge Antonio | Se asegura que se cumplan las normas, se verifica que los entregables del proyecto estén dentro de los límites de calidad pre-establecidos |
| Analista | Oliva Rivera Mitchael Ever | Se encarga de reporta al gerente de proyecto en la revisión de propuestas, informes y presentaciones del proyecto a su vez se asegura que el proyecto esté cumpliendo las metas y objetivos propuestos. |
| Programador | Cabellos Dionicio Jhojan Enoc | Persona que escribe, depura y mantiene el código fuente de un programa informático, que ejecuta el hardware de una computadora, para realizar una tarea determinada. |
| Programador de BD | Cabellos Dionicio Jhojan Enoc | Implementar, dar soporte y gestionar bases de datos del sistema. Crear y configurar bases de datos relacionales a la vez ser responsables de la integridad de los datos y la disponibilidad. |

Los roles se definieron en base a las capacidades de cada persona: Alemán Santana Jorge Antonio se ha desenvuelto como Control de calidad debido a su conocimiento en el campo de normativas de los requerimientos de usuarios, asimismo el rol de Analista ha estado a cargo de Oliva Rivera Mitchael Ever, debido a su especialización en la metodología Scrum, por lo cual dirige y apoya al equipo en el uso de la metodología. Como equipo de programación únicamente participo Cabellos Dionicio Jhojan Enoc, encargado de la programación y de la base de datos de la aplicación, así como la ejecución de las pruebas a cargo de Oliva Rivera Mitchael Ever, teniendo en consideración de que la cantidad de participantes pueda incrementarse en el futuro.

**Historias de usuarios**

**Tabla 11 :** *Historia de usuario 1.*

| Historia de usuarios | | Prioridad | T. estimado |
|---|---|---|---|
| Número: 1 | Usuario: Usuarios todos | 1 | 3 días |
| Nombre de historia: Login de ingreso. | | | |
| Programador: Oliva Rivera Mitchael, Cabellos Dionicio Jhojan | | | |
| Descripción: | El sistema debe contar con una sección donde se pueda verificar a los usuarios en general. | | |
| Restricciones: | Llenar obligatoriamente todos los campos | | |

Fuente: Elaboración propia

**Tabla 12 :** *Historia de usuario 2.*

| Historia de usuarios | | Prioridad | T. estimado |
|---|---|---|---|
| Número: 2 | Usuario: Administrador | 1 | 3 días |
| Nombre de historia: Módulo administrador. | | | |
| Programador: Oliva Rivera Mitchael, Cabellos Dionicio Jhojan | | | |
| Descripción: | El sistema debe contar con una sección donde se pueda verificar a los usuarios en general, donde podrá gestionarlos. | | |
| Restricciones: | Solo cuando se ingresa en modo administrador. | | |

Fuente: Elaboración propia

**Tabla 13 :** *Historia de usuario 3.*

| Historia de usuarios | | Prioridad | T. estimado |
|---|---|---|---|
| Número: 3 | Usuario: Administrador | 1 | 3 días |
| Nombre de historia: Módulo registro y edición. | | | |
| Programador: Oliva Rivera Mitchael, Cabellos Dionicio Jhojan | | | |
| Descripción: | El sistema contará con un registro de nuevos usuarios donde la contraseña se guardará de manera cifrada y cada usuario podrá editar sus datos en caso de ser necesario. | | |
| Restricciones: | Solo cuando se ingresa en modo administrador. | | |

Fuente: Elaboración propia

**Tabla 14 :** *Historia de usuario 4.*

| Historia de usuarios | | Prioridad | T. estimado |
|---|---|---|---|
| Número: 4 | Usuario: Usuarios todos | 2 | 14 días |
| Nombre de historia: Módulo salas de chat. | | | |
| Programador: Oliva Rivera Mitchael, Cabellos Dionicio Jhojan | | | |
| Descripción: | El sistema permitirá crear salas de chat donde se deberá incorporar una contraseña de seguridad. | | |
| Restricciones: | El ingreso de la contraseña será opcional. | | |

Fuente: Elaboración propia

**Tabla 15 :** *Historia de usuario 5.*

| Historia de usuarios | | Prioridad | T. estimado |
|---|---|---|---|
| Número: 5 | Usuario: Usuarios todos | 2 | 4 días |
| Nombre de historia: Módulo verificación. | | | |
| Programador: Oliva Rivera Mitchael, Cabellos Dionicio Jhojan | | | |
| Descripción: | El sistema pedirá contraseña para el ingreso a las salas de chat a excepción de cuando hayan sido agregados. | | |
| Restricciones: | Ninguna. | | |

Fuente: Elaboración propia

**Tabla 16 :** *Historia de usuario 6.*

| Historia de usuarios | | Prioridad | T. estimado |
|---|---|---|---|
| Número: 6 | Usuario: Usuarios todos | 3 | 4 días |
| Nombre de historia: Módulo de encriptación. | | | |
| Programador: Oliva Rivera Mitchael, Cabellos Dionicio Jhojan | | | |
| Descripción: | Los mensajes enviados dentro de las salas de chat serán encriptados o cifrados. | | |
| Restricciones: | Ninguna. | | |

Fuente: Elaboración propia

**Pila de producto**

**Tabla 17 :** *Requerimientos funcionales.*

| ITEM | REQUERIMIENTOS FUNCIONALES | HISTORIAS | T. E | PRIORIDAD |
|---|---|---|---|---|
| RQF01 | Contar con una ventana de inicio de sesión, se accederá con id y contraseña. | H1 | 3 días | 1 |
| RQF02 | Contar con una sección de registros de nuevos usuarios. | H2 | 3 días | 2 |
| RQF03 | La contraseña se deberá guardar de manera encriptada. | H3 | 3 días | 1 |
| RQF04 | Realizará la creación de sala de chat con una contraseña. | H4 | 8 días | 1 |
| RQF05 | Los miembros de la sala de chat podrán agregar a nuevos miembros. | H3 | 5 días | 2 |
| RQF06 | Los miembros podrán ingresar a la sala de chat ingresando la contraseña de la misma. | H5 | 3 días | 2 |
| RQF07 | Los mensajes enviados dentro de la sala de chat serán guardados de manera encriptada o cifrada. | H6 | 14 días | 1 |
| RQF08 | Los usuarios tendrán opción a editar sus datos. | H4 | 5 días | 3 |

Fuente: Elaboración propia

**Requerimientos no funcionales**

**Tabla 18 :** *Requerimientos no funcionales.*

| ÍTEM | REQUERIMIENTOS NO FUNCIONALES |
|---|---|
| RQNF01 | El sistema debe de ser lo suficientemente intuitivo para usuarios iniciados en informática puedan tener una curva de aprendizaje corta |
| RQNF02 | Las interfaces del sistema deben ser amigable e intuitiva |
| RQNF03 | Facilidad de análisis y modificación en caso de fallas de ingreso |
| RQNF04 | El sistema debe de estar disponible 24 x 7 y accedido de forma independiente |
| RQNF05 | La aplicación debe mantener los datos seguros y protegidos |

Fuente: Elaboración propia

**Definición de Sprint**

***Tabla 19:*** *Definición de sprint*

| SPRINT | REQUERIMIENTOS | ESTIMACIÓN |
|---|---|---|
| Sprint 1 | RQF01, RQF02, RQF03, RQF04, RQF06. | 15 días |
| Sprint 2 | RQF04, RQF05, RQF08. | 15 días |
| Sprint 3 | RQF07. | 14 días |

Fuente: Elaboración propia

**Sprint backlog**

***Tabla 20:*** *Sprint backlog*

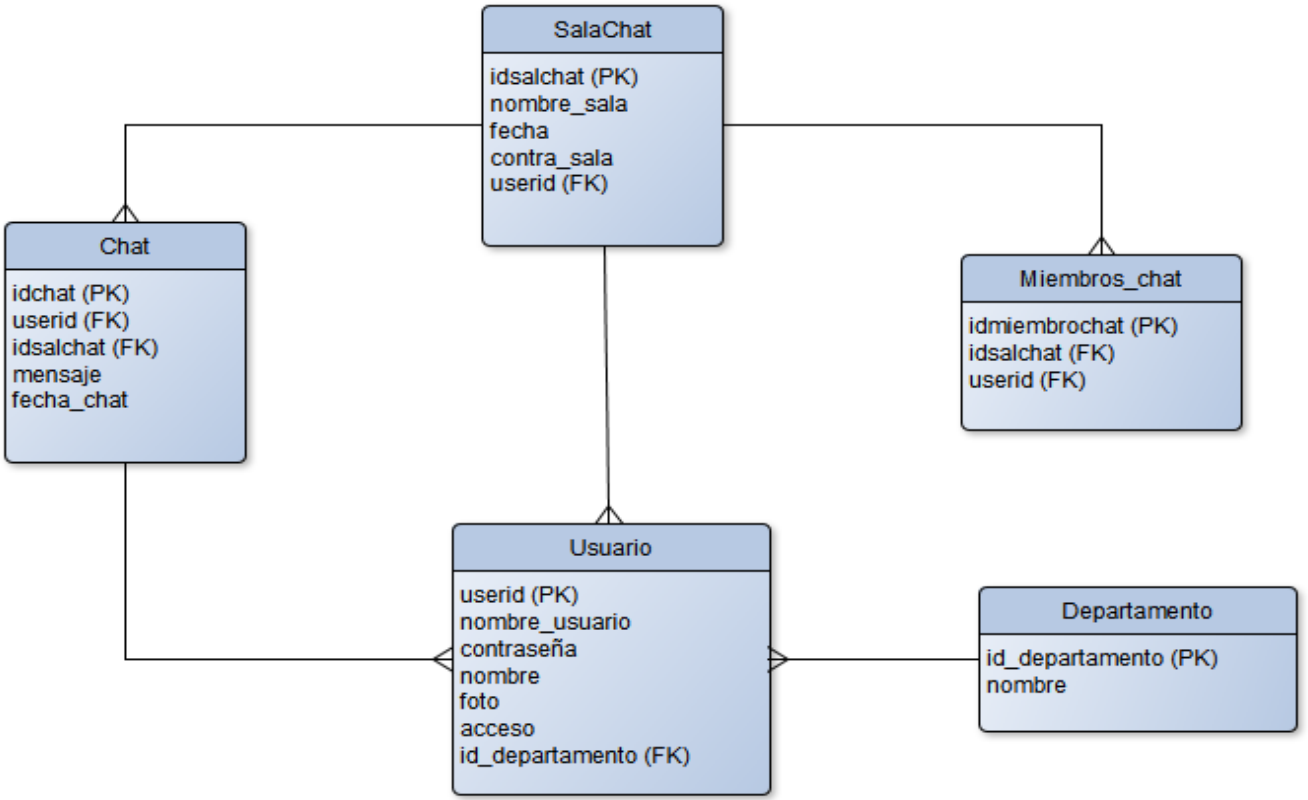
| **N° SPRINT** | **REQ. FUNCIONALES** | **HISTORIAS** | **TIEMPO REAL** | **PRIORIDAD** |
|---|---|---|---|---|
| SPRINT 1 | RQF01: Contar con una ventana de inicio de sesión, se accederá con id y contraseña. | H1 | 3 días | 1 |
| | RQF02: Contar con una sección de registros de nuevos usuarios. | H2 | 3 días | 2 |
| | RQF03: La contraseña se deberá guardar de manera encriptada. | H3 | 3 días | 1 |
| | RQF06: Los miembros podrán ingresar a la sala de chat ingresando la contraseña de la misma. | H4 | 3 días | 2 |
| SPRINT 2 | RQF05: Los miembros de la sala de chat podrán agregar a nuevos miembros. | H3 | 5 días | 2 |
| | RQF04: Realizará la creación de sala de chat con una contraseña. | H5 | 6 días | 1 |
| | RQF08: Los usuarios tendrán opción a editar sus datos. | H6 | 3 días | 3 |
| SPRINT 3 | RQF07: Los mensajes enviados dentro de la sala de chat serán guardados de manera encriptada o cifrada. | H4 | 12 días | 1 |

Fuente: Elaboración propia

*Figura 8:* Caso de uso.

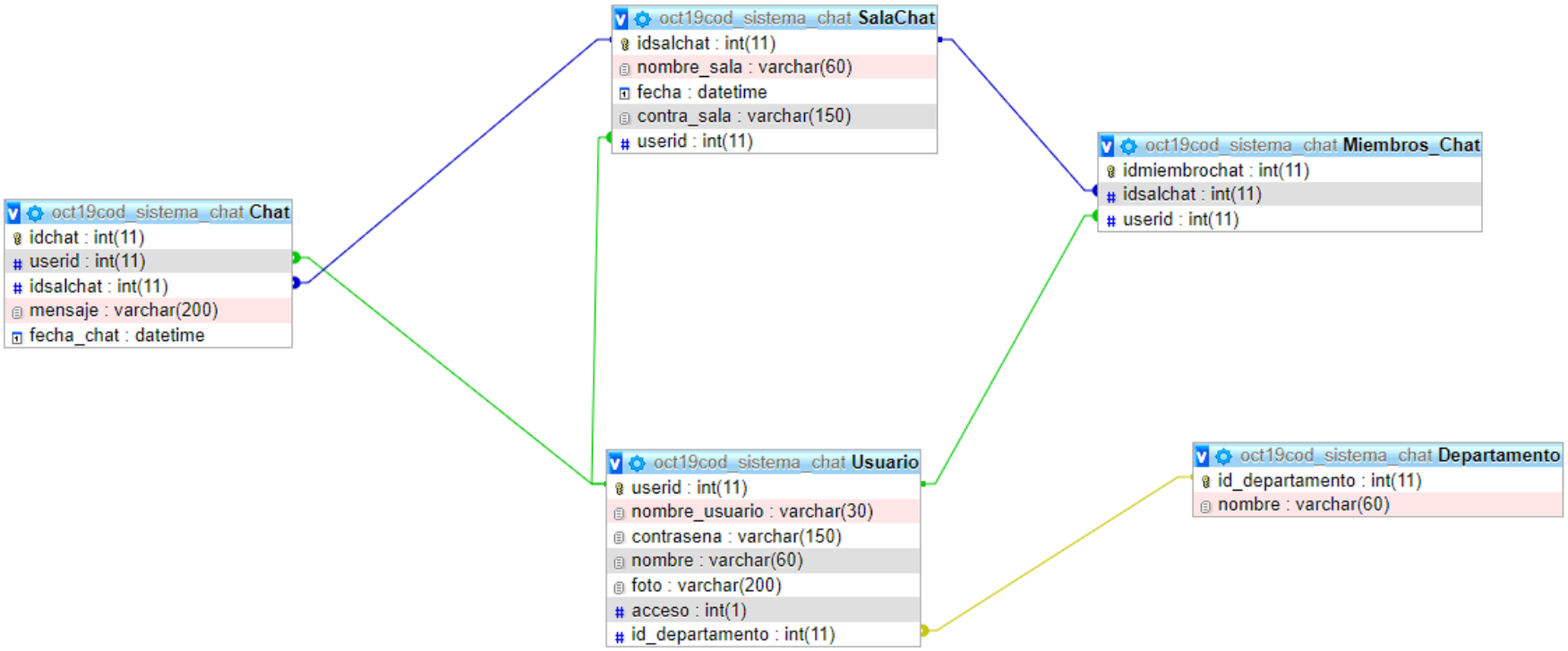

*Fuente*: Elaboración propia

*Figura 9:* Diagrama lógico de base de datos.




*Fuente*: Elaboración propia

*Figura 10:* Diagrama físico de base de datos.




*Fuente*: Elaboración propia

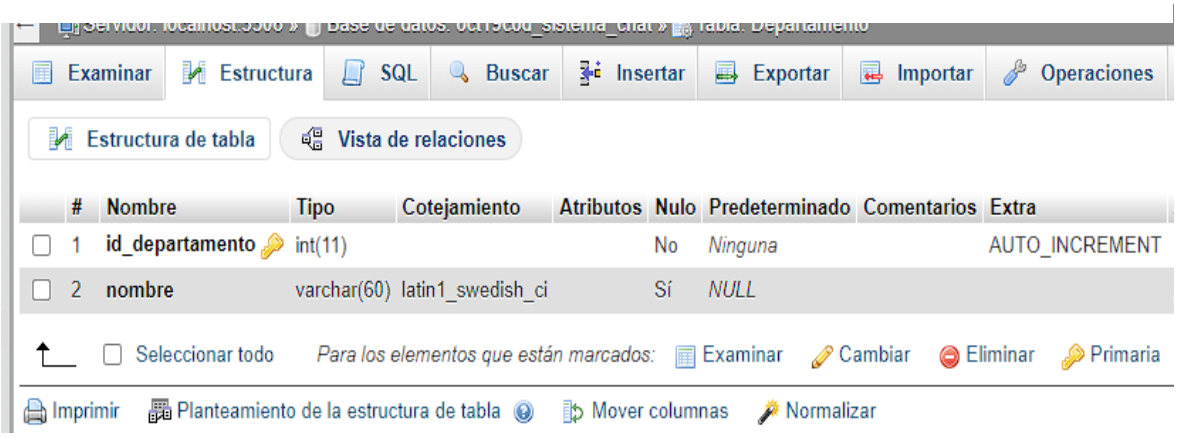
## Diccionario de la base de datos

*Figura 11:* Diccionario de la tabla Usuario.


| # | Nombre | Tipo | Cotejamiento | Atributos | Nulo | Predeterminado | Comentarios | Extra |
|---|---|---|---|---|---|---|---|---|
| 1 | **userid** | int(11) | | | No | *Ninguna* | | AUTO_INCREMENT |
| 2 | **nombre_usuario** | varchar(30) | latin1_swedish_ci | | Sí | *NULL* | | |
| 3 | **contrasena** | varchar(150) | latin1_swedish_ci | | Sí | *NULL* | | |
| 4 | **nombre** | varchar(60) | latin1_swedish_ci | | Sí | *NULL* | | |
| 5 | **foto** | varchar(200) | latin1_swedish_ci | | Sí | *NULL* | | |
| 6 | **acceso** | int(1) | | | Sí | *NULL* | | |
| 7 | **id_departamento** | int(11) | | | Sí | *NULL* | | |

*Fuente*: Elaboración propia

*Figura 12:* Diccionario de la tabla Departamento.




| # | Nombre | Tipo | Cotejamiento | Atributos | Nulo | Predeterminado | Comentarios | Extra |
|---|---|---|---|---|---|---|---|---|
| 1 | **id_departamento** | int(11) | | | No | *Ninguna* | | AUTO_INCREMENT |
| 2 | **nombre** | varchar(60) | latin1_swedish_ci | | Sí | *NULL* | | |

*Fuente*: Elaboración propia

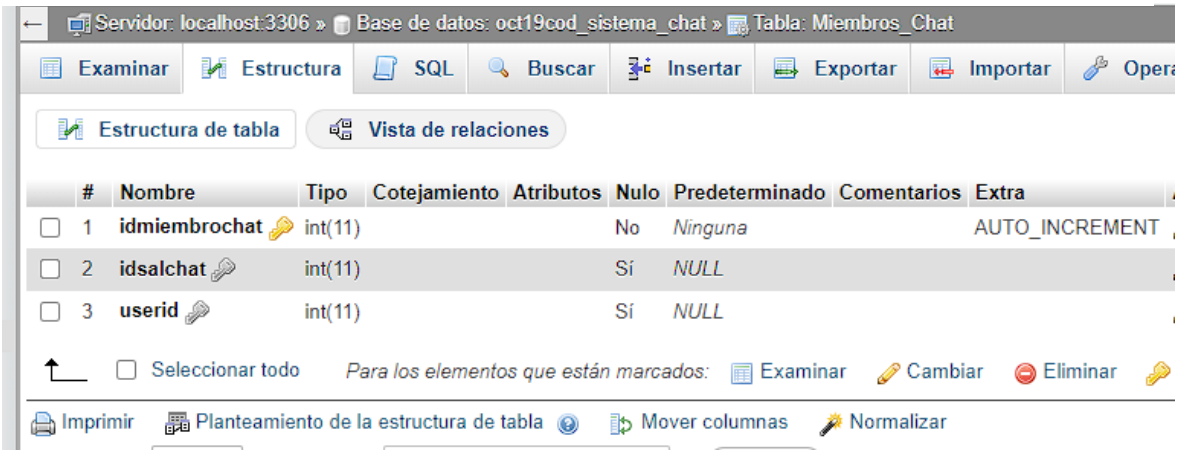
*Figura 13:* Diccionario de la tabla SalaChat.


*Fuente*: Elaboración propia

*Figura 14:* Diccionario de la tabla Chat.


*Fuente*: Elaboración propia

*Figura 15:* Diccionario de la tabla Miembros_Chat.




*Fuente*: Elaboración propia

**Sprint 1**

**Acta de inicio del Sprint 1**

ACTA DE INICIO: REUNIÓN DEL SPRINT 1

**Fecha:** 12 / 10 / 2022

| Rol | Persona |
|---|---|
| **Control de calidad** | Alemán Santana Jorge Antonio |
| **Analista** | Oliva Rivera Mitchael Ever |
| **Programador** | Cabellos Dionicio Jhojan Enoc |
| **Programador de BD** | Cabellos Dionicio Jhojan Enoc |

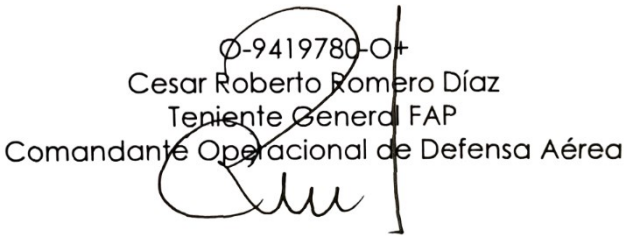
En la ciudad de Lima, Jesús María, a los doce días del mes de octubre del presente año en cumplimiento con los puntos establecidos en el plan de trabajo para el adecuado desarrollo de" Proceso de encriptación para la seguridad de la información en el Comando de Control Aeroespacial basado en ISO 27001" se realizará la carta de aprobación para el desarrollo de los cumplimientos funcionales correspondientes al Sprint 1.

Los elementos de la lista del entregable son:

| Sprint 01 | Nombre de la historia de usuario |
|---|---|
| **Crear interfaz del sistema** | Login de ingreso. |
| **Ingreso modo administrador** | Módulo administrador |
| **Ingreso modo usuario** | Módulo salas de chat. |

Luego de la verificación de las funcionalidades a desarrollar correspondiente al Sprint 1, el teniente general FAP manifiesta su total satisfacción y conformidad del producto de software el cual se desarrollará, y será entregado el 20 de octubre del 2022.

En muestra de aceptación y conformidad se procede a firmar la presente acta



# ACTA DE PRUEBAS FUNCIONALES DEL SPRINT 1

<table>
<tr><td colspan="6">PRUEBA FUNCIONAL</td></tr>
<tr><td>PRUEBA N°</td><td colspan="2">Sprint 01</td><td>VERSION DE EJECUCIÓN</td><td colspan="2">PFS-01</td></tr>
<tr><td></td><td colspan="2"></td><td>FECHA DE EJECUCIÓN</td><td colspan="2">20/10/2022</td></tr>
<tr><td>TAREA</td><td colspan="2">Sprint 01</td><td>MODELO DEL SISTEMA</td><td colspan="2">PF01</td></tr>
<tr><td>Descripción del caso de prueba:</td><td colspan="5"></td></tr>
<tr><td colspan="6">1. CASO DE PRUEBA</td></tr>
<tr><td colspan="6">a. Precondiciones</td></tr>
<tr><td colspan="6">• Recolección de requerimientos<br>• BD creado</td></tr>
<tr><td colspan="6">b. Pasos de la prueba</td></tr>
<tr><td colspan="6">• Verificación de requerimientos<br>• Ingresar con credenciales de administrador<br>• Verificar si el ingreso es correcto<br>• Ingresar con credenciales de usuario<br>• Verificar si el ingreso es correcto</td></tr>
<tr><td colspan="3">DATOS DE ENTRADA</td><td rowspan="2">RESPUESTA ESPERADA DE LA APLICACIÓN</td><td colspan="2">COINCIDE</td><td rowspan="2">RESPUESTA DEL SISTEMA</td></tr>
<tr><td>CAMPO</td><td>VALOR</td><td>TIPO ESCENARIO</td><td>SI</td><td>NO</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Entrada al sistema</td><td>X</td><td></td><td>Ingreso correcto</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Ingreso modo administrador</td><td>X</td><td></td><td>Bienvenido administrador</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Ingreso modo usuario</td><td>X</td><td></td><td>Bienvenido usuario</td></tr>
<tr><td colspan="6">c. Post condiciones</td></tr>
<tr><td colspan="6">Aplicada</td></tr>
<tr><td colspan="6">2. RESULTADO DE LA PRUEBA</td></tr>
<tr><td colspan="5">Defectos de desviaciones</td><td>Veredicto</td></tr>
<tr><td colspan="5">-</td><td>APROBADO<br>FALLADO</td></tr>
<tr><td colspan="3">Observaciones</td><td colspan="3">Probador</td></tr>
<tr><td colspan="3">-</td><td>Nombre: Alemán Santana Jorge Antonio<br>Fecha: 20/10/2022</td><td colspan="2">Ø-9419780-O+<br>Cesar Roberto Romero Díaz<br>Teniente General FAP<br>Comandante Operacional de Defensa Aérea</td></tr>
</table>

**Acta de cierre del Sprint 1**

ACTA DE REUNION DE CIERRE DEL SPRINT 1

Fecha: 20 / 10 / 2022

Datos:

| **Empresa** | **Fuerza Aérea del Perú** |
|---|---|
| **Proyecto** | Proceso de encriptación para la seguridad de la información en el Comando de Control Aeroespacial basado en ISO 27001 |

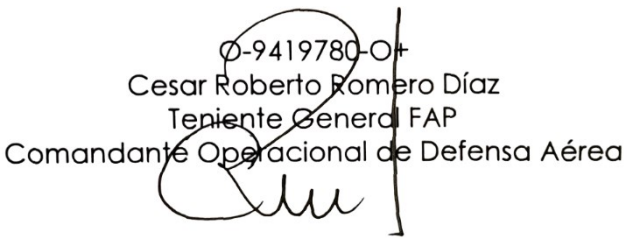
Participantes:

| **Rol** | **Persona** |
|---|---|
| **Control de calidad** | Alemán Santana Jorge Antonio |
| **Analista** | Oliva Rivera Mitchael Ever |
| **Programador** | Cabellos Dionicio Jhojan Enoc |
| **Programador de BD** | Cabellos Dionicio Jhojan Enoc |

Acuerdos:

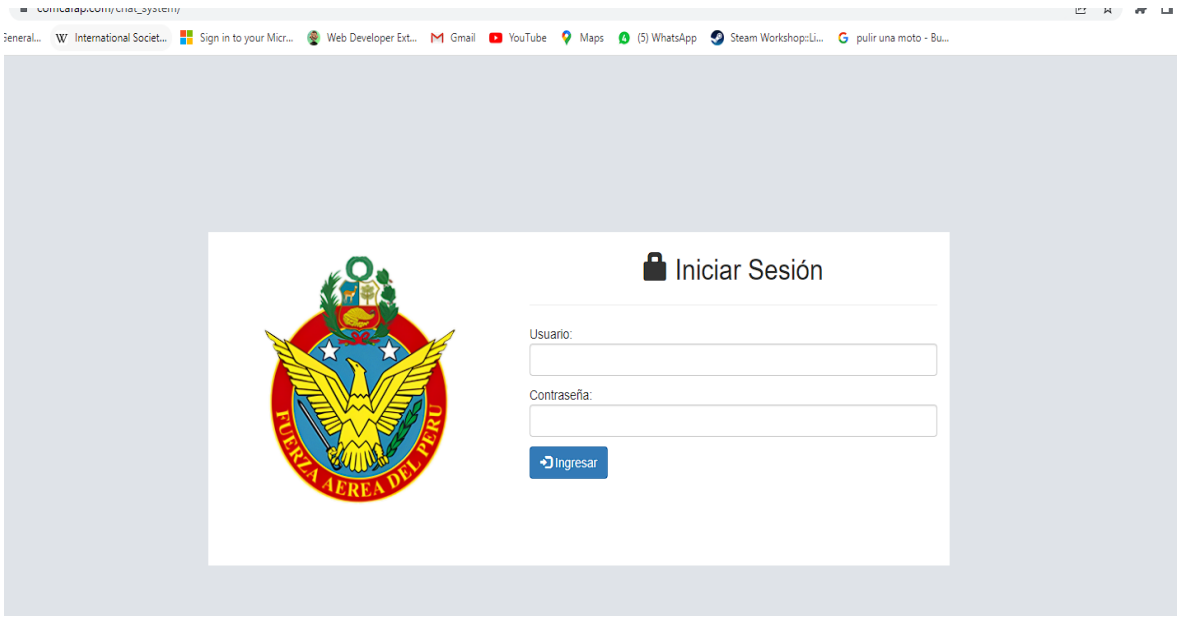
Marca con una “x” por los motivos de cierre, con lo referente a lo acordado sobre las funcionalidades del Sprint actual.

| **Nombre de la historia de usuario** | **No entrega** | **Entrega parcial** | **Entrega completa** |
|---|---|---|---|
| **Login de ingreso.** | | | X |
| **Módulo administrador** | | | X |
| **Módulo salas de chat.** | | | X |



## Interfaz del sistema

*Figura 16:* Crear interfaz del sistema.




*Fuente*: Elaboración propia

*Figura 17:* Código de interfaz del sistema.

```
    }
</style>
</head>
<body style="background-color:#DFE3E8">
    <br><br><br><br><br><br>
<div class="container-fluid" bg-white>
    <div id="login_form" style="background-color:white">
        <div class="form-group">
        <div class="col-sm-5 mb-3 mb-sm-0">
           <center><img src="img/fap.png" width="330" height="330" align="center"></center>
        </div>
        <div class="col-sm-7 mb-3 mb-sm-0">
        <h2><center><span class="glyphicon glyphicon-lock"></span> Iniciar Sesi贺n</center></h2>
        <hr>
        <form method="POST" action="login.php">
        Usuario: <input type="text" name="usuario" class="form-control" required>
        <div style="height: 10px;"></div>
        Contrase幅a: <input type="password" name="contrasena" class="form-control" required>
        <div style="height: 10px;"></div>
        <button type="submit" class="btn btn-primary"><span class="glyphicon glyphicon-log-in"></span> Ingresar</button><
        </form>
        <div style="height: 15px;"></div>
        <div style="color: red; font-size: 15px;">
            <center>
            <?php
                session_start();
                if(isset($_SESSION['msj'])){
                    echo $_SESSION['msj'];
                    unset($_SESSION['msj']);
                }
            ?>
            </center>
        </div>
```

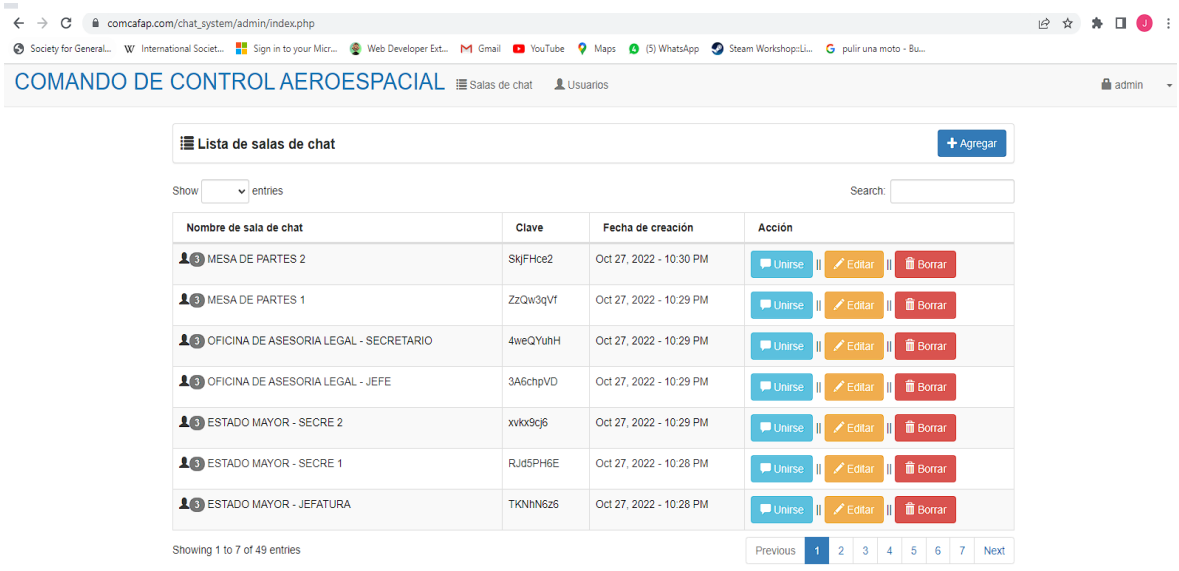
*Fuente*: Elaboración propia

*Figura 18:* Código autenticación de ingreso.

```php
if (!preg_match("/^[a-zA-Z0-9_]*$/",$usuario)) {
    $_SESSION['msj'] = "El nombre de usuario no debe contener espacios ni caracteres especiales!";
    header('location: index.php');
}
else{

$nusuario=$usuario;

$contrasena = check_input($_POST["contrasena"]);
$ncontrasena=md5($contrasena);

$query=mysqli_query($conn,"select * from `Usuario` where nombre_usuario='$nusuario' and contrasena='$ncontrasena'");

if(mysqli_num_rows($query)==0){
    $_SESSION['msj'] = "Inicio de sesi贸n fallido, entrada no v谩lida!";
    header('location: index.php');
}
else{

    $row=mysqli_fetch_array($query);
    if ($row['acceso']==1){
        $_SESSION['id']=$row['userid'];
        ?>
        <script>
            window.alert('Inicio de sesion exitoso, bienvenido administrador!');
            window.location.href='administrador/';
        </script>
        <?php
    }
    else{
        $_SESSION['id']=$row['userid'];
        ?>
        <script>
            window.alert('Inicio de sesion exitoso, bienvenido usuario!');
            window.location.href='usuario/';
        </script>
```

*Fuente*: Elaboración propia

*Figura 19:* Ingreso modo administrador.



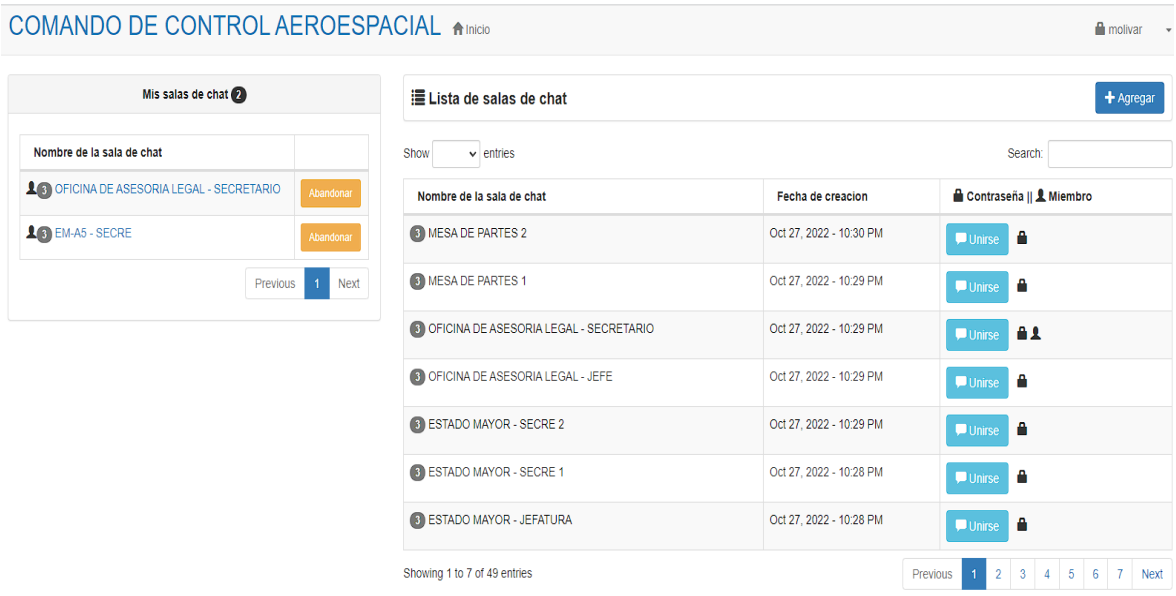

*Fuente*: Elaboración propia

*Figura 21:* Código de interfaz administrador.

```php
<?php include('session.php'); ?>
<?php include('header.php'); ?>
<body>
<?php include('navegar.php'); ?>
<div class="container">
    <div class="row">
        <?php include('ListasChat.php'); ?>
    </div>
</div>
<?php include('modal_index.php'); ?>
<?php include('modal_cuenta.php'); ?>

<script src="../js/jquery.dataTables.min.js"></script>
<script src="../js/dataTables.bootstrap.min.js"></script>
<script src="../js/dataTables.responsive.js"></script>
<script>
$(document).ready(function(){

    $('#SalaChat').DataTable({
    "bLengthChange": true,
    "bInfo": true,
    "bPaginate": true,
    "bFilter": true,
    "bSort": false,
    "pageLength": 7
    });

    $(document).on('click', '#agregarsalachat', function(){
        nombrechat=$('#nombre_chat').val();
        contrachat=$('#contra_chat').val();
            $.ajax({
                url:"agregar_salachat.php",
                method:"POST",
                data:{
                    nombrechat: nombrechat,
                    contrachat: contrachat,
                },
                success:function(data){
```

*Fuente*: Elaboración propia

*Figura 20:* Ingreso modo usuario.




*Fuente*: Elaboración propia

*Figura 22:* Código de interfaz usuario.

```
<?php include('session.php'); ?>
<?php include('header.php'); ?>
<body>
<?php include('navegar.php'); ?>
<div class="container-fluid">
    <div class="row">
        <?php include('mischats.php'); ?>
        <?php include('ListasChat.php'); ?>
    </div>
</div>
<?php include('modal_cuenta.php'); ?>
<?php include('modal_index.php'); ?>
<?php include('modal_mischats.php'); ?>
<?php include('modal_sala.php'); ?>

<script src="../js/jquery.dataTables.min.js"></script>
<script src="../js/dataTables.bootstrap.min.js"></script>
<script src="../js/dataTables.responsive.js"></script>
<script>
$(document).ready(function(){

    $('#SalasChat').DataTable({
    "bLengthChange": true,
    "bInfo": true,
    "bPaginate": true,
    "bFilter": true,
    "bSort": false,
    "pageLength": 7
    });

    $('#misSalasChat').DataTable({
    "sDom": '<"row view-filter"<"col-sm-12"<"pull-left"l><"pull-right"f><"clearfix">>>t<"row view-pager"<"col-sm-12"<"text-center"ip>>>',
    "bLengthChange": false,
    "bInfo": false,
    "bPaginate": true,
    "bFilter": false,
    "bSort": false,
    "pageLength": 8
```

*Fuente*: Elaboración propia

**Sprint 2**

**Acta de inicio del Sprint 2**

ACTA DE INICIO: REUNION DEL SPRINT 2

**Fecha:** 21 / 10 / 2022

| Rol | Persona |
|---|---|
| **Control de calidad** | Alemán Santana Jorge Antonio |
| **Analista** | Oliva Rivera Mitchael Ever |
| **Programador** | Cabellos Dionicio Jhojan Enoc |
| **Programador de BD** | Cabellos Dionicio Jhojan Enoc |

En la ciudad de Lima, Jesús María, a los veintiún días del mes de octubre del presente año en cumplimiento con los puntos establecidos en el plan de trabajo para el adecuado desarrollo de" Proceso de encriptación para la seguridad de la información en el Comando de Control Aeroespacial basado en ISO 27001" se realizará la carta de aprobación para el desarrollo de los cumplimientos funcionales correspondientes al Sprint 2.

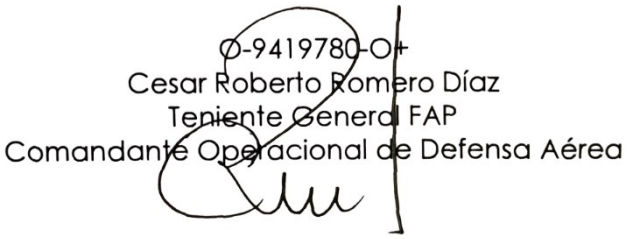
Los elementos de la lista del entregable son:

| Sprint 02 | Nombre de la historia de usuario |
|---|---|
| **Agregar salas de chat** | Módulo salas de chat. |
| **Agregar usuarios a las salas de chat** | Módulo verificación. |
| **Agregar nuevo usuario por el administrador** | Módulo verificación. |

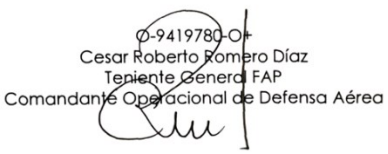
| | |
|---|---|
| **Editar datos de un usuario** | Módulo registro y edición. |
| **Eliminar un usuario** | Módulo administrador. |

Luego de la verificación de las funcionalidades a desarrollar correspondiente al Sprint 2, el teniente general FAP manifiesta su total satisfacción y conformidad del producto de software el cual se desarrollará, y será entregado el 7 de noviembre del 2022.

En muestra de aceptación y conformidad se procede a firmar la presente acta



# ACTA DE PRUEBAS FUNCIONALES DEL SPRINT 2

<table>
<tr><td colspan="6">PRUEBA FUNCIONAL</td></tr>
<tr><td colspan="2">PRUEBA N°</td><td>Sprint 02</td><td colspan="2">VERSION DE EJECUCIÓN</td><td>PFS-02</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2">FECHA DE EJECUCIÓN</td><td>07/11/2022</td></tr>
<tr><td colspan="2">TAREA</td><td>Sprint 02</td><td colspan="2">MODELO DEL SISTEMA</td><td>PF02</td></tr>
<tr><td colspan="2">Descripción del caso de prueba:</td><td colspan="4"></td></tr>
<tr><td colspan="6">3. CASO DE PRUEBA</td></tr>
<tr><td colspan="6">d. Precondiciones</td></tr>
<tr><td colspan="6">• Inicio de sesión exitoso en modo administrador y usuario</td></tr>
<tr><td colspan="6">e. Pasos de la prueba</td></tr>
<tr><td colspan="6">• Verificación de requerimientos<br>• Ingresar con credenciales de administrador o usuario<br>• Agregar nueva sala de chat<br>• Editar datos de su propio usuario<br>• Ingresar con credenciales de administrador<br>• Agregar nuevo usuario<br>• Eliminar un usuario</td></tr>
<tr><td colspan="3">DATOS DE ENTRADA</td><td rowspan="2">RESPUESTA ESPERADA DE LA APLICACIÓN</td><td colspan="2">COINCIDE</td><td rowspan="2">RESPUESTA DEL SISTEMA</td></tr>
<tr><td>CAMPO</td><td>VALOR</td><td>TIPO ESCENARIO</td><td>SI</td><td>NO</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Agregar sala de chat y agregar usuarios</td><td>X</td><td></td><td>Nueva sala de chat creada</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Editar usuario</td><td>X</td><td></td><td>Usuario actualizado</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Agregar nuevo usuario</td><td>X</td><td></td><td>Usuario agregado</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Eliminar usuario</td><td>X</td><td></td><td>Borrado exitoso</td></tr>
<tr><td colspan="6">f. Post condiciones</td></tr>
<tr><td colspan="6">Aplicada</td></tr>
<tr><td colspan="6">4. RESULTADO DE LA PRUEBA</td></tr>
<tr><td colspan="5">Defectos de desviaciones</td><td>Veredicto</td></tr>
<tr><td colspan="5">-</td><td>APROBADO<br>FALLADO</td></tr>
<tr><td colspan="4">Observaciones</td><td colspan="2">Probador</td></tr>
<tr><td colspan="4">-</td><td>Nombre: Alemán Santana Jorge Antonio<br>Fecha: 07/10/2022</td><td> 
</td></tr>
</table>

**Acta de cierre del Sprint 2**

ACTA DE REUNION DE CIERRE DEL SPRINT 2

Fecha: 07 / 11 / 2022

Datos:

| **Empresa** | **Fuerza Aérea del Perú** |
|---|---|
| **Proyecto** | Proceso de encriptación para la seguridad de la información en el Comando de Control Aeroespacial basado en ISO 27001 |

Participantes:

| **Rol** | **Persona** |
|---|---|
| **Control de calidad** | Alemán Santana Jorge Antonio |
| **Analista** | Oliva Rivera Mitchael Ever |
| **Programador** | Cabellos Dionicio Jhojan Enoc |
| **Programador de BD** | Cabellos Dionicio Jhojan Enoc |

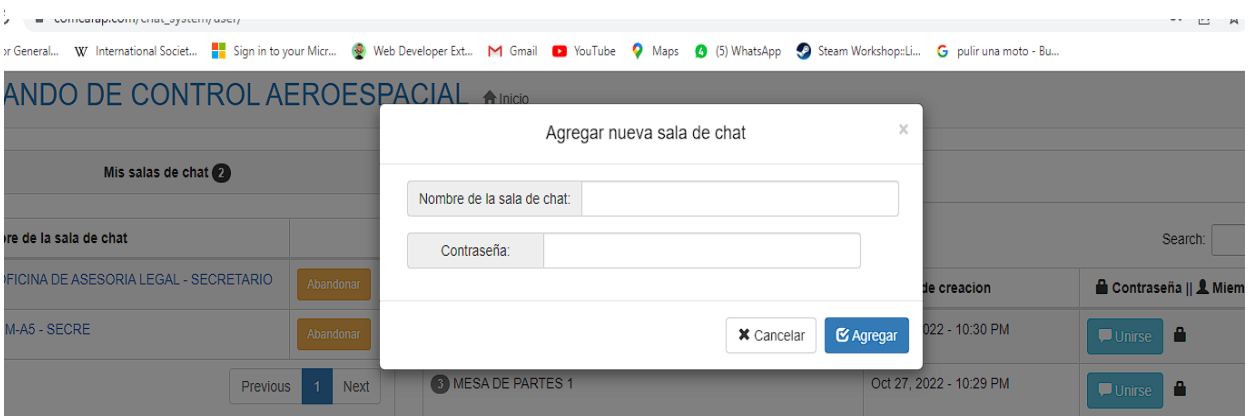
Acuerdos:

Marca con una “x” por los motivos de cierre, con lo referente a lo acordado sobre las funcionalidades del Sprint actual.

| **Nombre de la historia de usuario** | **No entrega** | **Entrega parcial** | **Entrega completa** |
|---|---|---|---|
| **Módulo salas de chat.** | | | X |
| **Módulo verificación.** | | | X |
| **Módulo verificación.** | | | X |
| **Módulo registro y edición.** | | | X |
| **Módulo administrador.** | | | X |

Ø-9419780-O+
Cesar Roberto Romero Díaz
Teniente General FAP
Comandante Operacional de Defensa Aérea

*Figura 23:* Agregar salas de chat.



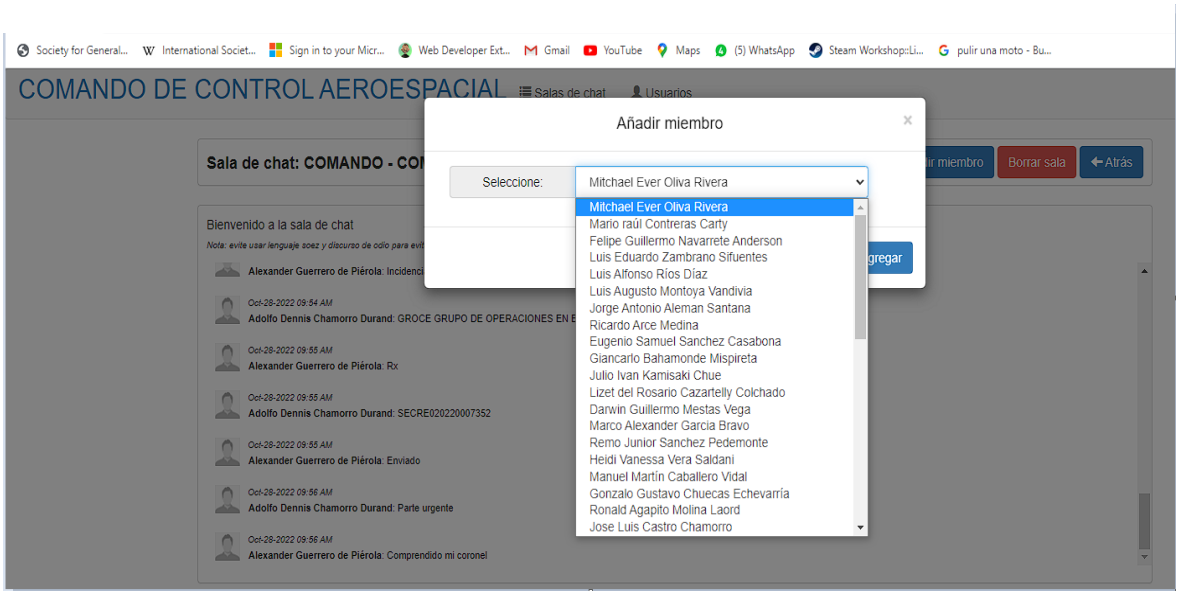

*Fuente*: Elaboración propia

*Figura 24:* Código agregar sala de chat.

```
<!-- Agregar Sala -->
    <div class="modal fade" id="agregar_sala" tabindex="-1" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">
        <div class="modal-dialog">
            <div class="modal-content">
                <div class="modal-header">
                    <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</button>
                    <center><h4 class="modal-title" id="myModalLabel">Agregar nueva sala de chat</h4></center>
                </div>
                <div class="modal-body">
                <div class="container-fluid">
                <form>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Nombre de sala de chat:</span>
                        <input type="text" style="width:350px;" class="form-control" id="nombre_chat" required>
                    </div>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Contrase単a:</span>
                        <input type="text" style="width:350px;" class="form-control" id="contra_chat">
                    </div>
                </div>
                </div>
                <div class="modal-footer">
                    <button type="button" class="btn btn-default" data-dismiss="modal"><span class="glyphicon glyphicon-remove"></span> Cancelar</button>
                    <button type="button" class="btn btn-primary" id="agregarsalachat"><span class="glyphicon glyphicon-check"></span> Agregar</button>
                </form>
                </div>
            </div>

        </div>

    </div>
```

*Fuente*: Elaboración propia

*Figura 25:* Agregar usuarios a las salas de chat.



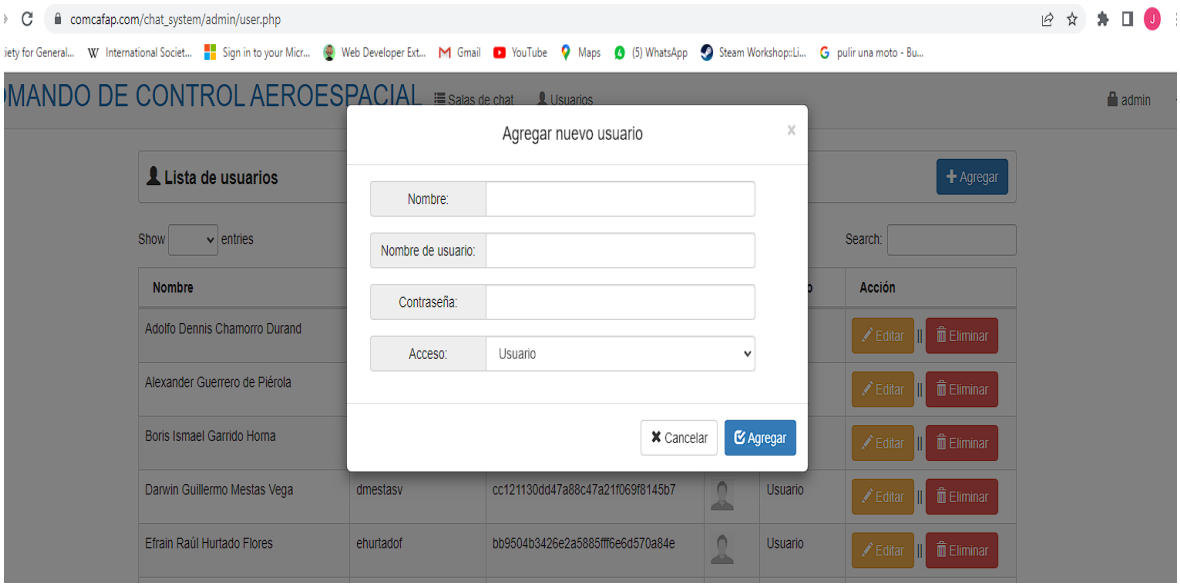

*Fuente*: Elaboración propia

*Figura 26:* Código de agregar usuario a sala de chat.

```
<!-- Agregar Miembro -->
    <div class="modal fade" id="add_member" tabindex="-1" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">
        <div class="modal-dialog">
            <div class="modal-content">
                <div class="modal-header">
                    <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</button>
                    <center><h4 class="modal-title" id="myModalLabel">Añadir miembro</h4></center>
                </div>
                <div class="modal-body">
                <div class="container-fluid">
                    <form method="POST" action="agregar_miembrochat.php?id=<?php echo $id; ?>">
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Seleccione:</span>
                        <select style="width:350px;" class="form-control" name="usuario">
                            <?php
                            include('../conn.php');
                                $mem=array();
                                $um=mysqli_query($conn,"select * from `Miembros_Chat` where idsalchat='$id'");
                                while($umrow=mysqli_fetch_array($um)){
                                    $mem[]=$umrow['userid'];
                                }
                                $users=implode($mem, "', '");

                                $u=mysqli_query($conn,"select * from `Usuario` where userid not in ('".$users."')");
                                if(mysqli_num_rows($u)<1){
                                    ?>
                                    <option value="">Ningún usuario disponible</option>
                                    <?php
                                }
                                else{
                                while($urow=mysqli_fetch_array($u)){
                                    ?>
                                        <option value="<?php echo $urow['userid']; ?>"><?php echo $urow['nombre']; ?></option>
                                    <?php
                                }
                                }
```

*Fuente*: Elaboración propia

*Figura 27:* Agregar nuevo usuario por el administrador.



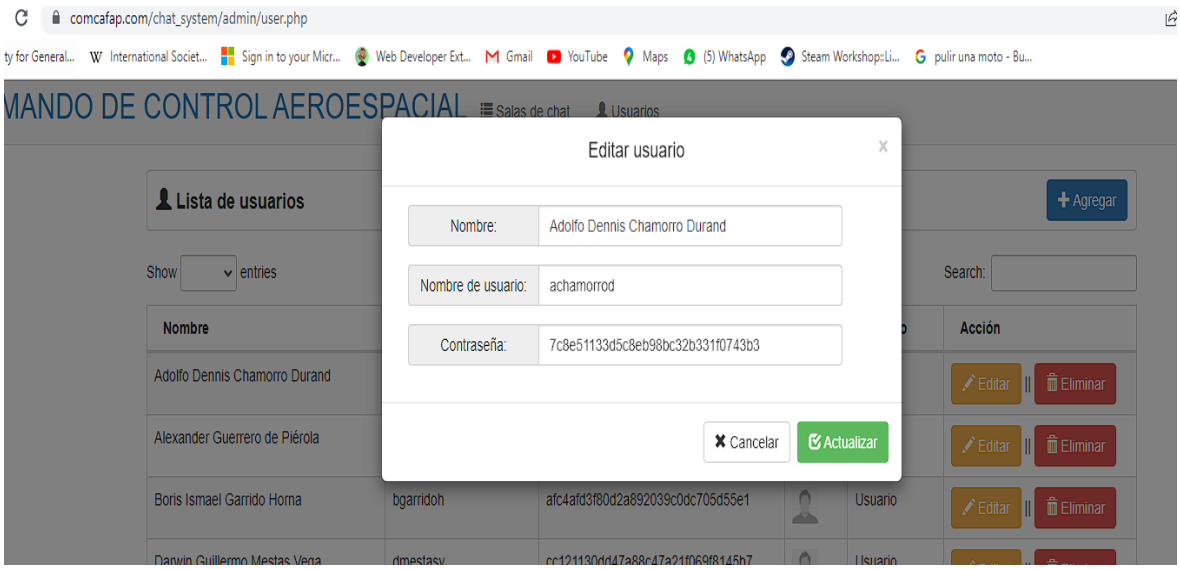

*Fuente*: Elaboración propia

*Figura 28:* Código de agregar nuevo usuario.

```
<!-- Agregar Usuario -->
    <div class="modal fade" id="agregar_usuario" tabindex="-1" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">
        <div class="modal-dialog">
            <div class="modal-content">
                <div class="modal-header">
                    <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</button>
                    <center><h4 class="modal-title" id="myModalLabel">Agregar nuevo usuario</h4></center>
                </div>
                <div class="modal-body">
                <div class="container-fluid">
                <form>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Nombre:</span>
                        <input type="text" style="width:350px;" class="form-control" id="nombre" required>
                    </div>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Nombre de usuario:</span>
                        <input type="text" style="width:350px;" class="form-control" id="usuarionombre" required>
                    </div>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Contrase▦a:</span>
                        <input type="text" style="width:350px;" class="form-control" id="contrasena" required>
                    </div>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Acceso:</span>
                        <select style="width:350px;" class="form-control" id="acceso">
                            <option value="2">Usuario</option>
                            <option value="1">Administrador</option>
                        </select>
                    </div>
                </div>
                </div>
                <div class="modal-footer">
                    <button type="button" class="btn btn-default" data-dismiss="modal"><span class="glyphicon glyphicon-remove"></span> Cancelar</button>
                    <button type="button" class="btn btn-primary" id="agregarusuario"><span class="glyphicon glyphicon-check"></span> Agregar</button>
                </form>
                </div>
            </div>
```

*Fuente*: Elaboración propia

*Figura 29:* Editar datos de un usuario.



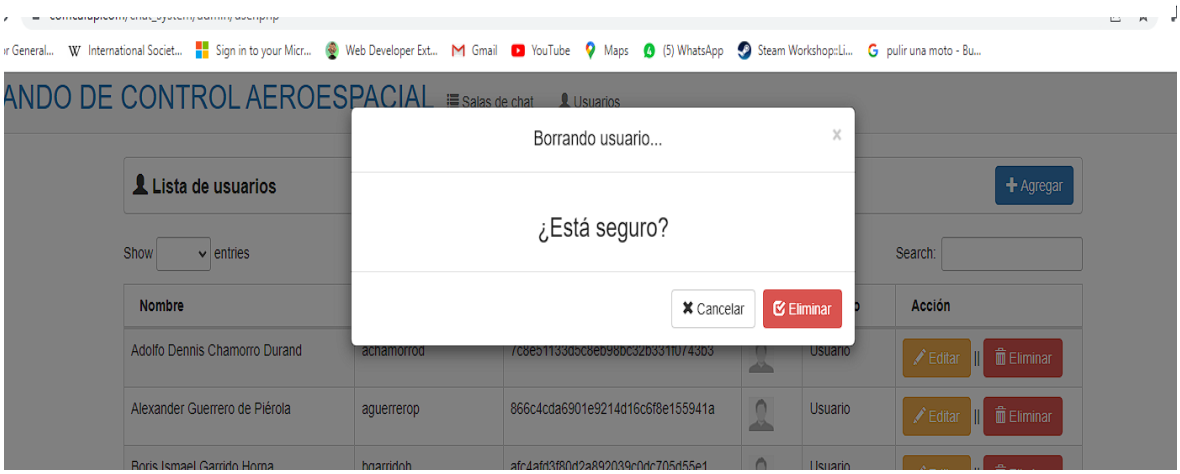

*Fuente*: Elaboración propia

*Figura 30:* Código de editar usuario.

```
<!-- Editar Usuario -->
    <div class="modal fade" id="editar_usuario" tabindex="-1" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">
        <div class="modal-dialog">
            <div class="modal-content">
                <div class="modal-header">
                    <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</button>
                    <center><h4 class="modal-title" id="myModalLabel">Editar usuario</h4></center>
                </div>
                <div class="modal-body">
                <div class="container-fluid">
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Nombre:</span>
                        <input type="text" style="width:350px;" class="form-control" id="nomb">
                    </div>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Nombre de usuario:</span>
                        <input type="text" style="width:350px;" class="form-control" id="nomusu">
                    </div>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Contrase単a:</span>
                        <input type="text" style="width:350px;" class="form-control" id="contra">
                    </div>
                </div>
                </div>
                <div class="modal-footer">
                    <button type="button" class="btn btn-default" data-dismiss="modal"><span class="glyphicon glyphicon-remove"></span> Cancelar</button>
                    <button type="button" class="btn btn-success" id="confirm_edicion"><span class="glyphicon glyphicon-check"></span> Actualizar</button>

                </div>
            </div>
        </div>
```

*Fuente*: Elaboración propia

*Figura 31:* Eliminar un usuario.




*Fuente*: Elaboración propia

*Figura 32:* Código eliminar usuario.

```
<!-- Eliminar Usuario -->
    <div class="modal fade" id="eliminar_usuario" tabindex="-1" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">
        <div class="modal-dialog">
            <div class="modal-content">
                <div class="modal-header">
                    <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</button>
                    <center><h4 class="modal-title" id="myModalLabel">Borrando usuario...</h4></center>
                </div>
                <div class="modal-body">
                <div class="container-fluid">
                    <h3><center>Est seguro?</center></h3>
                </div>
                </div>
                <div class="modal-footer">
                    <button type="button" class="btn btn-default" data-dismiss="modal"><span class="glyphicon glyphicon-remove"></span> Cancelar</button>
                    <button type="button" class="btn btn-danger" id="confirm_eliminado"><span class="glyphicon glyphicon-check"></span> Eliminar</button>
                </div>
            </div>
        </div>
    </div>
```

*Fuente*: Elaboración propia

**Sprint 3**

**Acta de inicio del Sprint 3**

ACTA DE INICIO: REUNION DEL SPRINT 3

**Fecha:** 08 / 11 / 2022

| Rol | Persona |
|---|---|
| **Control de calidad** | Alemán Santana Jorge Antonio |
| **Analista** | Oliva Rivera Mitchael Ever |
| **Programador** | Cabellos Dionicio Jhojan Enoc |
| **Programador de BD** | Cabellos Dionicio Jhojan Enoc |

En la ciudad de Lima, Jesús María, a los ocho días del mes de noviembre del presente año en cumplimiento con los puntos establecidos en el plan de trabajo para el adecuado desarrollo de" Proceso de encriptación para la seguridad de la información en el Comando de Control Aeroespacial basado en ISO 27001" se realizará la carta de aprobación para el desarrollo de los cumplimientos funcionales correspondientes al Sprint 1.

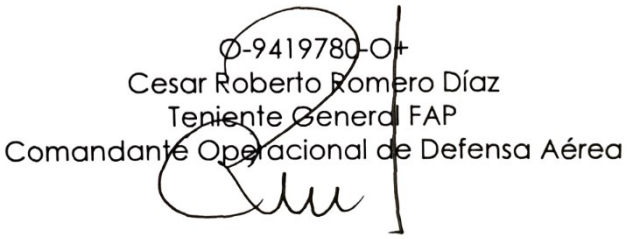
Los elementos de la lista del entregable son:

| Sprint 03 | Nombre de la historia de usuario |
|---|---|
| **Editar una sala de chat** | Módulo salas de chat. |
| **Envío de mensajes en la sala de chat** | Módulo de encriptación. |
| **Encriptado de los mensajes de las salas de chat** | Módulo de encriptación. |

| | |
|---|---|
| **Cerrar sesión** | Login de ingreso. |

Luego de la verificación de las funcionalidades a desarrollar correspondiente al Sprint 1, el teniente general FAP manifiesta su total satisfacción y conformidad del producto de software el cual se desarrollará, y será entregado el 21 de noviembre del 2022.

En muestra de aceptación y conformidad se procede a firmar la presente acta



# ACTA DE PRUEBAS FUNCIONALES DEL SPRINT 3

<table>
<tr><td colspan="6">PRUEBA FUNCIONAL</td></tr>
<tr><td colspan="2">PRUEBA N°</td><td>Sprint 03</td><td colspan="2">VERSION DE EJECUCIÓN</td><td>PFS-03</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2">FECHA DE EJECUCIÓN</td><td>21/10/2022</td></tr>
<tr><td colspan="2">TAREA</td><td>Sprint 03</td><td colspan="2">MODELO DELSISTEMA</td><td>PF03</td></tr>
<tr><td colspan="2">Descripción del caso de prueba:</td><td colspan="4"></td></tr>
<tr><td colspan="6">5. CASO DE PRUEBA</td></tr>
<tr><td colspan="6">g. Precondiciones</td></tr>
<tr><td colspan="6">• Recolección de requerimientos<br>• BD creado</td></tr>
<tr><td colspan="6">h. Pasos de la prueba</td></tr>
<tr><td colspan="6">• Verificación de requerimientos.<br>• Ingresar con credenciales de administrador o usuario.<br>• Editar una sala de chat creada por usted mismo.<br>• Ingresar a una sala de chat y enviar mensaje.<br>• Verificar si la edición de sala de chat.<br>• Verificar si el mensaje fue enviado y si en la base de datos se guardó de manera cifrada.</td></tr>
<tr><td colspan="3">DATOS DE ENTRADA</td><td rowspan="2">RESPUESTA ESPERADA DE LA APLICACIÓN</td><td colspan="2">COINCIDE</td><td rowspan="2">RESPUESTA DEL SISTEMA</td></tr>
<tr><td>CAMPO</td><td>VALOR</td><td>TIPO ESCENARIO</td><td>SI</td><td>NO</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Editar una sala de chat</td><td>X</td><td></td><td>Sala de chat actualizada</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Enviar mensaje</td><td>X</td><td></td><td>Mensaje enviado</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>Envío de mensaje cifrado</td><td>X</td><td></td><td>Mensaje guardado de manera cifrada</td></tr>
<tr><td colspan="6">i. Post condiciones</td></tr>
<tr><td colspan="6">Aplicada</td></tr>
<tr><td colspan="6">6. RESULTADO DE LA PRUEBA</td></tr>
<tr><td colspan="5">Defectos de desviaciones</td><td>Veredicto</td></tr>
<tr><td colspan="5">-</td><td>APROBADO<br>FALLADO</td></tr>
<tr><td colspan="4">Observaciones</td><td colspan="2">Probador</td></tr>
<tr><td colspan="4">-</td><td>Nombre: Alemán Santana Jorge Antonio<br>Fecha: 21/10/2022</td><td>Ø-9419780-O+<br>Cesar Roberto Romero Díaz<br>Teniente General FAP<br>Comandante Operacional de Defensa Aérea</td></tr>
</table>

**Acta de cierre del Sprint 3**

ACTA DE REUNION DE CIERRE DEL SPRINT 3

Fecha: 21 / 11 / 2022

Datos:

| **Empresa** | **Fuerza Aérea del Perú** |
|---|---|
| **Proyecto** | Proceso de encriptación para la seguridad de la información en el Comando de Control Aeroespacial basado en ISO 27001 |

Participantes:

| **Rol** | **Persona** |
|---|---|
| **Control de calidad** | Alemán Santana Jorge Antonio |
| **Analista** | Oliva Rivera Mitchael Ever |
| **Programador** | Cabellos Dionicio Jhojan Enoc |
| **Programador de BD** | Cabellos Dionicio Jhojan Enoc |

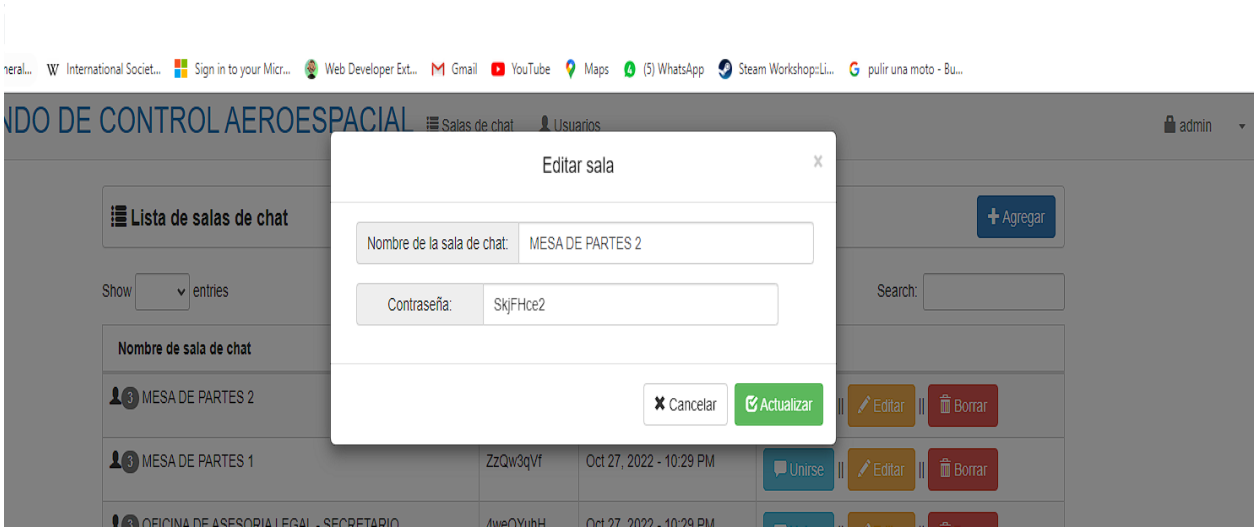
Acuerdos:

Marca con una “x” por los motivos de cierre, con lo referente a lo acordado sobre las funcionalidades del Sprint actual.

| **Nombre de la historia de usuario** | **No entrega** | **Entrega parcial** | **Entrega completa** |
|---|---|---|---|
| **Módulo salas de chat.** | | | X |
| **Módulo de encriptación.** | | | X |
| **Módulo de encriptación.** | | | X |
| **Login de ingreso.** | | | X |

Ø-9419780-O+
Cesar Roberto Romero Díaz
Teniente General FAP
Comandante Operacional de Defensa Aérea

*Figura 33:* Editar una sala de chat.



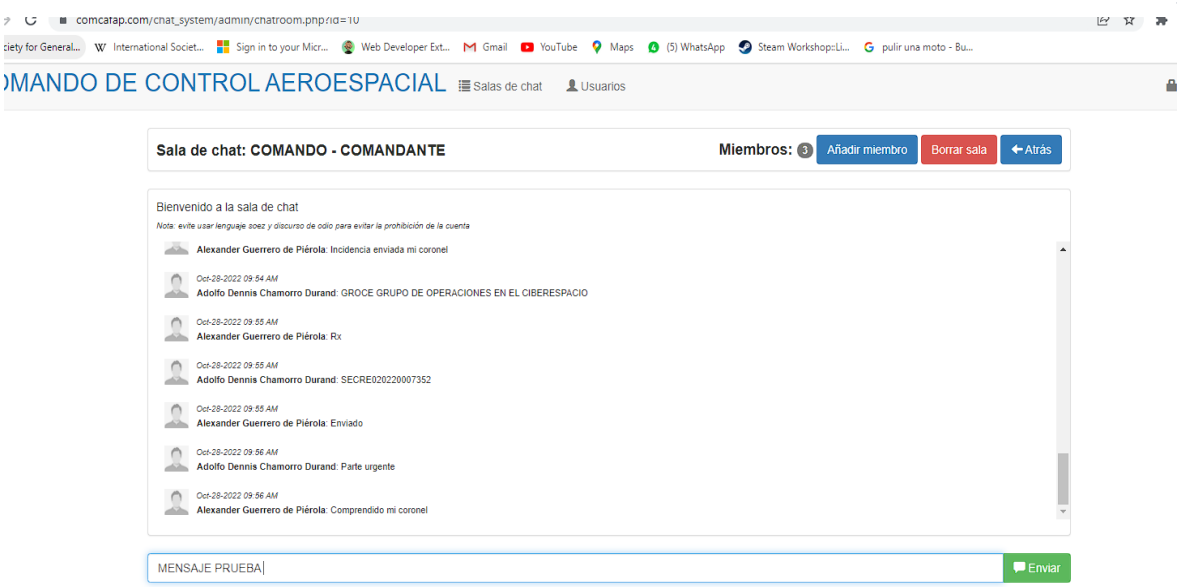

*Fuente*: Elaboración propia

*Figura 34:* Código de edición de una sala de chat.

```
<!-- Editar Sala -->
    <div class="modal fade" id="editar_sala" tabindex="-1" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">
        <div class="modal-dialog">
            <div class="modal-content">
                <div class="modal-header">
                    <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</button>
                    <center><h4 class="modal-title" id="myModalLabel">Editar sala</h4></center>
                </div>
                <div class="modal-body">
                <div class="container-fluid">
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Nombre de la sala de chat:</span>
                        <input type="text" style="width:350px;" class="form-control" id="nombre_sala" required>
                    </div>
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Contrase単a:</span>
                        <input type="text" style="width:350px;" class="form-control" id="contra_sala">
                    </div>
                </div>
                </div>
                <div class="modal-footer">
                    <button type="button" class="btn btn-default" data-dismiss="modal"><span class="glyphicon glyphicon-remove"></span> Cancelar</button>
                    <button type="button" class="btn btn-success" id="confirm_edicion"><span class="glyphicon glyphicon-check"></span> Actualizar</button>

                </div>
            </div>
        </div>
    </div>
```

*Fuente*: Elaboración propia

*Figura 35:* Envío de mensajes en la sala de chat.




*Fuente*: Elaboración propia

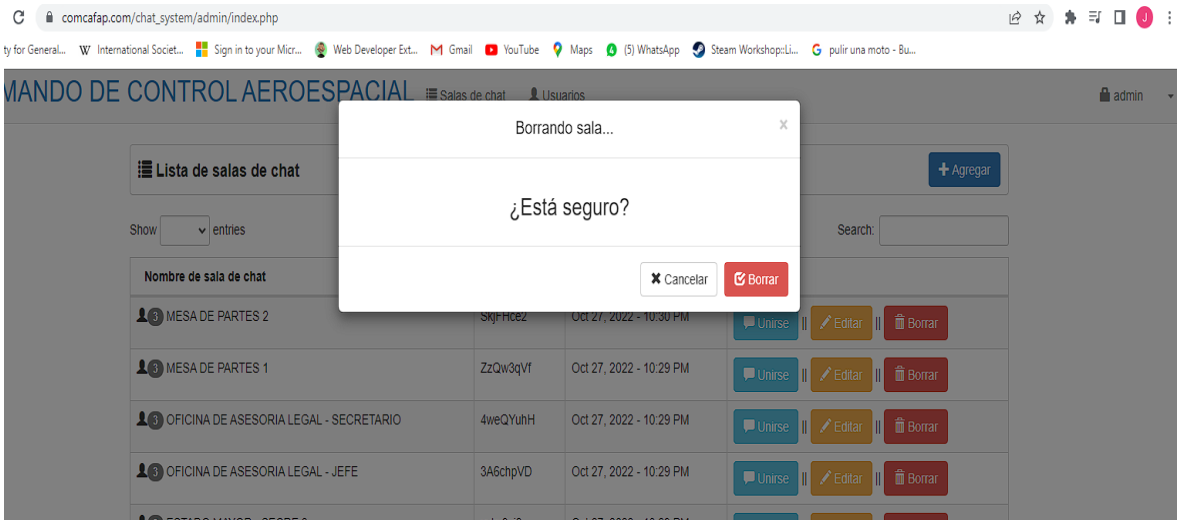
*Figura 36:* Código de envío y muestra de mensajes.

```php
<?php
    include('../conn.php');
    include 'Seguridad.php';
    session_start();
    if(isset($_POST['msj'])){
        $msj=$_POST['msj'];
        $id=$_POST['id'];

        $msjE=SEGURIDAD::encryption($msj);

        mysqli_query($conn,"insert into `Chat` (idsalchat, mensaje, userid, fecha_chat) values ('$id', '$msjE' , '".$_SESSION['id']."', NOW())") or die(mysqli_error());
    }
?>
```

```php
<?php
    include('../conn.php');
    include 'Seguridad.php';
    if(isset($_POST['buscar'])){
        $id = $_POST['id'];

        $query=mysqli_query($conn,"select * from `Chat` left join `Usuario` on Usuario.userid=Chat.userid where idsalchat='$id' order by fecha_chat asc") or die(mysqli_error());
        while($row=mysqli_fetch_array($query)){

            $msjD=SEGURIDAD::decryption($row['mensaje']);
        ?>
        <div>
            <img src="../<?php if(empty($row['foto'])){echo "perfil/profile.jpg";}else{echo $row['foto'];} ?>" style="height:30px; width:30px; position:relative; top:15px; left:10px;">
            <span style="font-size:10px; position:relative; top:7px; left:15px;"><i><?php echo date('M-d-Y h:i A',strtotime($row['fecha_chat'])); ?></i></span><br>
            <span style="font-size:11px; position:relative; top:-2px; left:50px;"><strong><?php echo $row['nombre']; ?></strong>: <?php echo $msjD; ?></span>
        </div>
        <?php
        }
    }
?>
```

*Fuente*: Elaboración propia

*Figura 37:* Eliminar una sala de chat.



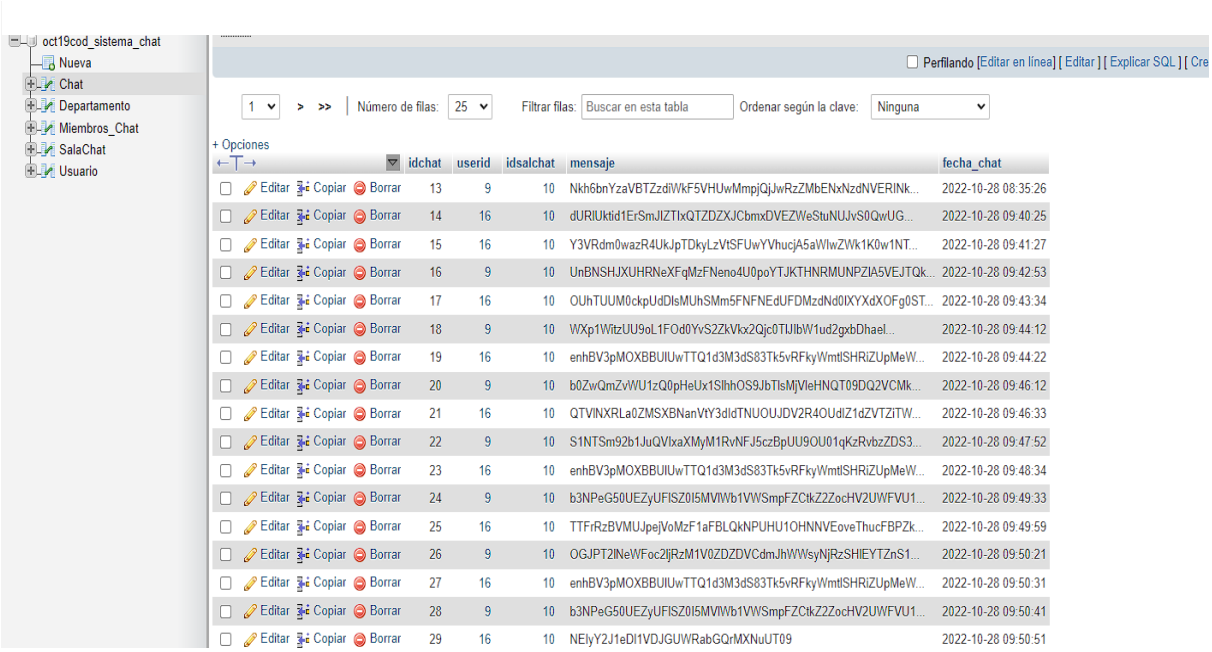

*Fuente*: Elaboración propia

*Figura 38:* Código de eliminado de sala.

```php
<?php
    include('../conn.php');

    if (isset($_POST['eliminar'])){
        $id=$_POST['id'];

        mysqli_query($conn,"delete from `Chat` where idsalchat='$id'");
        mysqli_query($conn,"delete from `Miembros_Chat` where idsalchat='$id'");
        mysqli_query($conn,"delete from `SalaChat` where idsalchat='$id'");
    }
?>
```

*Fuente*: Elaboración propia

*Figura 39:* Encriptado de los mensajes de las salas de chat.



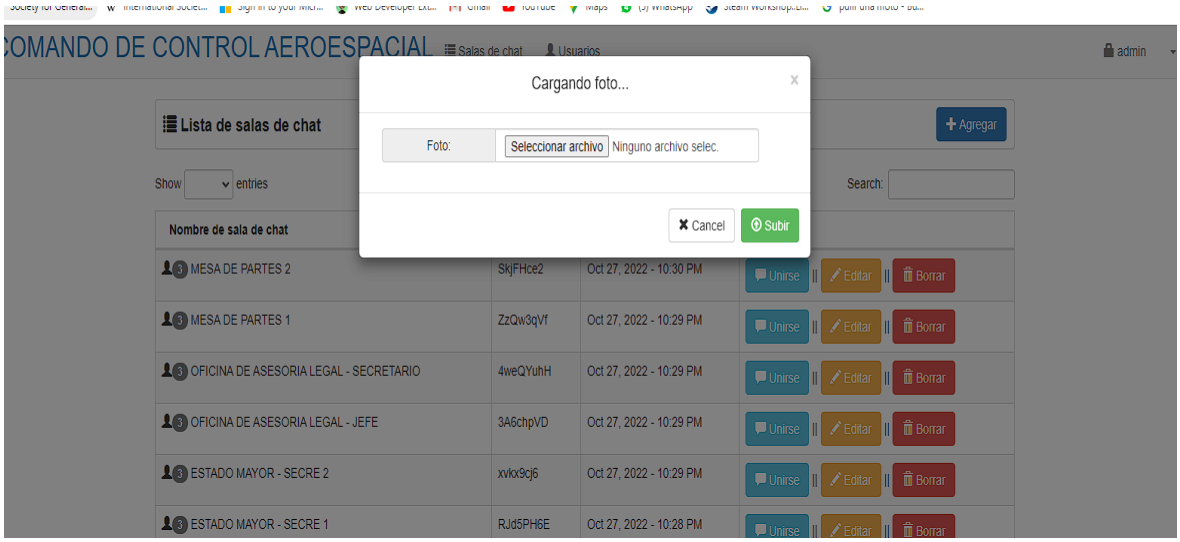

*Fuente*: Elaboración propia

*Figura 40:* Código del algoritmo de encriptado simétrico y desencriptado.

```php
<?php
    define('METODO','AES-256-CBC');
    define('LLAVE_SECRETA','$CARLOS@2016');
    define('IV_SECRETA','101712');
    class SEGURIDAD {
        public static function encryption($entrada){
            $salida=FALSE;
            $llave=hash('sha256', LLAVE_SECRETA);
            $iv=substr(hash('sha256', IV_SECRETA), 0, 16);
            $salida=openssl_encrypt($entrada, METODO, $llave, 0, $iv);
            $salida_final=base64_encode($salida);
            return $salida_final;
        }
        public static function decryption($entrada){
            $llave=hash('sha256', LLAVE_SECRETA);
            $iv=substr(hash('sha256', IV_SECRETA), 0, 16);
            $salida=openssl_decrypt(base64_decode($entrada), METODO, $llave, 0, $iv);
            return $salida;
        }
    }
```

*Fuente*: Elaboración propia

*Figura 41:* Actualización de foto de perfil



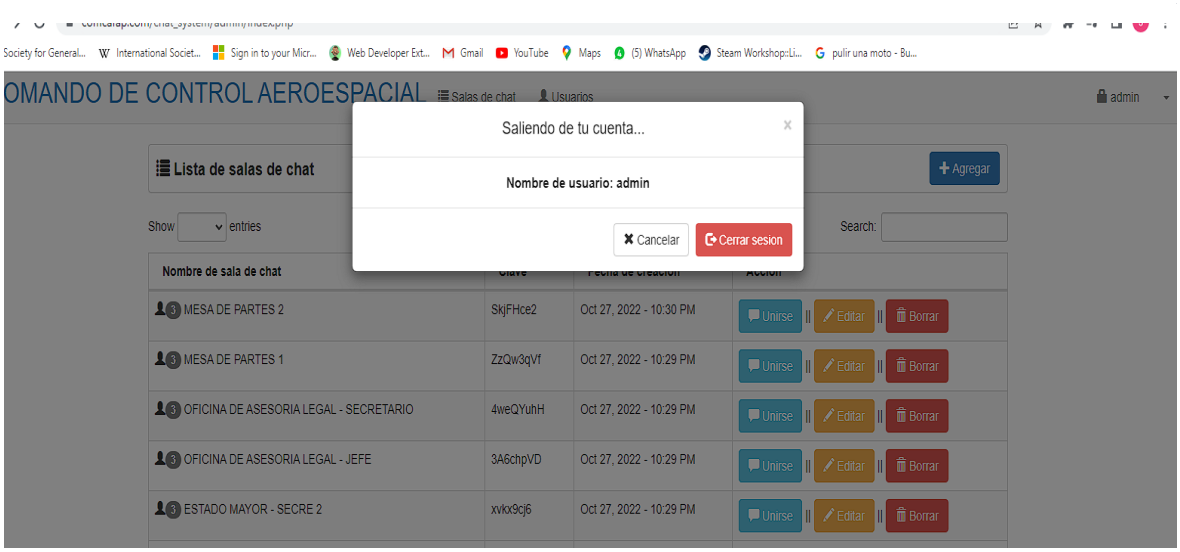

*Fuente*: Elaboración propia

*Figura 42:* Código actualización de foto de perfil.

```
<!-- Actualizar foto-->
    <div class="modal fade" id="foto" tabindex="-1" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">
        <div class="modal-dialog">
            <div class="modal-content">
                <div class="modal-header">
                    <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</button>
                    <center><h4 class="modal-title" id="myModalLabel">Cargando foto...</h4></center>
                </div>
                <div class="modal-body">
                <div class="container-fluid">
                    <form method="POST" enctype="multipart/form-data" action="actualizar_foto.php">
                    <div class="form-group input-group">
                        <span class="input-group-addon" style="width:150px;">Foto:</span>
                        <input type="file" style="width:350px;" class="form-control" name="imagen">
                    </div>
                </div>
                </div>
                <div class="modal-footer">
                    <button type="button" class="btn btn-default" data-dismiss="modal"><span class="glyphicon glyphicon-remove"></span> Cancel</button>
                    <button type="submit" class="btn btn-success"><span class="glyphicon glyphicon-upload"></span> Subir</button>
                    </form>
                </div>
            </div>
        </div>
    </div>
```

*Fuente*: Elaboración propia

*Figura 43:* Cerrar sesión.




*Fuente*: Elaboración propia

*Figura 44:* Código de cerrado de sesión.

```
<!-- Cerrado sesión-->
    <div class="modal fade" id="cerrar_sesion" tabindex="-1" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">
        <div class="modal-dialog">
            <div class="modal-content">
                <div class="modal-header">
                    <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</button>
                    <center><h4 class="modal-title" id="myModalLabel">Saliendo de tu cuenta...</h4></center>
                </div>
                <div class="modal-body">
                <div class="container-fluid">
                    <center><strong><span style="font-size: 15px;">Nombre de usuario: <?php echo $user; ?></span></strong></center>
                </div>
                </div>
                <div class="modal-footer">
                    <button type="button" class="btn btn-default" data-dismiss="modal"><span class="glyphicon glyphicon-remove"></span> Cancelar</button>
                    <a href="CerrarSesion.php" class="btn btn-danger"><span class="glyphicon glyphicon-log-out"></span> Cerrar sesion</a>
                </div>
            </div>
        </div>
    </div>
```

```
<?php
    session_start();
    session_destroy();
    header('location:../');
?>
```

*Fuente*: Elaboración propia

## Anexo 6. Cotización.

**PROPUESTA PARA IMPLEMENTACIÓN DE SISTEMA A MEDIDA**

COMANDO DE CONTROL AEROESPACIAL

SAN ISIDRO, 20 DE AGOSTO DEL 2022

**PROPUESTA ECONÓMICA**

| **INVERSION** | | **PRECIO USD$** |
|---|---|---|
| IMPLEMENTACIÓN DE SISTEMA A MEDIDA | | 1500.00 |
| SUBTOTAL | | 1500.00 |
| IGV | 18% | 270.00 |
| **TOTAL INVERSION USD$** | | **1770.00** |

**CONDICIONES DE LA PROPUESTA**

LOS PRECIOS ESTAN EXPRESADOS EN DOLARES AMERICANOS

El tipo de cambio referencial para la conversión de la propuesta es de S/.4.00 si el clientedecide pagar el precio final en nuevos soles.

**FORMA DE PAGO:**

| BANCO | CTA CTE DOLARES | CTA. CTE. SOLES |
|---|---|---|
| **CONTINENTAL** | 0011-0387-0100003630 | 0011-0387-0100003851 |
| **SCOTIABANK** | 000-0106355 | 000-0069353 |
| **CREDITO** | 193-1035058-1-40 | 193-1311950-0-19 |

**VIGENCIA: 27 DE AGOSTO DEL 2022**

CONSIDERACIONES GENERALES

- La empresa garantiza la óptima performance por cada uno de nuestro software en cuanto a su operatividad, funcionamiento con un completo soporte y respaldo profesional
- Una vez aceptada la propuesta o cotización y realizado el pago no habrá lugar a devoluciones.
- Solicitud de servicios adicionales con costo.

UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

# Declaratoria de Autenticidad del Asesor

Yo, HUGO VILLAVERDE MEDRANO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Proceso de encriptación para la seguridad de la información en el Comando de Control Aeroespacial basado en ISO 27001", cuyos autores son OLIVA RIVERA MITCHAEL EVER, CABELLOS DIONICIO JHOJAN ENOC, constato que la investigación tiene un índice de similitud de 16.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 10 de Diciembre del 2022

| **Apellidos y Nombres del Asesor:** | **Firma** |
|---|---|
| HUGO VILLAVERDE MEDRANO<br>**DNI:** 09587257<br>**ORCID:** 0000-0002-3802-4396 | Firmado electrónicamente por: HUVILLAVERDEMED el 19-12-2022 05:49:42 |

Código documento Trilce: TRI - 0481386

INVESTIGA UCV