



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL INGENIERÍA DE SISTEMAS

Desarrollo de un sistema hotelero para gestionar la información de los
clientes, basado en el apartado de operación de la norma iso
27001:2014, para el hotel el Puerto

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTORES:

Cabrera Chumbe, Renato Samuel (ORCID: 0000-0002-0009-8058)

Rojas Rett, Gilmer Armando (ORCID: 0000-0002-1672-8026)

ASESOR:

Mgtr. Liendo Arevalo, Milner David (ORCID: 0000-0002-7665-361X)

LÍNEA DE INVESTIGACIÓN:

Sistemas de información y comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2022

Dedicatoria

Dedicada a nuestros padres, por su esfuerzo, ya que sin ellos no lo hubiéramos logrado. Luego a todas las personas que nos han apoyado y han hecho que podamos llegar hasta acá.

Agradecimiento

A la Universidad del Cesar Vallejo, le agradecemos la inigualable oportunidad que nos ha dado de formar parte de esta universidad y permitirnos obtener un título profesional.

Índice de contenidos

Dedicatoria	ii
Agradecimiento	iii
Índice de tablas	v
Índice de figuras	vi
Índice de Anexos	viii
Resumen	ix
Abstract	x
I. INTRODUCCIÓN	1
II. MARCO TEÓRICO	5
III. METODOLOGÍA	15
3.1 Tipo y diseño de investigación	15
3.2. Variables y operacionalización	15
3.3. Población y muestra	16
3.4. Técnicas e instrumentos de recolección de datos	17
3.5. Procedimientos	17
3.6. Método de análisis de datos	19
3.7. Aspectos éticos	19
IV. RESULTADOS	20
V. DISCUSIÓN	55
VI. CONCLUSIONES	59
VII. RECOMENDACIONES	60
REFERENCIAS	61
ANEXOS	67

Índice de tablas

Tabla 1: Niveles de Confiabilidad	18
Tabla 2. Nombres de los expertos.....	18
Tabla 3: Estadísticos Descriptivos Planificación.....	46
Tabla 4: Estadísticos descriptivos Implementación	47
Tabla 5: Estadísticos descriptivos control.....	47
Tabla 6: Prueba de Normalidad de planificación	48
Tabla 7: Prueba de Normalidad implementación.....	49
Tabla 8: Prueba de Normalidad de control	49
Tabla 9: Prueba de rango de Wilcoxon de ANA	51
Tabla 10: Estadístico de contraste del Indicador 1	51
Tabla 11: Prueba t Student de Manipular Borrar Eliminar Datos.....	52
Tabla 12: Prueba de rango de Wilcoxon de CI	53
Tabla 13: Estadístico de contraste de CI.....	53
Tabla 14: Matriz de consistencia	71
Tabla 15: Matriz de operacionalización de variables.....	73
Tabla 16: Modelo de negocio actual.....	85
Tabla 17: Priorización de requerimiento funcionales.....	88
Tabla 18: Actores del negocio	89

Índice de figuras

Figura 1: Calculadora para hallar la muestra.....	16
Figura 2 Amenaza: Fuego	21
Figura 3 Amenaza: Tormenta eléctrica, rayo.....	22
Figura 4 Amenaza: Error de usuario	23
Figura 5 Amenaza: Errores del administrador	24
Figura 6 Amenaza: Alteración accidental de la información	25
Figura 7 Amenaza: Destrucción de la información	26
Figura 8 Amenaza: Fugas de la información	27
Figura 9 Amenaza: Vulnerabilidades de los programas (software)	28
Figura 10 Amenaza: Errores de mantenimiento /actualización de programas	29
Figura 11 Amenaza: Errores de mantenimiento / actualización de equipos	30
Figura 12 Amenaza: Indisponibilidad del personal por salud	31
Figura 13 Amenaza: Manipulación de los registros de actividad.....	32
Figura 14 Amenaza: Suplantación de la identidad del usuario.....	33
Figura 15 Amenaza: Abuso de privilegio de acceso.....	34
Figura 16 Amenaza: difusión de software dañino.....	35
Figura 17 Amenaza: Acceso no autorizado.....	36
Figura 18 Amenaza: Modificación deliberada de la información	37
Figura 19 Amenaza: Inestabilidad de la línea de internet.....	38
Figura 20 Amenaza: Manipulación de programa	39
Figura 21 Amenaza: Manipulación de equipo	40
Figura 22 Amenaza: Robo de equipo	41
Figura 23 Amenaza: Corte de suministro eléctrico	42
Figura 24 Amenaza: Condiciones inadecuadas de temperatura o humedad	43
Figura 25 Amenaza: Degradación de los soportes de almacenamiento de la información.....	44
Figura 26 Amenaza: Instalación de software no autorizado	45
Figura 27: Actores	89
Figura 28: Diagrama de caso de uso del negocio	90
Figura 29: Gestionar usuario	91
Figura 30: Gestionar Cliente.....	91
Figura 31: Diagrama de caso de uso del requerimiento Gestión del Administrador	92
Figura 32: Diagrama de caso de uso del requerimiento Gestión del Supervisor..	93

Figura 33: Diagrama de caso de uso del requerimiento Gestión del Recepcionista	93
Figura 34: Diagrama del modelo lógico de la base de datos.....	95
Figura 35: Diagrama del modelo físico de la base de datos.....	96
Figura 36: Login del sistema	97
Figura 37: Dashboard principal	97
Figura 38: Modulo de reserva.....	98
Figura 39: Lista de servicios.....	98
Figura 40: Lista de habitaciones.....	99
Figura 41: Reporte Diario de Visitas.....	99
Figura 42: Reporte de Inicios de sesión	99
Figura 43: Reporte de acciones en la aplicación web	100
Figura 44: Rutas protegidas	100
Figura 45: Laravel Passport	101
Figura 46: Listado de habitaciones.....	101
Figura 47: Listado de clientes.....	102
Figura 48: Creación de cliente.....	102
Figura 49: Dashboard principal	103

Índice de Anexos

Anexo 1: Declaratoria de Originalidad de Autores.....	68
Anexo 2: Declaratoria de Autenticidad del Asesor	69
Anexo 3: Autorización de Publicación en Repositorio Institucional	70
Anexo 4: Matriz de consistencia.....	71
Anexo 5: Matriz de operacionalización de variables.....	73
Anexo 6: Cuestionario	75
Anexo 7: Fichas de registro Pre-test	76
Anexo 8: Fichas de registro Re-test	77
Anexo 9: Fichas de registro Post-test.....	78
Anexo 10: Fichas de registro Pre-test	79
Anexo 11: Fichas de registro Re-test	80
Anexo 12: Fichas de registro Post-test.....	81
Anexo 13: Fichas de registro Pre-test	82
Anexo 14: Fichas de registro Re-test	83
Anexo 15: Fichas de registro Post-test.....	84
Anexo 16: Metodología de Desarrollo XP.....	85
Anexo 17: Sistema Hotelero.....	97
Anexo 18: Certificado de Validez	104
Anexo 19: Carta de autorización	110
Anexo 20: Evidencia del Turnitin	111

Resumen

En su estudio titulado: “desarrollo de un sistema hotelero para gestionar la información de los clientes, basado en el apartado de operación de la norma ISO 27001:2014, para el Puerto Hotel-La Libertad tiene por finalidad Determinar de qué manera influye el desarrollo de un sistema hotelero para gestionar la información de los clientes, basado en el apartado de operación de la Norma ISO 27001:2014, para la empresa El puerto Hotel La Libertad. Este estudio empleo una metodología de tipo aplicada de diseño pre experimental de enfoque cuantitativo, la población está compuesta por 70 trabajadores del Hotel y la muestra está compuesta por 50 trabajadores. Se realizó el análisis de datos mediante software SPSS V 26. Los resultados es que de implementarse mejorará la gestión de la información mantendrá la información segura, secreta y confiable. Se concluye el desarrollo de un sistema hotelero mejorara la gestión de la información, porque el desarrollo del sistema está amparado en la norma ISO 27001

Palabras clave: Sistema, gestionar, operación.

Abstract

In his study entitled: "development of a hotel system to manage customer information, based on the operation section of the ISO 27001: 2014 standard, for the Puerto Hotel-La Libertad" it aims to determine how the development of a hotel system to manage customer information, based on the operation section of ISO 27001:2014, for the company El Puerto Hotel La Libertad. This study used a methodology of applied type of pre-experimental design of quantitative approach, the population is made up of 70 workers of the Hotel and the sample is made up of 50 workers. The data analysis was carried out using SPSS V 26 software. The results are that if it is implemented, it will improve information management and keep the information safe, secret and reliable. The development of a hotel system is concluded to improve information management, because the development of the system is covered by the ISO 27001 standard.

Keywords: System, manage, operation.

I. INTRODUCCIÓN

En el contexto actual de la pandemia producida por el COVID 19 ha tomado gran importancia para las organizaciones los sistemas de gestión de seguridad de la información, que son aquellas que tienen como principal característica la preservación de la confidencialidad, disponibilidad e integridad de la información en la entidad; esta se realiza por medio de un análisis de las vulnerabilidades que lograra minimizar los posibles ataques informáticos, para mayor seguridad de las organizaciones que tendrán protegida su información. (Meriah, y Arfa ,2019)

A nivel internacional, en México el empleo de las tecnologías de la información en las instituciones está creciendo rápidamente, además permite cubrir las necesidades de seguridad empresarial de todas las organizaciones que buscan establecer su posición en el mercado internacional utilizando las normas de seguridad para establecer un vínculo entre los conceptos de seguridad y calidad. Asimismo, el apartado de la norma ISO 27000 es una norma internacional para la gestión de la seguridad de la información que tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad de la información, de los sistemas y aplicaciones que emplean; además permite a las empresas y a los usuarios comprobar sus TI mediante auditorías internas y externas. (Franco, y otros ,2019).

Mientras tanto en el Perú para instaurar la gestión de la seguridad de la información que ayude a cumplir los tres principios: confidencialidad, disponibilidad e integridad de la información. Se ha realizado un marco legal por la que todas entidades del estado, que pertenecen al Sistema Nacional de Informática, deben aportar a el diseño e implementación de un sistema de gestión de seguridad de la información (SGSI), justificado en la norma técnica peruana (NTP) ISO/IEC 27001:2014 el que fue aprobó mediante la resolución ministerial N° 004-2016-PCM, en la que se menciona que los activos más importantes para las entidades es la información, pero a menudo carecen de políticas adecuadas para protegerla, lo que da lugar a vulnerabilidades que pueden ser aprovechadas por delincuentes informáticos, comprometiendo la integridad, disponibilidad y confidencialidad de los activos de información de la entidad. (Gobierno Electrónico e Informática, 2019)

Asimismo, existe la necesidad en las organizaciones de proteger la información, para ello se identificará los activos de la organización (Ferrer, 2021). En el caso del Puerto Hotel-La libertad , maneja de forma directa la información personal de clientes y proveedores, esta es recopilada a través del área de atención al cliente y departamento de servicios, cuyo sistema de información no cuenta con un proceso adecuado y eficiente de gestión en la seguridad de activos y la información, esto se debe a que la gerencia aún no apuesta por la digitalización de sus operaciones, asimismo, muchos de los trabajadores de esta área no tienen una adecuada capacitación o desconocen el apartado de operación de la norma ISO 27001:2014. El manejo de la información en forma manual suele provocar la pérdida de datos, registros y pagos al no contar con un respaldo, lo que genera problemas internos y externos frente a una auditoría debido a un potencial incumplimiento de las políticas. Asimismo, los administradores del Puerto Hotel desconocen la existencia de la normativa peruana que permita garantizar el correcto manejo de la información provocando que se vulneren la información de los clientes o dificultando la revisión de datos protegidos en procesos de auditoría. Por lo tanto, este estudio propone integrar las secciones del apartado de operaciones basado en la norma ISO 27001:2014 en la planificación y gestión operativa, la evaluación de los riesgos de seguridad de la información y el tratamiento de los riesgos de seguridad de la información.

El presente estudio se justifica teóricamente porque según Meriah & Arfa (2019) las empresas tienen una débil cultura sobre el manejo de información, además de que existe poca información del apartado basado en la norma ISO 27001:2014, con lo que el presente estudio realizará un minucioso estudio sobre conceptos acerca de seguridad de la información que es uno de los problemas más relevantes dentro de las organizaciones públicas y privadas, a fin de poder aportar algunas definiciones sobre la materia evaluada y a su vez fortalecer a través de un análisis bibliográfico la cultura de manejo de información que se tiene a la actualidad. . Se justifica en forma práctica a que los trabajadores tendrán los procesos automáticos empleando las tecnologías de la información dejando atrás el proceso manual según Hernández & Mendoza (2018), su desarrollo va ayudar a resolver un problema o, por lo menos, propone estrategias que al aplicarse

contribuirían a resolverlo. En tanto, la justificación metodológica, Hernández & Mendoza (2018) mencionaron que una investigación tiene características particulares y soluciones que pueden modificarse de acuerdo a su contexto con ello se obtiene nuevo conocimiento que enriquece futuros estudios, con lo que el presente estudio contribuirá a través de un diseño aplicable a la empresa El puerto Hotel La libertad, a través del empleo de métodos adecuadamente descritos por otras investigaciones, los cuales serán redactados de forma ordenada para que puedan ser fácilmente replicables en futuras investigaciones y a su vez pueden ser aplicables en cualquier organización.

De acuerdo con lo anterior se plantea el siguiente problema: ¿De qué manera influye el desarrollo de un sistema hotelero para gestionar la información de los clientes basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad; los problemas específicos de la investigación fueron:

- PE1: ¿Cómo influye el desarrollo de un sistema hotelero en la planificación basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad?
- PE2: ¿Cómo influye el desarrollo de un sistema hotelero en la implementación de políticas basado en el apartado de operación de la norma ISO 27001:2014 para la empresa El puerto Hotel La libertad?
- PE3: ¿Cómo influye el desarrollo de un sistema hotelero en controlar o elimina las amenazas, basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad?

El objetivo general fue Determinar de qué manera influye el desarrollo de un sistema hotelero para gestionar la información de los clientes, basado en el apartado de operación de la Norma ISO 27001:2014, para la empresa El puerto Hotel La libertad; los objetivos específicos de la investigación fueron:

- OE1: Determinar cómo influye el desarrollo de un sistema hotelero en la planificación basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad
- OE2: Determinar cómo influye el desarrollo de un sistema hotelero en la implementación de políticas basado en el apartado de operación de la norma ISO 27001:2014 para la empresa El puerto Hotel La libertad
- OE3: Determinar Cómo influye el desarrollo de un sistema hotelero en controlar o eliminar las amenazas, basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad

La hipótesis general del estudio es El desarrollo de un sistema hotelero mejorará la gestión de la información de los clientes basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad; las hipótesis específicas de la investigación son:

- HE1: El desarrollo de un sistema hotelero mejorará la planificación que está basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad
- HE2: El desarrollo de un sistema hotelero mejorará la implementación de políticas basado en el apartado de operación de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad
- HE3: El desarrollo de un sistema hotelero mejorará control o eliminación de las amenazas, basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad

II. MARCO TEÓRICO

Teniendo en cuenta las variables de estudio, se encontró los siguientes antecedentes de la investigación:

(Solano, 2021) en su estudio tiene por finalidad presentar un modelo para la gestión de la seguridad de la información en la empresa Udersol, con base en ISO 27001 para la mitigación de los incidentes informáticos en 2020. Este estudio empleó una metodología de tipo aplicada de enfoque cualitativo nivel explorativo. Se concluyó que se debe de concientizar a la gerencia, por medio de la guía para que pueda lograr sus objetivos mientras y decidir su propia arquitectura física y de cliente, porque el verdadero progreso viene de la decisión del CEO que está buscando el rumbo que debe tomar la empresa.

(Guerra, y otros, 2021) en su artículo su finalidad es emplear un sistema de gestión de la información basado en métodos de identificación y análisis de riesgos en los procesos bibliotecarios universitarios. Este estudio empleó una metodología de tipo aplicada de enfoque cualitativo nivel explorativo. Se concluyó que la integración de los formatos propuestos para desarrollar el control y auditorías a los indicadores de calidad permite la perfección del sistema de gestión de la seguridad de la información (SGSI) para los procesos de la biblioteca universitaria.

(Tonyse, 2021) en su artículo su propósito es describir los requisitos de implementación y la documentación requerida para un Sistema de Gestión de Seguridad de la Información (SGSI). Este estudio empleó una metodología de tipo aplicada de enfoque cualitativo nivel explorativo. La conclusión es establecer un SGSI o implementar un proceso de certificación ISO 27001 para garantizar la reducción de riesgos y la protección de la información en las computadoras o sistemas conectados, ya que es uno de los activos más importantes de una organización, para seguridad o procesos sensibles. La confidencialidad e integridad de los datos y la información, la pérdida, la fuga o la ausencia de información pueden causar problemas a la organización.

(Moreno, y otros, 2020) en su estudio tuvo por finalidad realizar el diseño de un sistema de gestión de seguridad de la información, por medio de la norma NTC

ISO/IEC 27001:2013 en la empresa. Para ello este estudio utilizó una metodología de tipo aplicada de enfoque cualitativo de instrumento era cuestionario por medio de la encuesta. Concluyó que un análisis en forma adecuada de la SGSI permitirá que se realicen un adecuado análisis de los problemas ya sean internos o externo y de acuerdo a esto realizar un adecuado plan para prevenir cualquier vulneración al SGSI.

(Torres, 2020) en su estudio tiene por finalidad realizar plan de seguridad informática basado en la norma iso 27001. Para este estudio se emplea una metodología es de tipo aplicada de nivel explicativo de método científico de diseño cuasi-experimental. Se encontró que al desarrollar un plan de implementación de la norma ISO 27001 aplicable, ayudé a proponer un sistema de gestión de seguridad de la información para Megaprofer S.A., con un control adecuado sobre la seguridad de la información.

(Sikora, 2020) en su estudio tuvo por finalidad el diseño de un instrumento de control de gestión para el período 2021 utilizando como herramienta un cuadro de mando integral. Para ello el estudio empleó una metodología de tipo aplicada de enfoque cualitativo nivel explorativo de instrumento era cuestionario por medio de la encuesta. Concluyó que nos permite al realizar el control de gestión se reducirá las posibles vulneraciones tanto internas, así como externas.

(Cirstoiu, 2021) en su estudio tuvo por finalidad el desarrollo de una aplicación móvil y web mediante herramientas open source para la reserva de habitaciones en empresa de ámbito hotelero. Este estudio empleó una metodología de tipo aplicada de enfoque cualitativo nivel explorativo. Concluyó se cumplió el objetivo de la empresa al sistematizar todos los procesos además de cumplir con la SGSI de esta manera la empresa tendría grandes beneficios a futuro ya que evita que sus operaciones con los clientes no sean vulneradas por agentes internos o externos contrarios a los intereses de la empresa.

(Xiaoyan, 2020) en su estudio tuvo como finalidad realizar un sistema de gestión de seguridad de la información en la empresa de recursos humanos, COC M.T., con el fin de perfeccionar la seguridad de los recursos informáticos de la empresa. Este estudio empleó una metodología de tipo aplicada de enfoque

cualitativo nivel explorativo. Se puede argumentar que el sistema de administración actual es imperfecto, la conciencia de seguridad es deficiente, los mecanismos de monitoreo son imperfectos y las amenazas de seguridad se ignoran. Con base en el cumplimiento de diversas medidas de control determinadas por el análisis de brechas GAP, así como el análisis y evaluación de riesgos de MAGERIT, proponer políticas y medidas para establecer y mejorar el sistema de gestión de seguridad de la información COC M.T. tiene como objetivo disminuir los riesgos y vulnerabilidades que pueden impactar las operaciones comerciales para proteger eficazmente seguridad de información.

(Freire, y otros, 2019) en su estudio tuvo por objetivo fue crear un sitio web y aplicación móvil para el hotel AL SAFI “El Paraíso” para mejorar el proceso de reserva manual, control de alojamiento y gestión de pedidos. Para continuar con el proyecto de manera óptima, se implementó un enfoque SCRUM flexible, que garantiza una comunicación fluida y eficiente entre el cliente y el desarrollador, y también ayuda a cumplir con la fecha de entrega. Finalmente usó los frameworks JSF y jQuery, que nos facilitaron la creación de interfaces de una manera más sencilla y rápida, gracias a que tienen componentes reutilizables y también decidieron usar PostgreSQL para la gestión de datos.

(Molano, 2018) en su estudio tuvo propósito es mostrar la mejor estrategia para implementar un sistema de gestión de seguridad de la información basado en ISO 27001 en la industria de TI para Market Mix. Este estudio empleó una metodología de tipo aplicada de enfoque cualitativo nivel explorativo. Se ha encontrado que adoptar una estrategia y monitorear continuamente las tareas y responsabilidades asignadas a cada miembro permitirá identificar las amenazas que enfrentan dentro de la organización, así como atacarlas y hacer correcciones relacionadas con ellas. Mejorar y proteger constantemente la información para que la empresa no se vea comprometida.

(Contreras, 2018) en su estudio tuvo por finalidad diseñar el Sistema de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 en la Dirección de Sistemas de la Gobernación de Boyacá. Este estudio empleo una metodología de diseño experimental del tipo pre experimental. Se encuentra que

las entidades necesitan actualizar sus planes de continuidad del negocio debido a situaciones de riesgo que podrían afectar seriamente la continuidad del negocio. Sin importar el tamaño de la entidad o el costo de las medidas de seguridad implementadas, cada entidad debe actualizar su plan de continuidad del negocio, porque tarde o temprano ocurrirá un incidente de seguridad.

(Risco, 2021) en su estudio vemos como objetivo principal decretar el impacto de un sistema de gestión de seguridad de la información basado en la norma de construcción 27001:2013 de Pérez & Pérez SAC, este estudio utilizó un enfoque de diseño de prueba previa y concluyó que impacta positivamente el sistema de gestión de seguridad de la información basado en la norma iso27001 de la firma de arquitectura Pérez & Pérez SAC.

(Vargas, y otros, 2019) en su estudio tuvo como finalidad proponer un diseño de sistema de gestión de seguridad de la información para la Universidad del Pacífico que le permita a la organización contar con un estándar de seguridad global acorde con la norma técnica peruana ISO/IEC 27001:2014. Este estudio empleó una metodología de tipo aplicada de enfoque cualitativo nivel explorativo. Se encuentra que, para cumplir con el borrador del SGSI, se propondrá una plantilla que contenga la política de seguridad para los cinco mecanismos de control de ISO 27002 para permitir que la Escuela aborde los problemas identificados.

(Atencio, 2019) en su estudio tuvo por objetivo es diseñar un sistema de gestión de seguridad de la información especificado por la NTP ISO/IEC 27001:2014, que tiene como objetivo mejorar la integridad, confidencialidad y disponibilidad de las fuentes de información en las aplicaciones. Este estudio utilizó un enfoque de diseño descriptivo, no experimental, de corte transversal. La población y muestra incluye 8 administradores y Directores de la DGIE UNDAC. Las observaciones y encuestas se utilizan como técnicas de recopilación de datos, así como herramientas para los paneles de observación. Se concluyó que el diseño SGSI va mejorar en forma notable los 3 principios y que traerá mayor productividad a la empresa.

(Escalante, 2019) en su estudio tuvo por finalidad implementación de un diseñar un Sistema de Gestión de Seguridad de la Información normado por la NTP

- ISO/IEC 27001:2014 para la organización. Para este estudio se empleó una metodología de tipo descriptiva de diseño no experimental. Se concluyó se procedió a realizar un estado a favor y contra del proyecto por lo que la implementación de diseño de un sistema de gestión de la seguridad.

(Guillen, 2018) en su estudio tuvo por objetivo determinar el impacto de los sistemas informáticos en la gestión de hoteles de 3 estrellas en la ciudad de Abancay – 2016. El método de investigación utilizado es investigación aplicada, el diseño del estudio es no empírico, en cuanto a población y muestra incluye a todos los empleados de un hotel de 3 estrellas, la población muestral de 75 empleados está definida por un motor de aplicación estructurado. El impacto de los sistemas informáticos es del 5%.

(Zacarias, 2018) en su estudio tuvo por objetivo determinar el impacto de un modelo de seguridad de la información basado en la norma ISO/IEC 27001:2013 en la reducción de amenazas a las fuentes de información en el Centro de Operaciones Policiales de la Región Policial Junín. Para este estudio se emplea una metodología es de tipo aplicada de nivel explicativo de método científico de diseño cuasi-experimental. Se ha encontrado que la evaluación interna del SGSI es necesaria para determinar el estado de los mecanismos de seguridad desplegados.

(Pizarro, 2018) en su estudio tuvo por finalidad Diseñar un modelo de seguridad de la información con un enfoque en el factor humano para proteger la información del ICPNA Región Centro. Esta investigación es de tipo aplicado-descriptivo de diseño no experimental método analítico-sintético. Se concluyó que la institución debe invertir en su seguridad de la información y ayudar a sus trabajadores a adquirir conocimiento y hábitos de seguridad de la información. Asimismo, debería implementar el modelo realizado con este fin.

(Ortiz, 2018) en su estudio tuvo por finalidad desarrollar de forma incremental la Norma Internacional ISO/IEC 27002:2013 para perfeccionar la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva Para este estudio se emplea una metodología es de tipo aplicada de nivel explicativo de método científico de diseño cuasi-experimental. Se concluyó que al implementar un Sistema de Gestión de Seguridad de la Información siguiendo las especificaciones

de la NTP-ISO/IEC 27001 que mediante la resolución ministerial N° 129-2012-PCM, el estado peruano aprueba para el uso obligatorio de esta norma. De este modo se podrá cumplir con los requisitos legales relacionados con la seguridad de la información y aspirar a una certificación internacional a largo plazo.

(Jara, 2018) en su estudio tuvo por finalidad calcular el efecto de la aplicación de un sistema de gestión de seguridad de la información en la gestión de riesgos. Como parte del enfoque cuantitativo, basado en el método de inferencia hipotética, se efectuó un estudio aplicado con un diseño pre experimental y un perfil longitudinal. Se ha observado una mejora en la aplicación del sistema de gestión de seguridad de la información en el proceso de gestión de riesgos de Municipalidad Distrital de Carabayllo, como lo demuestra el proceso estadístico de Wilcoxon.

(Huacasi, 2018) en su estudio tuvo por finalidad es implementar un sistema de gestión de seguridad de la información utilizando la NTP ISO/IEC 27001 para mejorar los procesos de seguridad de la información en el Ejército del Perú. Para este estudio se emplea una metodología es de tipo aplicada de nivel explicativo de método científico de diseño cuasi-experimental. Se ha encontrado que la realización de un sistema de gestión de seguridad de la información utilizando NTP ISO/IEC 27001 puede perfeccionar los procesos de seguridad de la información en una organización.

Asimismo, se desarrollaron los conceptos de las variables dependiente e independiente:

Sistema

Según (Arellano, 2020) es una agrupación de elementos que guardan relación entre sí y que se encargan de una determinada función

Para (Sanchez, y otros, 2019) el sistema es un conglomerado que se encarga de una determinada función según especificaciones requeridas para dicha tarea.

Pero para (Chaux, y otros, 2020) para que un sistema sea óptimo se necesita que tenga lo último en tecnología para que cumpla a la perfección la misión por la cual fue elaborado.

Sistema inteligente

Según, (Arellano, 2020) Una agrupación de elementos que trabajan en forma automatizada para realizar una función en menos tiempo y con la menor cantidad de recursos empleados en su fin.

Pero (Sanchez, y otros, 2019) nos dice que un sistema inteligente es el conjunto de acciones que nos permitirá realizar un fin en forma automatizada para ello recurre a las tecnologías de la información y softwares.

Además, (Chaux, y otros, 2020) nos señala que debe ir complementado de toda una gama de productos de última generación que estén interconectados entre sí en forma ágil, segura y que tengan gran capacidad de almacenamiento

ISO/IEC 27001

Es una entidad que depende de la norma internacional ISO 27001 y especifica los requisitos de seguridad de la información que deben cumplir las organizaciones para implantar, establecer, mantener y mejorar sus sistemas de gestión de la seguridad de la información (Alberto, 2018). Esta norma es aplicable a las pequeñas y medianas organizaciones y puede ser certificada, ya que ayuda a identificar, analizar y mitigar los riesgos que pueden afectar a los recursos de información (Andrés, 2018). La norma técnica peruana ISO/IEC 27001: 2014 está dividida en etapas según el ciclo de mejora continua o ciclo PDCA (Plan - Do - Check - Act), que permite la correcta implementación de la gestión de la seguridad de la información. Gobierno Electrónico e Informática (2019)

La etapa de planificación: Ayuda a las organizaciones a planificar políticas de seguridad y metas de seguridad de la información que sean adecuadas con las

políticas generales de seguridad de la información, y a tomar decisiones en relación con los controles que se aplican a la organización. (Arellano, 2020)

La etapa de Implementación: Esta etapa implica el desarrollo de las conclusiones anteriores, la aplicación de los controles aplicables y el seguimiento para generar pruebas (Alberto, 2018)

La etapa de revisión: Es la etapa en la que se realiza una auditoría para cuantificar la eficacia de los sistemas de control establecidos y comprobar que el SGSI cumple los objetivos previstos. (Arellano, 2020)

La etapa de mejora: En esta fase se mejoran los puntos débiles encontrados en las auditorías del punto anterior (Alberto, 2018)

La Norma se divide en 7 requisitos, que son los siguientes (Alberto, 2018) Contexto organizativo donde se definen los requisitos del contexto interno y externo del SGSI y se identifican los requerimientos necesarios.

1. Liderazgo: La política de seguridad de la información y sus objetivos están definidos y alineados con los objetivos del negocio.
2. Planificación: Se identifican los riesgos y oportunidades de seguridad de la información relacionados con los activos de información.
3. Soporte: Este requisito evalúa los recursos disponibles de la empresa y verifica que el personal que implementa el SGSI ha sido formado y comunicado a las partes interesadas.
4. Operaciones: identifica los riesgos asociados a la confidencialidad, integridad y disponibilidad estableciendo indicadores para medir la eficacia del SGSI.
5. Evaluación del rendimiento: desarrollar planes de acción para mitigar cualquier no conformidad identificada por la auditoría interna.
6. Mejora: Se establecen acciones correctivas para las no conformidades y se evita su repetición.

Gestión de riesgos

La ISO 27000 define la gestión de riesgos como "una ocupación coordinada para orientar y mantener el control de los riesgos en una organización" (Arellano, 2020) . La gestión de riesgos representa un conjunto de acciones que ayudan a

proteger los activos de información y a respetar su significado intrínseco, equilibrando las acciones empresariales causadas por los incidentes de estabilidad de la información relacionados a la pérdida de activos con los costes de mantenimiento de los sistemas de información y los datos que sustentan el rendimiento de la organización. Permitir un equilibrio. (Arellano, 2020) . La ISO 27001 es la parte más adecuada para su uso en los sistemas de gestión de la información, ya que establece directrices para la identificación, evaluación e implementación de los riesgos y ayuda a las empresas a detectar los recursos de información y las debilidades que pueden verse afectadas por la activación. (Gómez, y otros, 2018)

La metodología de evaluación de peligros tiene el objetivo de sensibilizar a cada una de las piezas de la compañía sobre esta metodología, y la administración de peligros se desarrolla de forma uniforme en cada una de las superficies (Arellano, 2020) .

Al llevar a cabo una evaluación de riesgos, hay que tener en cuenta todos los activos que tiene la organización y las amenazas y debilidades a las que está expuesta, y calcular la probabilidad de que se produzca una combinación de activos, amenazas y debilidades (Arellano, 2020) .

Gestión de seguridad: Es la selección, el uso y el seguimiento de los recursos físicos y humanos para evitar o reducir las pérdidas por riesgo absoluto. Los recursos humanos se refieren a los directivos, supervisores y empleados en general. (Arellano, 2020) .

Normas ISO: Es un conjunto de normas conocidas en todo el mundo y se creó para que las empresas puedan establecer un nivel uniforme de gestión, prestación de servicios y desarrollo de productos en la industria (Torres, 2019)

Evaluación riesgos: según (Torres, 2019) dice que el análisis de riesgos consiste en describir la probabilidad de ocurrencia y las posibles consecuencias del daño o evento resultante de la exposición a ciertos riesgos. Es un proceso interactivo que comienza con la detección de un evento y continúa hasta que el evento se trata como tal

Estándares: Es un patrón seguido por una de las variables que determina la utilidad de una actividad económica. Al observar estos datos, se puede ver si una empresa está funcionando de manera eficiente o no. (Torres, 2019)

Protección de datos: según (Arellano, 2020) .la privacidad es el proceso de proteger la información crítica de daños, pérdida o compromiso de los datos y aumenta a medida que la cantidad de datos creados y almacenados crece a un ritmo sin precedentes. También hay poca tolerancia para el tiempo de inactividad que puede hacer que la información crítica sea inaccesible.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

Según (Hernández, y otros, 2018) este estudio es pre experimental, ya que utilizara 2 tiempos de estudio, el antes y el después del experimento para que a partir de allí realizar una comparación de ambos resultados y ver su mejoría Según (Carrasco, 2018) una investigación de tipo aplicada es aquella que busca dar una respuesta ante una interrogante.

3.2. Variables y operacionalización

A. Definición conceptual

Variable dependiente: Desarrollar un sistema Hotelero

Según (Chaux, y otros, 2020) es el conjunto de tecnologías que un sistema operativo necesita para que realice una función de manera correcta.

Variable dependiente: gestión de seguridad de la información Apartado de operación de la norma ISO 27001:2014

Según (Proenca, y otros, 2018) las decisiones estratégicas de la organización para mantener la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de procesos de gestión de riesgos. Apartado de la norma ISO, que contribuye en establecer un control sobre los procesos de registro de la información.

B. Definición operacional

Variable dependiente: Desarrollar un sistema Hotelero

Según (Chaux, y otros, 2020) para el sistema sus dimensiones son según los requerimientos del cliente y del administrador por lo que sus dimensiones son: registrar y solicitudes del cliente

Variable dependiente: gestión de seguridad de la información Apartado de operación de la norma ISO 27001:2014

Según (Proenca, y otros, 2018) según las normas ISO sus dimensiones son: Planificación, implementación y control.

3.3. Población y muestra

Población

Según (Carrasco, 2018) nos dice que “es el conjunto de elementos diferentes pero que tienen características similares, estas son lo que será materia de estudio”. La población para este estudio será los 70 trabajadores del puerto Hotel La libertad

Muestra

Según (Hernández, y otros, 2018) “es el subconjunto de una población, que tiene características similares”. La muestra será de 50 trabajadores del puerto Hotel La libertad



Calculadora de Muestras

Margen de error: 10%
Nivel de confianza: 99%
Tamaño de Poblacion: 70
Calcular

Margen: 10%
Nivel de confianza: 99%
Poblacion: 70

Tamaño de muestra: 50

Ecuacion Estadística para Proporciones poblacionales

$$n = \frac{z^2(p \cdot q)}{e^2 + \frac{z^2(p \cdot q)}{N}}$$

n= Tamaño de la muestra
z= Nivel de confianza deseado
p= Proporción de la población con la característica deseada (éxito)
q= Proporción de la población sin la característica deseada (fracaso)
e= Nivel de error dispuesto a cometer
N= Tamaño de la población

Figura 1: Calculadora para hallar la muestra

Nota: (Condori, 2020)

Muestreo

Según (Caycho, y otros, 2019) que para el muestreo se considera es parte de una realidad antes y después en este estudio (población o universo) debe examinarse con la finalidad de hacer inferencias sobre dicha población. El muestreo será los 50 trabajadores del puerto Hotel La libertad

- **Criterios de muestreo**

Para el muestreo se consideró una muestra probabilística aleatoria que constituye un subgrupo representativo del total de la población donde todos han tenido la misma opción de ser seleccionados.

Una muestra probabilística se realiza de medir y analizar una prueba estadística de la muestra que serán elegidos de la población (Caycho, y otros, 2019)

3.4. Técnicas e instrumentos de recolección de datos

Técnicas: según (Caycho, y otros, 2019) nos hace mención que se usa para cotejar porcentajes o puntuaciones medias (en caso de usar el tipo de método cuantitativo) o hacer análisis de contenido, si es método cualitativo.

Fichaje: según (Caycho, y otros, 2019) nos dice que es toda aquella información que debe ser recopilada para que el estudio sea más fácil y sencillo.

3.5. Procedimientos

Confiabilidad: según [Carrasco, 2018] dice que en los instrumentos de realizarán la medición para los resultados deben arrojar datos exactos. Para medir la confiabilidad, se utilizaban pruebas y reevaluaciones, este método involucra utilizar la misma escala de medición en la muestra en base a dos condiciones similares para comparar las dos evaluaciones. Debido a esto, se utiliza el coeficiente de correlación de Pearson para hacer la medición y verificar su nivel de confiabilidad.

Según (Caycho, y otros, 2019) nos dice que en el método de confiabilidad,

los niveles de confiabilidad de la caja de recolección de datos se manejan en base al nivel de importancia, estos valores se detallan en la siguiente tabla:

Tabla 1: Niveles de Confiabilidad

Escala	Nivel
0.00 < sig. < 0.20	Muy bajo
0.20 ≤ sig. < 0.40	Bajo
0.40 ≤ sig. < 0.60	Regular
0.60 ≤ sig. < 0.80	Aceptable
0.80 ≤ sig. < 1.00	Elevado

Nota: (Hernández, y otros, 2018)

Instrumentos: según (Hernández, y otros, 2018) se emplearán para compilar información por medio de entrevistas o indagaciones.

Ficha de registro: según Carrasco (2018) nos indica que será para recopilar los datos que se considere necesarios para el estudio”

Validez: según Carrasco (2018) es aquella que se realiza por el jurado, el aspecto que los instrumentos utilizados tendrán grado de veracidad en el medio donde se va a aplicar. Se realizó mediante juicio de expertos.

Tabla 2. Nombres de los expertos

Ítems	Nombre y Apellido	Cargo
1		
2		
3		

Nota: SPSS V.26

3.6. Método de análisis de datos

Según [Carrasco, 2018] para proceder a realizar comparación de resultados Pre y Post que se hayan adquirido después del desarrollo del sistema hotelero. Las hipótesis se confirman o descartan, para ello se aplicará la prueba t de "Student", para que determine la "aceptación" o "rechazo" nuestra hipótesis, para lo que se empleará el software estadístico "SPSS Versión 26".

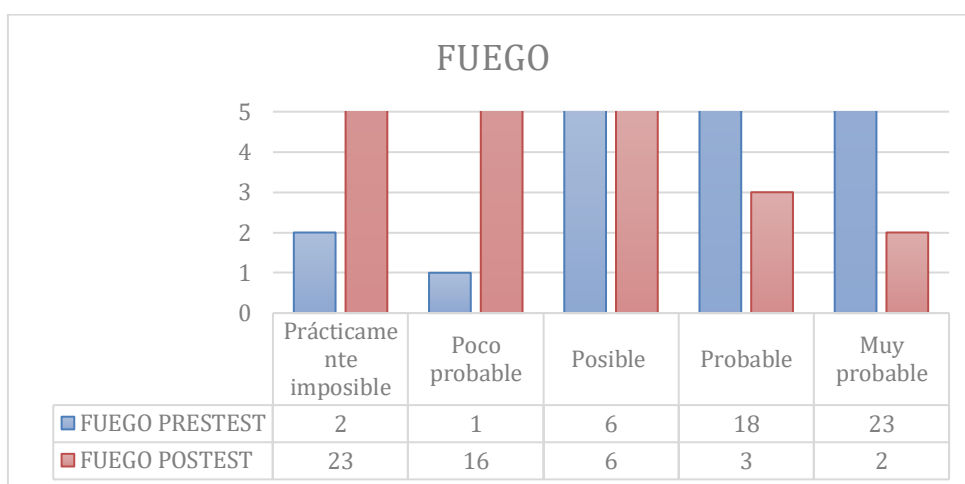
3.7. Aspectos éticos

Según Castro [2020] en este estudio se respetará la propiedad intelectual de los autores, para ello se incorporó las citas y las referencias bibliográficas en forma adecuada, también se cumplió con los directrices de la Universidad como también los dictámenes científicos del enfoque cuantitativo. Además, será pasado por el sistema Turnitin con grado similitud menor al 25% en formato ISO.

IV. RESULTADOS

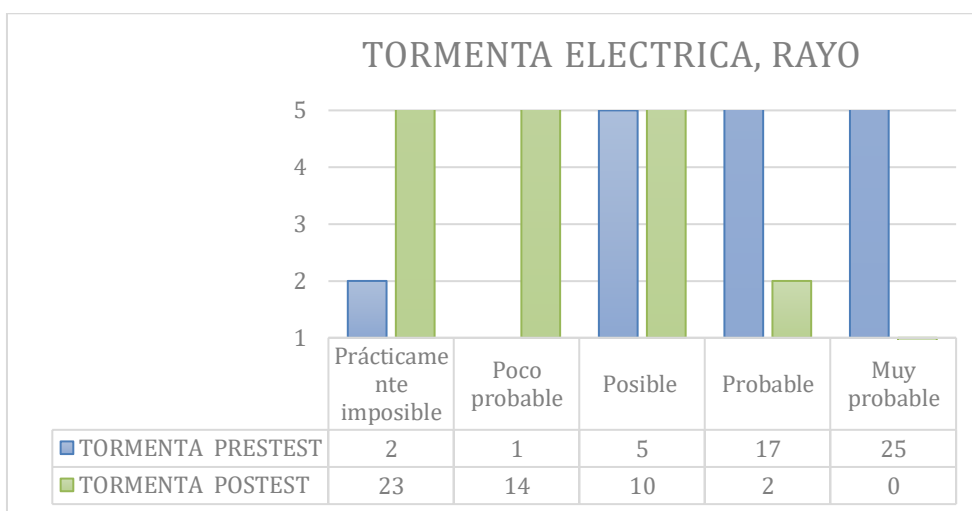
En este capítulo se realizará un análisis de una encuesta que se hizo antes y después de la implementación norma ISO para poder identificar las principales amenazas o vulneraciones que tiene la organización para proteger su información para ello se preguntó al personal de la empresa a través de un cuestionario donde se procedió a colocar todas las amenazas posibles que puede tener la empresa, para lo cual se emplea el programa SPSS V 26, según la percepción de los encuestados las principales amenazas que pueden poner en riesgo la información de la empresa son las siguientes:

Figura 2 Amenaza: Fuego



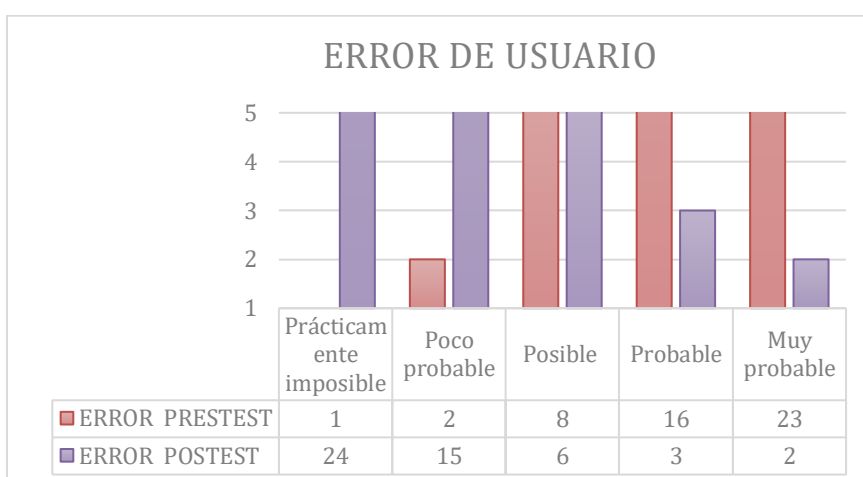
De acuerdo a la amenaza “Fuego” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 23 de ellos indicaron Muy probable la ocurrencia de fuego considerándose una amenaza, seguido de: Probable que ocurra (n=18), Posible (n=6), Poco probable (n=1) y Prácticamente imposible (n=2); Por otro lado en el Post-test, de los 50 trabajadores, 23 de ellos indicaron prácticamente imposible la ocurrencia de fuego considerándose una amenaza, seguido de: Poco probable (n=16), Posible (n=6), Probable (n=3) y Muy probable (n=2).

Figura 3 Amenaza: Tormenta eléctrica, rayo



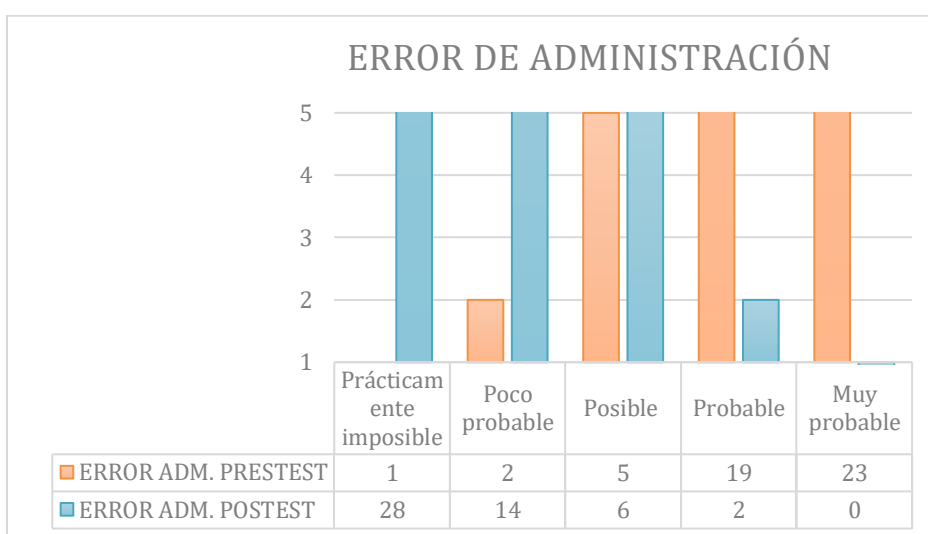
De acuerdo a la amenaza “Tormenta eléctrica, rayo” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 25 de ellos indicaron Muy probable la ocurrencia de Tormenta eléctrica, rayo considerándose una amenaza, seguido de: Probable que ocurra (n=17), Posible (n=5), Poco probable (n=1) y Prácticamente imposible (n=2); Por otro lado en el Post-test, de los 50 trabajadores, 23 de ellos indicaron prácticamente imposible de la ocurrencia de fuego considerándose una amenaza, seguido de: Poco probable (n=14), Posible (n=10), Probable (n=2) y Muy probable (n=0).

Figura 4 Amenaza: Error de usuario



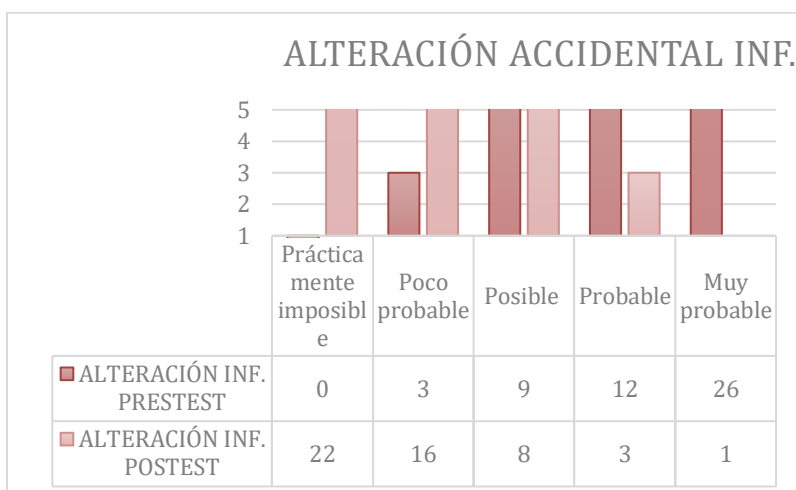
De acuerdo a la amenaza “Error de usuario” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 23 de ellos indicaron Muy probable de la ocurrencia de Error de usuario considerándose una amenaza, seguido de: Probable que ocurra (n=16), Posible (n=8), Poco probable (n=2) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 24 de ellos indicaron prácticamente imposible de la ocurrencia de fuego considerándose una amenaza, seguido de: Poco probable (n=15), Posible (n=6), Probable (n=3) y Muy probable (n=2).

Figura 5 Amenaza: Errores del administrador



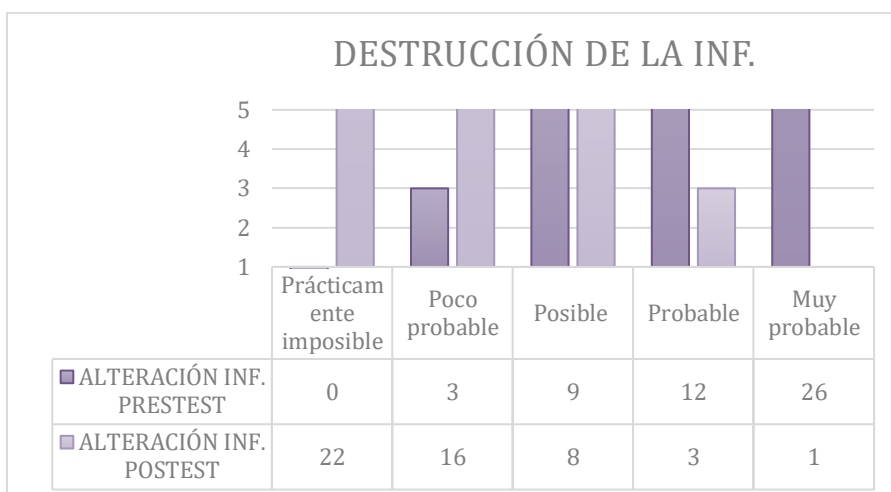
De acuerdo a la amenaza “Errores del administrador” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 23 de ellos indicaron Muy probable la ocurrencia de Errores del administrador considerándose una amenaza, seguido de: Probable que ocurra (n=19), Posible (n=5), Poco probable (n=2) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 28 de ellos indicaron prácticamente imposible la ocurrencia de Errores del administrador considerándose una amenaza, seguido de: Poco probable (n=14), Posible (n=6), Probable (n=2) y Muy probable (n=0).

Figura 6 Amenaza: Alteración accidental de la información



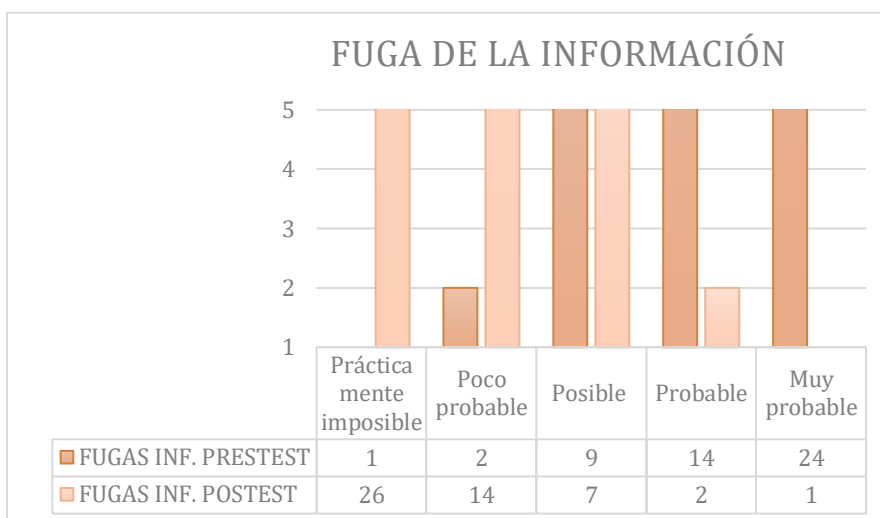
De acuerdo a la amenaza “Alteración accidental de la información” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 26 de ellos indicaron Muy probable la ocurrencia de Alteración accidental de la información considerándose una amenaza, seguido de: Probable que ocurra (n=12), Posible (n=9), Poco probable (n=3) y Prácticamente imposible (n=0); Por otro lado, en el Post-test, de los 50 trabajadores, 22 de ellos indicaron prácticamente imposible la ocurrencia de Alteración accidental de la información considerándose una amenaza, seguido de: Poco probable (n=16), Posible (n=8), Probable (n=3) y Muy probable (n=1).

Figura 7 Amenaza: Destrucción de la información



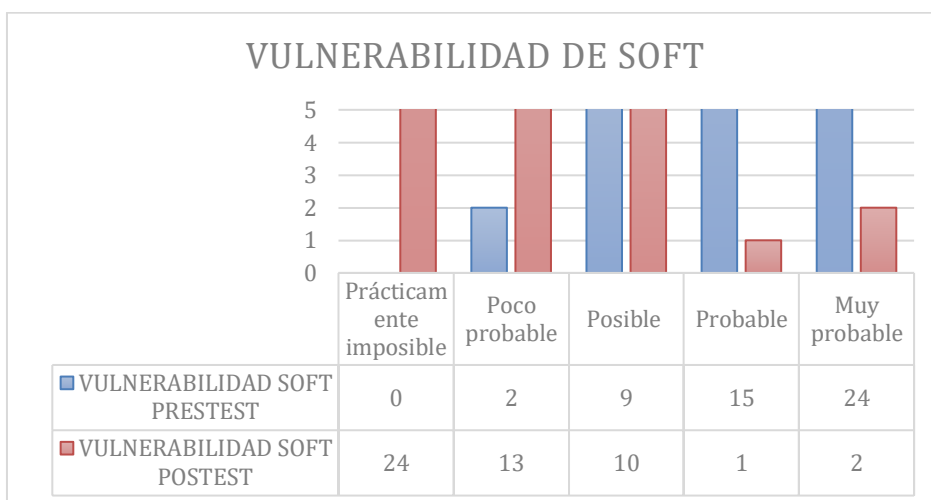
De acuerdo a la amenaza “Destrucción de la información” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 26 de ellos indicaron Muy probable la ocurrencia de Destrucción de la información considerándose una amenaza, seguido de: Probable que ocurra (n=12), Posible (n=9), Poco probable (n=3) y Prácticamente imposible (n=0); Por otro lado en el Post-test, de los 50 trabajadores, 22 de ellos indicaron prácticamente imposible la ocurrencia de Destrucción de la información considerándose una amenaza, seguido de: Poco probable (n=16), Posible (n=8), Probable (n=3) y Muy probable (n=1).

Figura 8 Amenaza: Fugas de la información



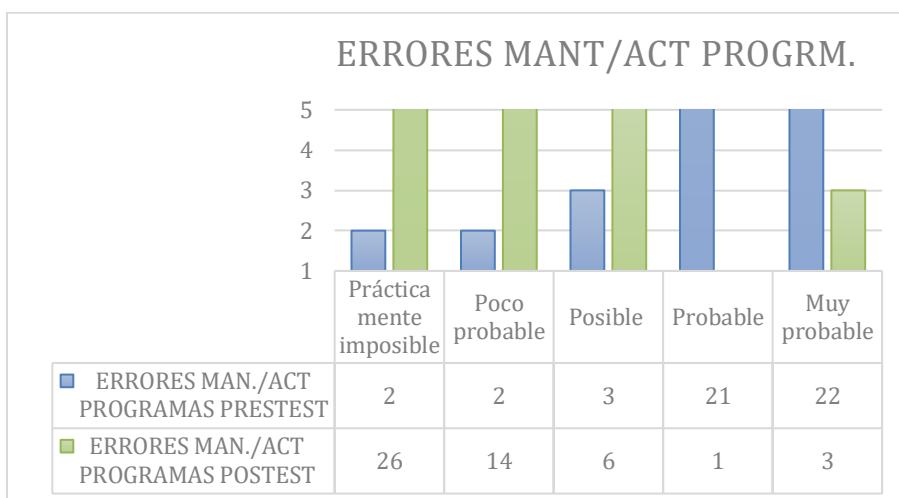
De acuerdo a la amenaza “Fugas de la información” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 24 de ellos indicaron Muy probable la ocurrencia de Fugas de la información considerándose una amenaza, seguido de: Probable que ocurra (n=14), Posible (n=9), Poco probable (n=2) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 26 de ellos indicaron prácticamente imposible la ocurrencia de Fugas de la información considerándose una amenaza, seguido de: Poco probable (n=14), Posible (n=7), Probable (n=2) y Muy probable (n=1).

Figura 9 Amenaza: Vulnerabilidades de los programas (software)



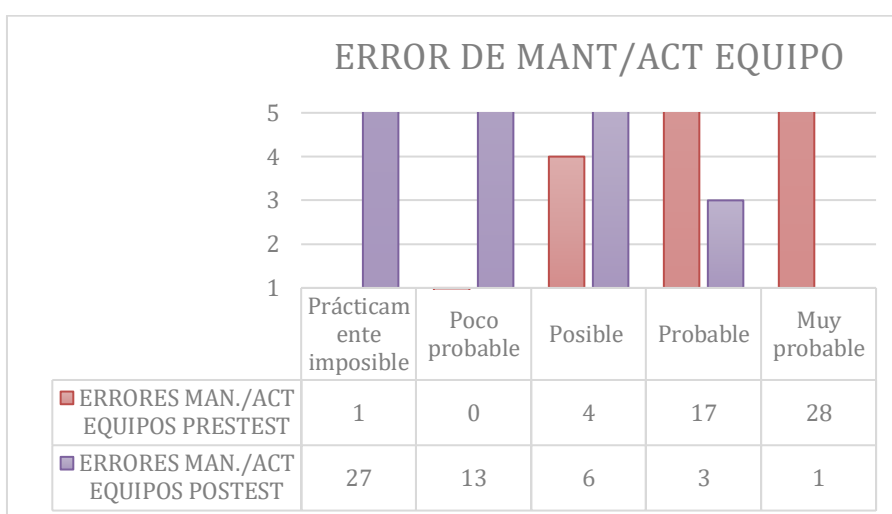
De acuerdo a la amenaza “Vulnerabilidades de los programas (software)” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 24 de ellos indicaron Muy probable de la ocurrencia de Vulnerabilidades de los programas (software) considerándose una amenaza, seguido de: Probable que ocurra (n=15), Posible (n=9), Poco probable (n=2) y Prácticamente imposible (n=0); Por otro lado en el Post-test, de los 50 trabajadores, 24 de ellos indicaron prácticamente imposible la ocurrencia de Vulnerabilidades de los programas (software) considerándose una amenaza, seguido de: Poco probable (n=13), Posible (n=10), Probable (n=1) y Muy probable (n=2).

Figura 10 Amenaza: Errores de mantenimiento /actualización de programas



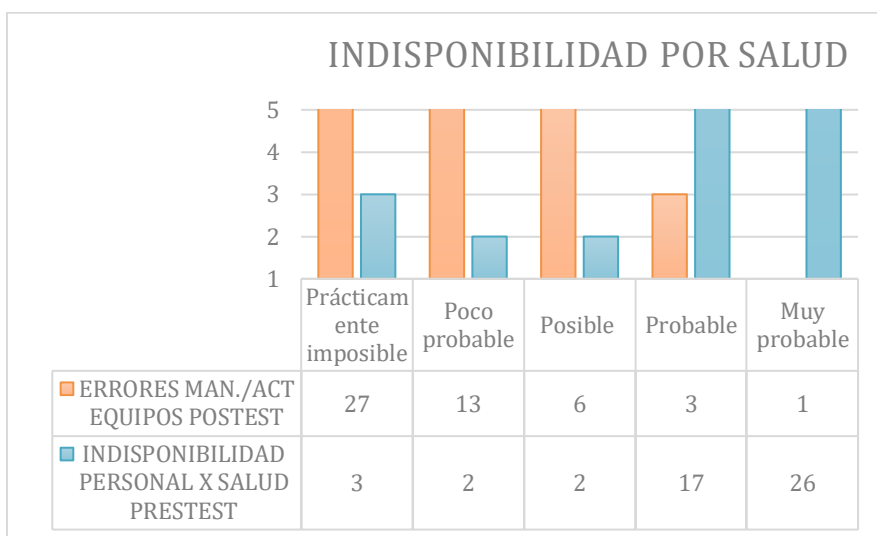
De acuerdo a la amenaza “Errores de mantenimiento /actualización de programas” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 22 de ellos indicaron Muy probable la ocurrencia de Errores de mantenimiento /actualización de programas considerándose una amenaza, seguido de: Probable que ocurra (n=21), Posible (n=3), Poco probable (n=2) y Prácticamente imposible (n=2); Por otro lado en el Post-test, de los 50 trabajadores, 26 de ellos indicaron prácticamente imposible la ocurrencia de Errores de mantenimiento /actualización de programas considerándose una amenaza, seguido de: Poco probable (n=14), Posible (n=6), Probable (n=1) y Muy probable (n=3).

Figura 1 Amenaza: Errores de mantenimiento / actualización de equipos



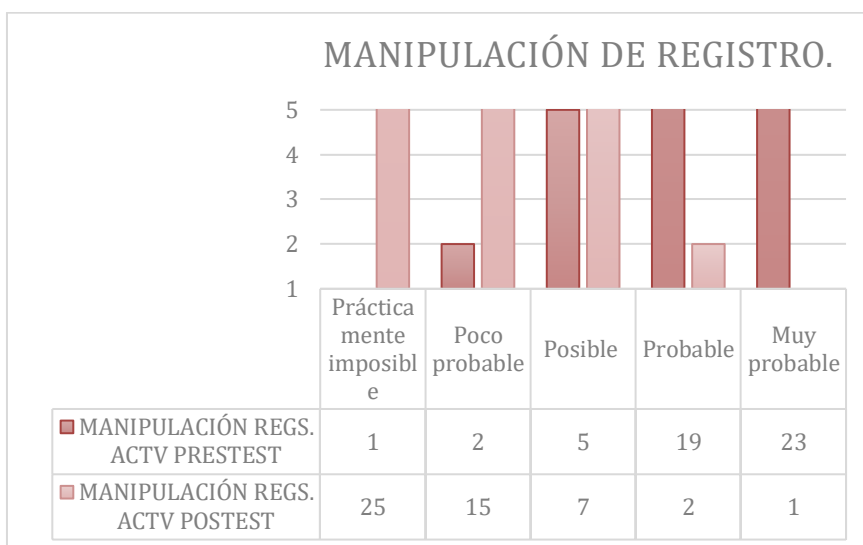
De acuerdo a la amenaza “Errores de mantenimiento / actualización de equipos” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 28 de ellos indicaron Muy probable la ocurrencia de Errores de mantenimiento / actualización de equipos considerándose una amenaza, seguido de: Probable que ocurra (n=17), Posible (n=4), Poco probable (n=0) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 27 de ellos indicaron prácticamente imposible la ocurrencia de “Errores de mantenimiento / actualización de equipos” considerándose una amenaza, seguido de: Poco probable (n=13), Posible (n=6), Probable (n=3) y Muy probable (n=1).

Figura 12 Amenaza: Indisponibilidad del personal por salud



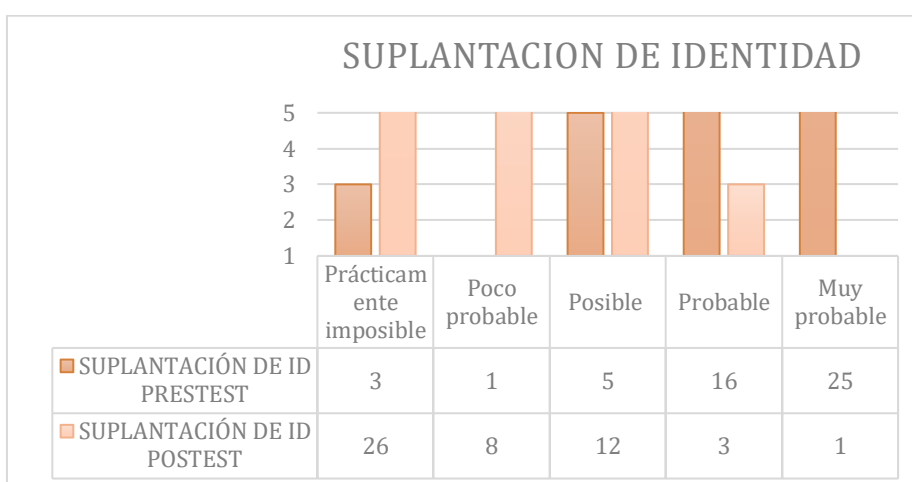
De acuerdo a la amenaza “Indisponibilidad del personal por salud” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 23 de ellos indicaron Muy probable la ocurrencia de Indisponibilidad del personal por salud considerándose una amenaza, seguido de: Probable que ocurra (n=18), Posible (n=6), Poco probable (n=1) y Prácticamente imposible (n=2); Por otro lado en el Post-test, de los 50 trabajadores, 23 de ellos indicaron prácticamente imposible la ocurrencia de Indisponibilidad del personal por salud considerándose una amenaza, seguido de: Poco probable (n=16), Posible (n=6), Probable (n=3) y Muy probable (n=2).

Figura 2 Amenaza: Manipulación de los registros de actividad



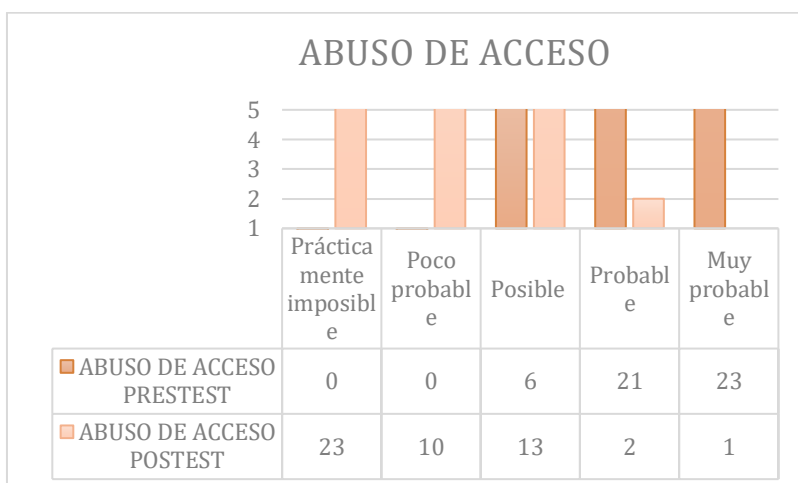
De acuerdo a la amenaza “Manipulación de los registros de actividad” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 23 de ellos indicaron Muy probable la ocurrencia de Manipulación de los registros de actividad considerándose una amenaza, seguido de: Probable que ocurra (n=19), Posible (n=5), Poco probable (n=2) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 25 de ellos indicaron prácticamente imposible la ocurrencia de Manipulación de los registros de actividad considerándose una amenaza, seguido de: Poco probable (n=15), Posible (n=7), Probable (n=2) y Muy probable (n=1).

Figura 14 Amenaza: Suplantación de la identidad del usuario



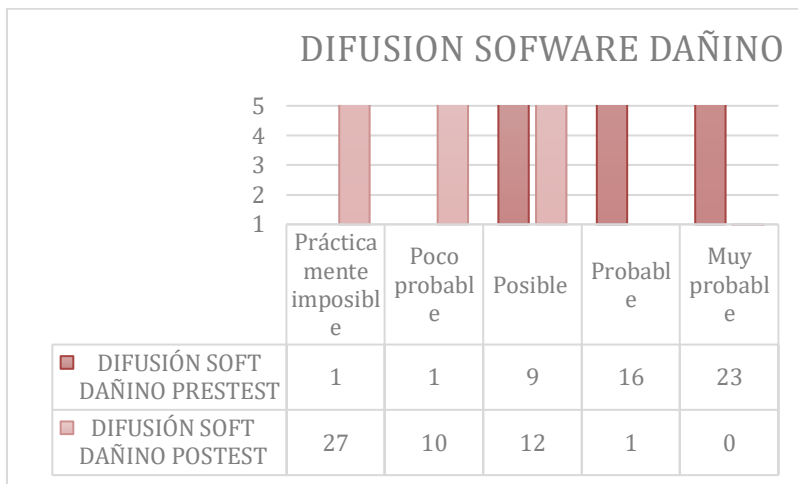
De acuerdo a la amenaza “suplantación de identidad” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 25 de ellos indicaron Muy probable la ocurrencia de suplantación de identidad considerándose una amenaza, seguido de: Probable que ocurra (n=16), Posible (n=5), Poco probable (n=1) y Prácticamente imposible (n=3); Por otro lado en el Post-test, de los 50 trabajadores, 26 de ellos indicaron prácticamente imposible la ocurrencia de suplantación de identidad considerándose una amenaza, seguido de: Poco probable (n=8), Posible (n=12), Probable (n=3) y Muy probable (n=1).

Figura 15 Amenaza: Abuso de privilegio de acceso



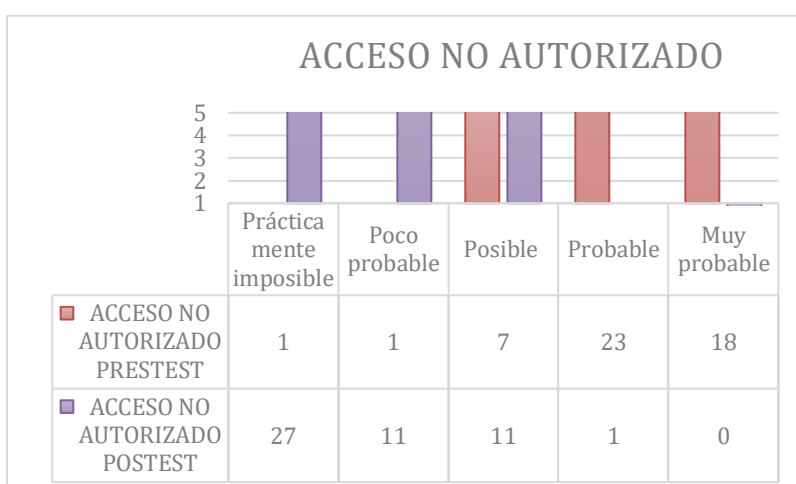
De acuerdo a la amenaza “abuso de privilegios de acceso” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 23 de ellos indicaron Muy probable la ocurrencia de abuso de privilegios de acceso considerándose una amenaza, seguido de: Probable que ocurra (n=21), Posible (n=6), Poco probable (n=0) y Prácticamente imposible (n=0); Por otro lado en el Post-test, de los 50 trabajadores, 23 de ellos indicaron prácticamente imposible la ocurrencia de abuso de privilegios de acceso considerándose una amenaza, seguido de: Poco probable (n=10), Posible (n=13), Probable (n=2) y Muy probable (n=1).

Figura 3 Amenaza: difusión de software dañino



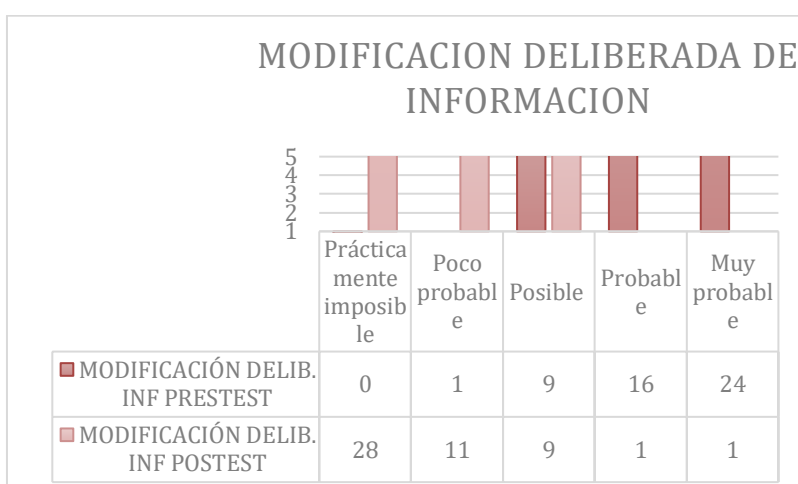
De acuerdo a la amenaza “difusión de software dañino” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 23 de ellos indicaron Muy probable la ocurrencia de difusión de software dañino considerándose una amenaza, seguido de: Probable que ocurra (n=16), Posible (n=9), Poco probable (n=1) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 27 de ellos indicaron prácticamente imposible la ocurrencia de difusión de software dañino considerándose una amenaza, seguido de: Poco probable (n=10), Posible (n=11), Probable (n=1) y Muy probable (n=0).

Figura 4 Amenaza: Acceso no autorizado



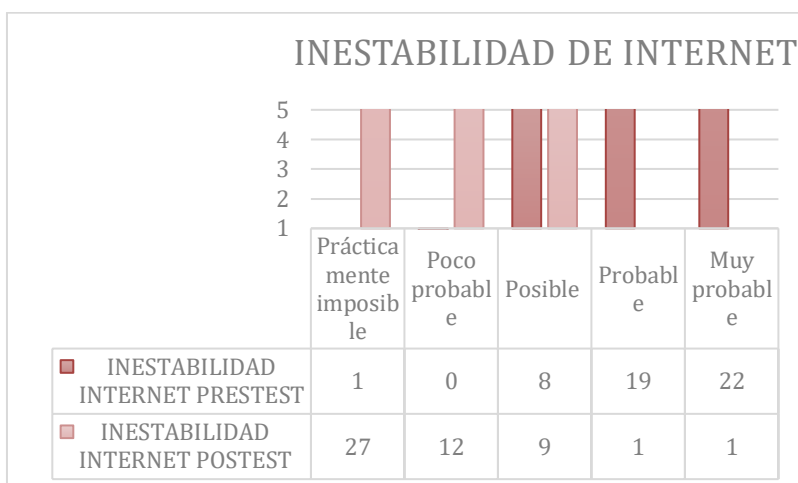
De acuerdo a la amenaza “acceso no autorizado” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 18 de ellos indicaron Muy probable la ocurrencia de acceso no autorizado considerándose una amenaza, seguido de: Probable que ocurra (n=23), Posible (n=7), Poco probable (n=1) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 27 de ellos indicaron prácticamente imposible la ocurrencia de acceso no autorizado considerándose una amenaza, seguido de: Poco probable (n=11), Posible (n=11), Probable (n=1) y Muy probable (n=0).

Figura 18 Amenaza: Modificación deliberada de la información



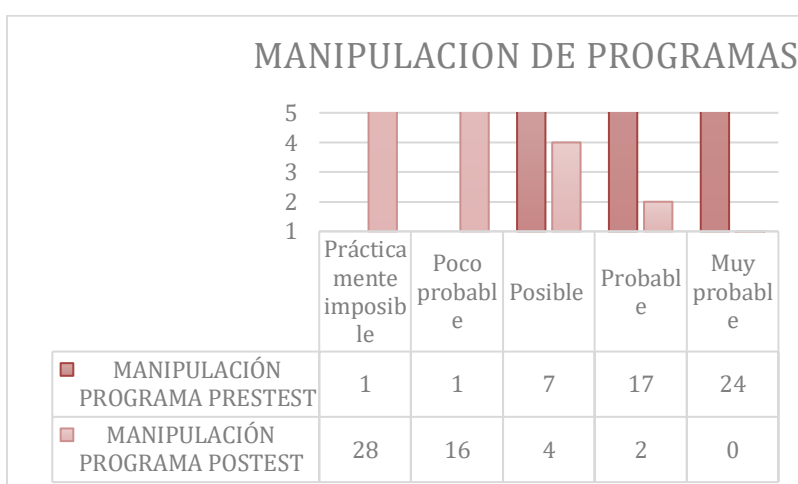
De acuerdo a la amenaza “modificación deliberada de información” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 24 de ellos indicaron Muy probable la ocurrencia de modificación deliberada de información considerándose una amenaza, seguido de: Probable que ocurra (n=16), Posible (n=9), Poco probable (n=1) y Prácticamente imposible (n=0); Por otro lado, en el Post-test, de los 50 trabajadores, 28 de ellos indicaron prácticamente imposible la ocurrencia de modificación deliberada de información considerándose una amenaza, seguido de: Poco probable (n=11), Posible (n=9), Probable (n=1) y Muy probable (n=1).

Figura 5 Amenaza: Inestabilidad de la línea de internet



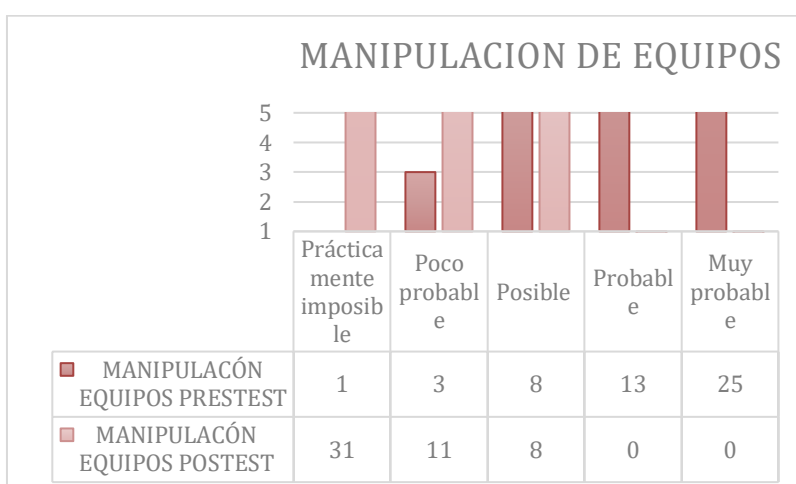
De acuerdo a la amenaza “inestabilidad de la línea de internet” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 22 de ellos indicaron Muy probable la ocurrencia de inestabilidad de la línea de internet considerándose una amenaza, seguido de: Probable que ocurra (n=19), Posible (n=8), Poco probable (n=0) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 27 de ellos indicaron prácticamente imposible la ocurrencia de inestabilidad de la línea de internet considerándose una amenaza, seguido de: Poco probable (n=12), Posible (n=9), Probable (n=1) y Muy probable (n=1).

Figura 20 Amenaza: Manipulación de programa



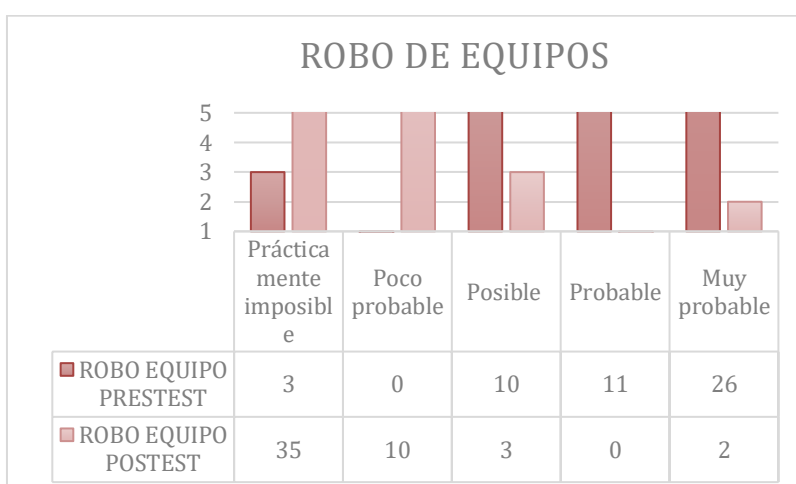
De acuerdo a la amenaza “manipulación de programas” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 24 de ellos indicaron Muy probable la ocurrencia de manipulación de programas considerándose una amenaza, seguido de: Probable que ocurra (n=17), Posible (n=7), Poco probable (n=1) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 28 de ellos indicaron prácticamente imposible la ocurrencia de manipulación de programas considerándose una amenaza, seguido de: Poco probable (n=16), Posible (n=4), Probable (n=2) y Muy probable (n=0).

Figura 21 Amenaza: Manipulación de equipo



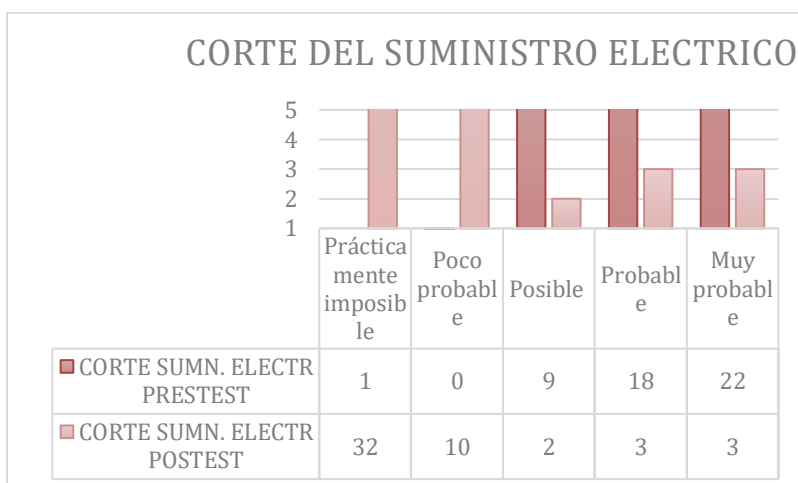
De acuerdo a la amenaza “manipulación de equipos” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 25 de ellos indicaron Muy probable la ocurrencia de manipulación de equipos considerándose una amenaza, seguido de: Probable que ocurra (n=13), Posible (n=8), Poco probable (n=3) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 31 de ellos indicaron prácticamente imposible la ocurrencia de manipulación de equipos considerándose una amenaza, seguido de: Poco probable (n=11), Posible (n=8), Probable (n=0) y Muy probable (n=0).

Figura 22 Amenaza: Robo de equipo



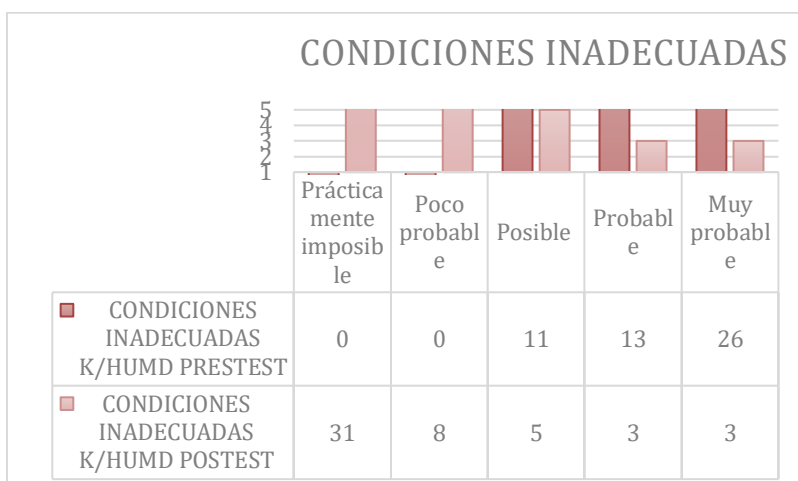
De acuerdo a la amenaza “robo de equipos” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 26 de ellos indicaron Muy probable la ocurrencia de robo de equipos considerándose una amenaza, seguido de: Probable que ocurra (n=11), Posible (n=10), Poco probable (n=0) y Prácticamente imposible (n=3); Por otro lado, en el Post-test, de los 50 trabajadores, 35 de ellos indicaron prácticamente imposible la ocurrencia de robo de equipos considerándose una amenaza, seguido de: Poco probable (n=10), Posible (n=3), Probable (n=0) y Muy probable (n=2).

Figura 23 Amenaza: Corte de suministro eléctrico



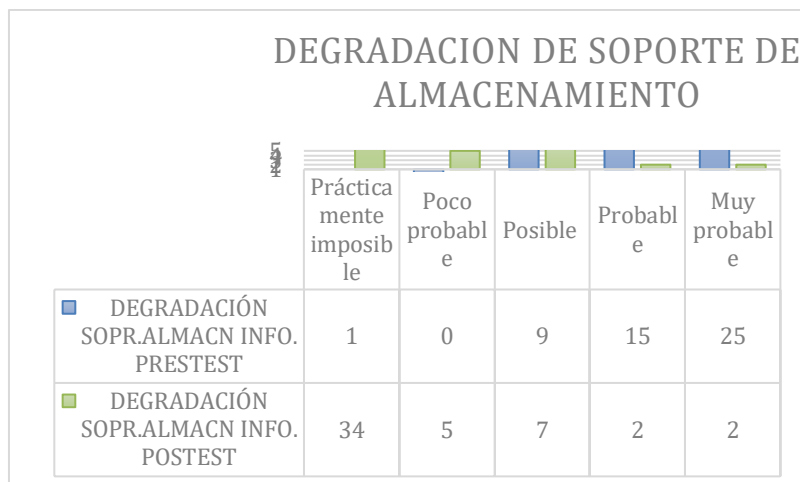
De acuerdo a la amenaza corte del suministro eléctrico visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 22 de ellos indicaron Muy probable la ocurrencia de corte del suministro eléctrico considerándose una amenaza, seguido de: Probable que ocurra (n=18), Posible (n=9), Poco probable (n=0) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 32 de ellos indicaron prácticamente imposible la ocurrencia de corte del suministro eléctrico considerándose una amenaza, seguido de: Poco probable (n=10), Posible (n=2), Probable (n=3) y Muy probable (n=3).

Figura 24 Amenaza: Condiciones inadecuadas de temperatura o humedad



De acuerdo a la amenaza “condiciones inadecuadas de temperatura o humedad” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 26 de ellos indicaron Muy probable la ocurrencia de condiciones inadecuadas de temperatura o humedad considerándose una amenaza, seguido de: Probable que ocurra (n=13), Posible (n=11), Poco probable (n=0) y Prácticamente imposible (n=0); Por otro lado en el Post-test, de los 50 trabajadores, 31 de ellos indicaron prácticamente imposible la ocurrencia de condiciones inadecuadas de temperatura o humedad considerándose una amenaza, seguido de: Poco probable (n=8), Posible (n=5), Probable (n=3) y Muy probable (n=3).

Figura 25 Amenaza: Degradación de los soportes de almacenamiento de la información



De acuerdo a la amenaza “degradación de los soportes de almacenamiento de la información” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 25 de ellos indicaron Muy probable la ocurrencia de Degradación de los soportes de almacenamiento de la información considerándose una amenaza, seguido de: Probable que ocurra (n=15), Posible (n=9), Poco probable (n=0) y Prácticamente imposible (n=1); Por otro lado en el Post-test, de los 50 trabajadores, 35 de ellos indicaron prácticamente imposible la ocurrencia de Degradación de los soportes de almacenamiento de la información considerándose una amenaza, seguido de: Poco probable (n=5), Posible (n=7), Probable (n=2) y Muy probable (n=2).

Figura 26 Amenaza: Instalación de software no autorizado

INSTALACION DE SOFTWARE NO AUTORIZADO					
	Práctica mente imposibl e	Poco probabl e	Posible	Probabl e	Muy probabl e
■ INSTALACIÓN SOFT NO AUTORIZADO PRETEST	2	0	9	16	23
■ INSTALACIÓN SOFT NO AUTORIZADO POSTEST	28	13	7	1	1

De acuerdo a la amenaza “instalación de software no autorizado” visualizamos en la figura anterior, en el Pre-test, de los 50 trabajadores, 23 de ellos indicaron Muy probable la ocurrencia de Instalación de software no autorizado considerándose una amenaza, seguido de: Probable que ocurra (n=16), Posible (n=9), Poco probable (n=0) y Prácticamente imposible (n=2); Por otro lado en el Post-test, de los 50 trabajadores, 28 de ellos indicaron prácticamente imposible la ocurrencia de Instalación de software no autorizado considerándose una amenaza, seguido de: Poco probable (n=13), Posible (n=7), Probable (n=1) y Muy probable (n=1).

En este capítulo se realizará el Análisis de los resultados obtenidos en el estudio de investigación. Se realizó el pre y post test para ello se empleó el programa SPSS V26 y los hallazgos de la estadística descriptiva conseguidos para la investigación se pueden observar en las siguientes tablas:

Indicador 1: planificación:

Los resultados descriptivos para el primer indicador se pueden apreciar en el siguiente cuadro:

Tabla 3: Estadísticos Descriptivos Planificación

	N	Min	Max	Med	Desviación Estándar	Varianza
Pretest_ANA	20	45	83	68.85	12,991	168,766
Postest_ANA	20	0	30	15.40	8,165	66,674
N valido (por lista)	20					

La Tabla 3 muestra que, para nuestra muestra, la planificación media fue de 68,85% en pre-test y 15,40% en post-test, lo que significa una reducción del 53% del % promedio obtenido, conduce a la implementación de un sistema de gestión de seguridad de la información que puede limitar la información no autorizada.

Indicador 2: Implementación:

Los resultados descriptivos para el segundo indicador se pueden apreciar en el siguiente cuadro:

Tabla 4: Estadísticos descriptivos Implementación

	N	Min	Max	Med	Desviación Estándar	Varianza
Pretest_EMB	20	0	70	56,60	8,708	75,832
Postest_EMB	20	40	22	11,40	7,287	56,095
N valido (por lista)	20					

En la tabla 4 se puede medir que la tasa de implementación promedio es de 56.60%, mientras que en esta última prueba es de 11.40% de la muestra, por lo que al calcular el promedio notamos una disminución de 45.20%, haciendo diferente el manejo de datos y teniendo más control sobre todas las áreas del sistema de gestión de seguridad de la información.

Indicador 3: Control informático

Los resultados descriptivos para el tercer indicador se pueden apreciar en el siguiente cuadro

Tabla 5: Estadísticos descriptivos control

	N	Min	Max	Med	Desviación Estándar	Varianza
Pretest_CI	20	30	75	47,15	12,419	154,239
Postest_CI	20	0	29	11,95	9,795	95,945
N valido (por lista)	20					

En la tabla 5 se puede medir que la tasa media de control alcanza el 47,15 %, mientras que en el examen post test el valor de la muestra correspondiente alcanza el 11,95 %, disminuyendo así en un 35,20 % cuando en las muestras. Encontramos la similitud entre los valores medios, para realizar el sistema de gestión de seguridad de la información para la eliminación de virus informáticos.

Análisis Inferencial

En tal carácter, se utilizará el método Kolmogorov- Smirnov ya que sus cifras dependen de los detalles dados al utilizar una distribución normal sobre muestras mayores de 50 (Carrasco, 2018). Si el valor es mayor a 0,05, la información se distribuye normalmente, de lo contrario, si es menor a 0,05, la información está fuera de lo común. La prueba con el programa estadístico SPSS v26 arrojó los siguientes resultados:

Indicador 1: Planificación

En la primera prueba de normalidad métrica en los ensayos de pretest y post-test se obtuvieron los siguientes resultados estadísticos:

Tabla 6: Prueba de Normalidad de planificación

	KOLMOGOROV – SMIRNOV		
	Estadístico	GI	Sig.
Pretest_ANA	,254	20	.002
Postest_ANA	,213	20	.018
Corrección de significación de Lilliefors			

En la Tabla 6, los resultados de las pruebas muestran que la Sig de la muestra previamente creada es 0.002 y su valor es menor a 0.05 (nivel significativo), por lo que se rechaza la hipótesis nula. Asimismo, las pruebas muestran que Sig. es 0.018 y su valor es menor. Por lo tanto, usaremos Wilcoxon ya que ambos tienen distribuciones atípicas.

Indicador 2: Implementación

Los datos en la primera prueba, se verifica la normalidad de la segunda métrica y se obtienen los siguientes resultados estadísticos durante la última prueba

Tabla 7: Prueba de Normalidad implementación

	KOLMOGOROV – SMIRNOV		
	Estadístico	GI	Sig.
Pretest_ EMDB	,167	20	.144
Postest_ EMDB	,102	20	.200
Corrección de significación de Lilliefors			

En la Tabla 7, los resultados estimados están en buena concordancia con la distribución normal, ya que el valor de significación pre-test es 0.114 y el valor de significación post-test 0.200, ambos cumplen sus funciones y son mayores que el rango de error ($\alpha = 0.05$)

Indicador 3: Control Informático

El tercer indicador se probó la normalidad en las pruebas de pretest y post-test con los siguientes resultados estadísticos:

Tabla 8: Prueba de Normalidad de control

	KOLMOGOROV – SMIRNOV		
	Estadístico	GI	Sig.
Pretest_CI	,268	20	.001
Postest_CI	,189	20	.060
Corrección de significación de Lilliefors			

En la Tabla 8, los resultados estimados son de valores atípicos porque la significancia antes del ensayo es 0.001 y la significación después del ensayo es 0.060, en este caso usaremos Wilcoxon ya que tiene el valor más bajo en el rango de error ($\alpha = 0.05$)

Prueba de hipótesis

En este estudio se utilizaron T-Student y Wilcoxon. Según (Caycho Carlos, Castillo Carlos, Merino Víctor, 2020) los datos experimentales o muestrales obtenidos para la hipótesis deben satisfacer la condición estándar, asumiendo que los resultados contienen datos no paramétricos.

Hipótesis de investigación 1:

H0: El desarrollo de un sistema hotelero NO mejorará la planificación que está basado en el apartado de operación de la norma ISO 27001:2014, para la empresa Puerto Hotel La Libertad

$H_0 = ANA \geq ANA$

H1: El desarrollo de un sistema hotelero SI mejorará la planificación que está basado en el apartado de operación de la norma ISO 27001:2014, para la empresa Puerto Hotel La Libertad

$H_1 = ANA < ANA$

Para la contratación de la hipótesis de la investigación 1, se explicó la prueba de Wilcoxon, en vista que la información adoptó una distribución no normal, en la Tabla 9 se observa que el valor de 0.000 es menor a 0.05, lo que indica que existe una diferencia en la tasa de acceso no autorizado antes y después de la información del sistema de gestión de la seguridad

Tabla 9: Prueba de rango de Wilcoxon de ANA

		N	Rango promedio	Suma de rangos
Pretest_ANA	Rangos negativos	20a	10,50	210,00
Postest_ANA	Rangos positivos	0b	,00	,00
	Empates	0c		
	Total	20		

a. Postest_ANA < Pretest_ANA
b. Postest_ANA > Pretest_ANA
c. Postest_ANA = Pretest_ANA

Tabla 10: Estadístico de contraste del Indicador 1

	Pretest_ANA & Postest_ANA
z	-3,922b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Una forma de probar una hipótesis es aproximar la normal (Z), ya que se obtiene un valor (-3,922) < α (0,05) utilizado en el nivel de significación. En conclusión, la descripción anterior es cierta y la hipótesis alterna es la hipótesis aceptada.

Hipótesis de investigación 2:

H0: El desarrollo de un sistema hotelero NO mejorará la implementación de políticas basado en el apartado de operación de operación de la norma ISO 27001:2014, para la empresa Puerto Hotel La Libertad

H0 = EMBDa \geq EMBDd

H1: El desarrollo de un sistema hotelero SI mejorará la implementación de políticas basado en el apartado de operación de operación de la norma ISO 27001:2014, para la empresa Puerto Hotel La Libertad

H1 = EMBDa < EMBDd

Para la contratación de la hipótesis de investigación 2, se utilizó la prueba t de Student, asumiendo que la información se distribuye normalmente. Como se puede observar en la Tabla 11, las medias antes y después del procedimiento son significativamente diferentes debido al valor de t (17.588) < α (0,05)

Tabla 11: Prueba t Student de Manipular Borrar Eliminar Datos

	Media	t	Gl	Sig.(bilateral)
Pretest_EMDB	,268	17,588	19	,000
Postest_EMDB	,189			

Hipótesis de investigación 3:

H0: El desarrollo de un sistema hotelero NO mejorara control o eliminación de las amenazas, basado en el apartado de operación de la norma ISO 27001:2014, para la empresa Puerto Hotel La Libertad

H0= CI \geq CI

H1: El desarrollo de un sistema hotelero SI mejorara control o eliminación de las amenazas, basado en el apartado de operación de la norma ISO 27001:2014, para la empresa Puerto Hotel La Libertad

H1 = CI <CI

Para la contratación de la hipótesis de la investigación 3, explicó la prueba de Wilcoxon, en vista que la información adoptó una distribución no normal, en la tabla 12, se apreció que existe un valor de 0.000 menor a 0.05 lo que significa que hay una diferencia en el % de accesos no autorizados antes y después del sistema de gestión para la seguridad de la información.

Tabla 12: Prueba de rango de Wilcoxon de CI

		N	Rango promedio	Suma de rangos
Pretest_CIE	Rangos negativos	20a	10,50	210,00
Postest_CIE	Rangos positivos	0b	,00	,00
	Empates	0c		
	Total	20		

a. Postest_ CI < Pretest_ CI
b. Postest_ CI > Pretest_ CI
c. Postest_ CI = Pretest_ CI

Tabla 13: Estadístico de contraste de CI

Postest_CI & Pretest_CI	
z	-3,921b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Una forma de probar la hipótesis es aproximar la normal (Z), ya que se obtiene un valor $(-3,921) < \alpha (0,05)$ utilizado en el nivel de significación. En conclusión, la descripción anterior es cierta y la hipótesis alterna es la hipótesis aceptada.

Posteriormente se presentan los resultados de la encuesta Pre y Post para identificar las amenazas y establecer probabilidad de ocurrencia adquirido después del desarrollo del sistema hotelero.

V. DISCUSIÓN

En nuestro trabajo de investigación se obtiene que al implementar el sistema hotelero mejorará nuestra seguridad de la información ya que se implementará con el apartado de operaciones de las normas ISO 27001:2014 para ello se realizó las pruebas de pre y post test en donde nuestro resultado de porcentaje de planificación aumento en un 84.6% a partir de la implementación, nuestro porcentaje de implementación también aumento favorablemente a un 88.6% y por ultimo porcentaje de control aumento en 88.05% después de la implementación del sistema Hotelero.

En el estudio realizado por (Cueva, y otros, 2018) titulado: “Gestión de la historia clínica y la seguridad de la información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014” los resultados obtenidos de la implementación de la norma ISO 27001:2014 es que mejoro en forma notable todos los procesos de planificación de la entidad, mejorando en un 79% después de su implementación, además de mejorar su eficiencia en un 71% y con el curso del tiempo se verán progresos en medida que el personal se acostumbre y sobre todo se capacite. En comparación con nuestros resultados obtenidos en nuestra investigación, el 68,85% de los encuestados nos dijo que no habría mejora sin una planificación previa al desarrollo del sistema de gestión; según los encuestados después del desarrollo se produjo una disminución de 40,45%, por ello la planificación es un eje fundamental en un correcto funcionamiento de SGSI, además que mejorará en un 60% la eficiencia de los sistemas informáticos. Nuestros resultados tienen cierta similitud con los estudios realizados por Cueva & Ríos (2018) y los resultados está dentro de los márgenes de error del 3%, Ya que el proceso de planificación en ambos estudios va mejorando sus indicadores.

En el estudio de (Chuna, 2018) titulado: “Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - filial Piura” los resultados obtenidos de la

ejecución de la propuesta de un sistema ISO es que mejoró el conocimiento de las políticas por parte de los usuarios y administradores ya que con ello se reduce notablemente posibles riesgos en la información, después de la implementación de las capacitaciones en políticas de seguridad el 78% de los administrados manifiesta que reducirá notablemente los problemas y además 80% tiene aceptación de estas normas para aplicar las políticas de seguridad de la información en la entidad. En comparación con nuestros resultados obtenidos en nuestra investigación la aceptación de las normas ISO obtienen un 52,60% en la antes del desarrollo y aumentando un 64% después del desarrollo, además que un 88,60% de los encuestados manifiesta tener aceptación de la seguridad de la información, después del desarrollo del SGSI bajo norma ISO 27001:2014 además que con el desarrollo de un sistema de gestión de seguridad reducirá en un 80% los posibles riesgos. Estos resultados tienen mucha similitud con el estudio Chuna (2018), ya que en ambos estudios la aceptación de las normas ISO con medida que se implementan van aumentando su aceptación debido a la seguridad en la que estará protegida nuestra información.

En el estudio de [Flores, 2019] titulado: “Sistema de gestión de seguridad de la información de acuerdo con la ISO 27001:2014 para el área de historias clínicas del Centro de Salud Puente Chao en el año 2018” los resultados obtenidos en esta investigación fueron que un 85% de los administrados dicen que las amenazas serán controladas antes que realicen algún daño a la organización con la implementación del sistema de gestión bajo las normas ISO 27001, que después de la implementación un 90% de los administrados nos dice que el SGSI está cumpliendo su función de controlar posibles amenazas. En comparación con nuestros resultados obtenidos en nuestra investigación nos dicen que hay un 47.15% antes del desarrollo que dice que las amenazas tiene que ser controladas antes de producir algún tipo de daño a la empresa, después en la después del desarrollo el 59.1% nos dice que se está produciendo un control eficiente de las amenazas, además en otro resultado un 88.05%

nos dice que se cumplió la función de seguridad de la información, podemos observar que el SGSI ayuda a mejorar el control de la información aplicando la norma ISO 27001:2014 y reduciendo los riesgos asociados con la protección de la información corporativa. Podemos concluir que en ambos estudios el control en la norma ISO es fundamental ya que se produce un mayor control en la información, en su flujo y sobre todo en proteger la información de agentes extraños.

En el estudio de (Chalco, y otros, 2019) titulado “Sistema de gestión de seguridad de la información basado en la Norma NTP ISO/IEC 27001:2014 en el Control de Monitoreo de la RENIEC, 2019 “ los resultados obtenidos de la implementación de la norma ISO 27001 es que mejorara todos los aspectos en seguridad e la información, lo que quiere decir que se podrá realizar operaciones en forma segura, rápida y confidencialmente. Para ello realizó Pre y post en las que dio como resultado que 42.3% estaba en contra de la norma ISO 27001 en la pre implementación, después en la post encuesta esta desaprobación se redujo a un 10.5%. En comparación con nuestros resultados obtenidos en nuestra investigación la implementación de normas ISO obtienen un 52,60% antes del desarrollo aumentando un 11,40% después del desarrollo produciendo una reducción del 41,20%, en esta medida significa que el 88,60% de los encuestados muestra aceptación por la seguridad de la información después de la implementación de seguridad de la información bajo norma ISO 27001:2014. Nuestros resultados tienen cierta similitud con los estudios realizados por Chalco & Ramírez (2019) ya que en ambos estudios se concuerda que la gestión de la información va ir aumentando en medida que se vaya implementado y que los usuarios sepan las ventajas de cumplir con el apartado de operaciones de la norma ISO 27001:2014.

VI. CONCLUSIONES

Se puede concluir de la investigación lo siguiente:

- Se concluye que al aproximar la normal (Z), se obtiene un valor $(-3,922) < \alpha$ (0,05) utilizado en el nivel de significación por lo que se puede decir que la hipótesis alterna es la hipótesis específica 1 es aceptada.
- Se concluye que para la contratación de la hipótesis de investigación 2, se utilizó la prueba t de Student, asumiendo que la información se distribuye normalmente. Las medias antes y después del procedimiento son significativamente diferentes debido al valor de $t (17.588) < \alpha$ (0,05) por lo que mi hipótesis alterna es aceptada
- Se concluye que al aproximar la normal (Z), se obtiene un valor $(-3,921) < \alpha$ (0,05) utilizado en el nivel de significación. por lo que se puede decir que la hipótesis alterna es la hipótesis específica 3 es aceptada.

VII. RECOMENDACIONES

Se puede realizar las siguientes recomendaciones:

- Se recomienda que para próximos estudios también habrá que ampliar la muestra de clientes y empresas que brindan servicios al Hotel, para observar desde otro ángulo y dar su punto de vista sobre las debilidades, fortalezas y amenazas que pueda tener el sistema.
- Se recomienda realizar otros estudios más exhaustivos para hallar otros problemas que pueden ocurrió después de la implementación del sistema.
- Se recomienda realizar auditorías internas y externas para verificar el buen funcionamiento del sistema y de ser caso presentar alternativas de solución.

REFERENCIAS

Alberto, A. 2018. *Diseño de un Sistema de Gestion de la Seguridad de la información.* Colombia : AlfaOmega, 2018.

Andress, J. 2018. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.* USA : Elsevier, 2018.

Arellano, C. 2020. *El derecho de protección de datos personales.* 2020. págs. 163-174.

Atencio, E. 2019. *Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú.* Pasco : Universidad Nacional Daniel Alcides Carrión, 2019. Disponible: <http://repositorio.undac.edu.pe/handle/undac/1474>.

Carrasco, D. 2018. *Metodología de la investigación científica. Pautas metodológicas para diseñar y elaborar el proyecto de investigación.* Lima : San Marcos E.I.R.L, 2018.

Castro, P. 2020. *Diseño de un sistema de gestión de seguridad de la información para la Corte Superior de Justicia de Piura, mediante la normativa ISO/IEC 27001.* Piura : Universidad Cesar Vallejo, 2020. Disponible: <https://repositorio.ucv.edu.pe/handle/20.500.12692/59572>.

Caycho, C, Castillo, C y Merino, V. 2019. *Manual de estadística no paramétrica aplicada a los negocios.* Lima : Alianza editorial, 2019.

Chalco, F y Ramirez, J. 2019. *Sistema de gestión de seguridad de la información basado en la Norma NTP ISO/IEC 27001:2014 en el Control de Monitoreo de la RENIEC, 2019.* Lima : Universidad Tecnológica del Perú, 2019. Disponible: <https://repositorio.utp.edu.pe/handle/20.500.12867/2162>.

Chaux, J, Polania, H y Moreno, L. 2020. *Sistema inteligente de entrega de productos mediante la integración de visión artificial, robótica móvil y un sistema de manufactura flexible (FMS).* 2020. Disponible: <https://doi.org/10.23850/25004476.2927>.

Chuna, G. 2018. *Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - filial Piura.* Piura : Universidad Cesar Vallejo, 2018. Disponible: <https://repositorio.ucv.edu.pe/handle/20.500.12692/53852>.

Cirstoiu, A. 2021. *Sistema web y aplicación móvil para la reservación de habitaciones en empresa de ámbito hotelero.* Ecuador : Universidad Estatal Península de Santa Elena, 2021. Disponible: <https://repositorio.upse.edu.ec/handle/46000/6483>.

Condori, P. 2020. *Universo, población y muestra.* España : Curso Taller, 2020.

Contreras, L. 2018. *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA DIRECCION DE SISTEMAS DE LA GOBERNACIÓN DE BOYACÁ.* Colombia : Universidad Nacional Abierta y a distancia, 2018. disponible:<https://repository.unad.edu.co/bitstream/handle/10596/11895/33367604.pdf>.

Cueva, P y Rios, J. 2018. *Gestión de la historia clínica y la seguridad de la información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014.* Lima : Universidad Privada del Norte, 2018. disponible: <https://repositorio.upn.edu.pe/handle/11537/13676>.

Escalante, D. 2019. *Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la ntp iso/iec 27001 para la Dirección de Salud Virgen de Cocharcas – Chincheros.* Lima : Universidad Nacional José Maria Arguedas, 2019. disponible: <https://repositorio.unajma.edu.pe/handle/123456789/504>.

Ferrer, M. 2021. *Exportación de servicios y el saldo a favor del exportador en una empresa del sector hotelero Arequipa 2020.* Lima : Universidad Cesar Vallejo, 2021. disponible: <https://repositorio.ucv.edu.pe/handle/20.500.12692/78998>.

Flores, J. 2019. *Sistema de gestión de seguridad de la información de acuerdo con la ISO 27001:2014 para el área de historias clínicas del Centro de Salud Puente*

Chao en el año 2018. Lambayeque : Universidad Privada Antenor Orrego, 2019. disponible: <http://repositorio.upao.edu.pe/handle/20.500.12759/4869>.

Franco, D. C., Porras, H. O., Corredor, F. A y Calderón, C. 2019. *SANI: Assistant for Information Security Auditing on ISO/IEC 27001*. 2019. págs. 324-333.

Freire, C y Maveda, J. 2019. *Desarrollo de un sistema web y aplicacion movil para la gestion de reservas, control de hospedaje y comandas caso a aplicar en el Hotel Alsafi "El Paraiso"*. Ecuador : ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, 2019. disponible: <http://dspace.esPOCH.edu.ec/handle/123456789/12195>.

Gobierno Electrónico e Informática. 2019. *Boletín Informativo de la Oficina Nacional de Gobierno Electrónico e Informática*. Lima : ONGEI, 2019.

Gómez, L y Fernández, P. 2018. *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*. España : AENOR, 2018.

Guerra, E., Neira, H., Diaz, J y Patiño, J. 2021. *Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias*. Colombia : Información tecnológica, 2021. disponible: <http://dx.doi.org/10.4067/S0718-07642021000500145>.

Guillen, R. 2018. *Sistemas de información en la gestión, de los hoteles de 3 estrellas, de la ciudad de Abancay, Período 2016*. Moquegua : Universidad José Carlos Mariategui, 2018. disponible: <http://repositorio.ujcm.edu.pe/handle/20.500.12819/430>.

Hernández, R y Mendoza, C. 2018. *Metodología de la investigación*. México : MC Graw Hill, 2018.

Huacasi, J. 2018. *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NTP ISO/IEC 27001 PARA MEJORAR EL PROCESO DE SEGURIDAD DE INFORMACIÓN EN EL EJÉRCITO DEL PERÚ*. Lima : Universidad Privada Telesup, 2018. disponible: <https://repositorio.utelesup.edu.pe/handle/UTELESUP/781>.

Jara, O. 2018. *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018.* Lima : Universidad César Vallejo, 2018. disponible: <https://repositorio.ucv.edu.pe/handle/20.500.12692/31209>.

Meriah, I y Arfa, . 2019. *Comparative study of ontologies based iso 27000 series security standards.* 2019. págs. 52-92.

Molano, R. 2018. *Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa Market Mix.* Colombia : Universidad Católica de Colombia, 2018. disponible: <https://repository.ucatolica.edu.co/handle/10983/15240>.

Moreno, R y Otarola, A. 2020. *Diseño de un sistema de gestión de seguridad de la información para la empresa Sociedad Hotelera San Pablo basado en la norma ISO/IEC 27001:2013.* Colombia : Universidad Piloto de Colombia, 2020. disponible: <http://repository.unipiloto.edu.co/handle/20.500.12277/7436>.

Ortiz, E. 2018. *Controles de seguridad según la norma ISO/IEC 27002:2013 para el mejoramiento de la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva.* Tingo Maria : Universidad Nacional Agraria de la Selva, 2018. disponible: <http://repositorio.unas.edu.pe/handle/UNAS/1710>.

Pizarro, I. 2018. *Diseño de un modelo de gestión de seguridad de la información con un enfoque en el factor humano para el ICPNA Región Centro en el año 2017.* Huancayo : Universidad Continental, 2018. disponible: <https://repositorio.continental.edu.pe/handle/20.500.12394/4902>.

Proenca, D y Borbinha, J. 2018. *Information security management systems-a maturity model based on ISO/IEC 27001. In International Conference on Business Information Systems.* 2018. págs. 102-111.

Risco, E. 2021. *Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín, 2021.* Lima : Universidad Cesar Vallejo, 2021. disponible: <https://repositorio.ucv.edu.pe/handle/20.500.12692/63424>.

- Sanchez, N, Comas, R y Garcia, M. 2019.** *Sistema Inteligente de Información Geográfica para las empresas eléctricas cubanas.* 2019. disponible: https://scielo.conicyt.cl/scielo.php?pid=S0718-33052019000200197&script=sci_arttext&tIng=p.
- Sikora, M. 2020.** *Plan de gestión de información interna y externa para la Empresa Hotel.* Argentina : Universidad Siglo 21, 2020. disponible: <https://repositorio.uesiglo21.edu.ar/handle/ues21/21874>.
- Solano, G. 2021.** *Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica.* Costa Rica : Universidad Latina de Costa Rica, 2021. disponible: <https://repositorio.ulatina.ac.cr/handle/20.500.12411/293?locale=es>.
- Tonyse, M. 2021.** *Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001.* Ecuador : Revista Universidad y Sociedad, 2021. disponible: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495.
- Torres, C. 2020.** *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.* Ecuador : Universidad Técnica de Ambato, 2020. disponible: <https://repositorio.uta.edu.ec/handle/123456789/30690>.
- Torres, D. 2019.** *Gestión para resultados al alcance de todos.* Venezuela : Crcatcspace, 2019.
- Torres, I. 2019.** *El Sistema de Gestión y sus componentes: estratégico, táctico y operacional.* Venezuela : Revistas Uclave, 2019.
- Vargas, E y Marchan, A. 2019.** *Propuesta de diseño de un Sistema de Gestión de la Seguridad de la Información según la NTP ISO/IEC 27001:2014 para la Universidad del Pacífico.* Lima : Universidad Tecnológica del Perú, 2019. disponible: <https://repositorio.utp.edu.pe/handle/20.500.12867/2786>.
- Xiaoyan, M. 2020.** *Diseño de un sistema de gestión de la seguridad de la información en una empresa de recursos humanos.* España : Universidad de Alcalá, 2020. disponible; <https://ebuah.uah.es/xmlui/handle/10017/44660>.

Zacarias, J. 2018. *Modelo de seguridad de la información basado en la ISO/IEC 27001:2013 para mitigar los riesgos de los activos de información en la Central de Operaciones Policiales de la Región Policial Junín.* Huancayo : Universidad Continental, 2018. disponible:
<https://repositorio.continental.edu.pe/handle/20.500.12394/4105>.

ANEXOS

Anexo 1: Declaratoria de Originalidad de Autores

Nosotros Cabrera Chumbe Renato Samuel y Rojas Rett Gilmer Armando egresados de la Facultad de Ingeniería y Arquitectura y Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo Campus Lima Norte, declaramos bajo juramento que todos los datos e información que acompañan a nuestra Tesis titulada:



“DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD”,

es de nuestra autoría, por lo tanto, declaramos que el Trabajo de Investigación / Tesis:

1. No ha sido plagiado ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicado ni presentado anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumimos 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, 11 de mayo del 2022

DNI: 71528969	Firma: 
ORCID: 0000-0002-0009-8058	
Apellidos y Nombres del Autor	Renato Samuel Cabrera Chumbe
DNI: 75792113	Firma: 
ORCID: 0000-0002-1672-8026	
Apellidos y Nombres del Autor	Gilmer Armando Rojas Rett

Anexo 2: Declaratoria de Autenticidad del Asesor

Yo, Milner David Liendo Arevalo, docente de la Facultad de Ingeniería y Arquitectura, y Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo Campus Lima Norte, asesor (a) del Trabajo de Investigación / Tesis titulada:


“DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD”

de los autores Renato Samuel Cabrera Chumbe y Gilmer Armando Rojas Rett, constato que la investigación tiene un índice de similitud de 20% 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 el trabajo de investigación / 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, día de mes de 2022

DNI 00792777	Firma 
ORCID 0000-0002-7665-361X	

Anexo 3: Autorización de Publicación en Repositorio Institucional

Nosotros, Cabrera Chumbe Renato Samuel y Rojas Rett Gilmer Armando identificados con DNI N° 71528969 – 75792113, egresados de la Facultad de Ingeniería y Arquitectura y Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo, autorizamos (X), no autorizamos () la divulgación y comunicación pública de nuestra Tesis:



“DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD”.

En el Repositorio Institucional de la Universidad César Vallejo (<http://repositorio.ucv.edu.pe/>), según lo estipulada en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33.

Fundamentación en caso de NO autorización:

.....
.....

Lima, 11 de mayo del 2022

DNI: 71528969	Firma : 
ORCID: 0000-0002-0009-8058	
Apellidos y Nombres del Autor:	Renato Samuel Cabrera Chumbe
DNI: 75792113	Firma : 
ORCID: 0000-0002-1672-8026	
Apellidos y Nombres del Autor:	Gilmer Armando Rojas Rett

Anexo 4: Matriz de consistencia

Tabla 14: Matriz de consistencia

Problemas	Objetivos	Hipótesis	Variables, dimensiones e indicadores	Metodología
<p>Problema General ¿De qué manera influye el desarrollo de un sistema hotelero para gestionar la información de los clientes basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad</p>	<p>Objetivo General Determinar de qué manera influye el desarrollo de un sistema hotelero para gestionar la información de los clientes, basado en el apartado de operación de la Norma ISO 27001:2014, para la empresa El puerto Hotel La libertad</p>	<p>Hipótesis General El desarrollo de un sistema hotelero mejorara la gestión de la información de los clientes basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad</p>	<p>X: Variable independiente</p> <p>Desarrollo de un sistema hotelero</p> <p>Dimensiones</p> <p>X1 Registrar</p> <p>X1.1. Control</p> <p>X.1.2. Verificación</p> <p>X.1.3. Validación</p> <p>X.2. Solicitudes del cliente</p> <p>X.2.1. servicios</p> <p>X.2.2. Reservación</p> <p>Y: Variable dependiente</p> <p>Gestión de seguridad de la información. Apartado de operación de la norma ISO 27001:2014</p>	<p>POBLACIÓN 70 trabajadores del puerto Hotel La libertad</p> <p>MUESTRA 50 trabajadores del puerto Hotel La libertad</p> <p>MUESTREO 50 trabajadores del puerto Hotel La libertad</p> <p>ENFOQUE Cuantitativo</p> <p>TIPO DE INVESTIGACIÓN Aplicada</p> <p>NIVEL DE INVESTIGACIÓN Deductivo</p> <p>DISEÑO DE INVESTIGACIÓN Pre-experimental</p> <p>TÉCNICAS Ficha de registro</p> <p>INSTRUMENTOS SPSS V 26</p>
<p>Problema Específicos</p>	<p>Objetivo Específicos</p>	<p>Hipótesis Específicos</p>		
<p>PE1: ¿Cómo influye el desarrollo de un sistema hotelero en la planificación basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad?</p> <p>PE2: ¿Cómo influye el desarrollo de un sistema hotelero en la implementación de políticas basado en el apartado de operación de la norma ISO 27001:2014,</p>	<p>OE1: Determinar cómo influye el desarrollo de un sistema hotelero en la planificación basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad</p> <p>OE2: Determinar cómo influye el desarrollo de un sistema hotelero en la implementación de políticas basado en el apartado de operación de la norma ISO 27001:2014,</p>	<p>HE1: El desarrollo de un sistema hotelero mejorará la planificación que está basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad</p> <p>HE2: El desarrollo de un sistema hotelero mejorará la implementación de políticas basado en el apartado de operación de la</p>		

<p>para la empresa El puerto Hotel La libertad?</p> <p>PE3: ¿Cómo influye el desarrollo de un sistema hotelero en controlar o elimina las amenazas, basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad?</p>	<p>para la empresa El puerto Hotel La libertad</p> <p>OE3: Determinar Cómo influye el desarrollo de un sistema hotelero en controlar o eliminar las amenazas, basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad</p>	<p>norma ISO 27001:2014, para la empresa El puerto Hotel La libertad</p> <p>HE3: El desarrollo de un sistema hotelero mejorara control o eliminación de las amenazas, basado en el apartado de operación de la norma ISO 27001:2014, para la empresa El puerto Hotel La libertad</p>	<p>Dimensiones</p> <p>Y.1. Planificación</p> <p>Y.1.1. Eliminar manipular datos</p> <p>Y.1.2. accesos no autorizados</p> <p>Y.1.3. Vulneraciones de los programas</p> <p>Y.2. Implementación</p> <p>Y.2.1. Controles</p> <p>Y.2.2. Políticas</p> <p>Y.3. Controlar</p> <p>Y.3.1. Reducción o eliminación de amenazas</p>	
---	--	--	--	--

Anexo 5: Matriz de operacionalización de variables

Tabla 15: Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
VARIABLE INDEPENDIENTE Desarrollo de un sistema hotelero	Según Chaux, Polania, & Moreno (2020) son aquellas tecnologías que se necesita para el sistema operativo realice su función de manera correcta, estas se ubican en un servidor en la nube o físicamente en un equipo.	Según Chaux, Polania, & Moreno (2020) para el sistema sus dimensiones son según los requerimientos del cliente y del administrador por lo que sus dimensiones son: registrar y solicitudes del cliente	Registrar	<ul style="list-style-type: none"> • Control • Verificación • Validación 	Razón
			Solicitudes del cliente	<ul style="list-style-type: none"> • Servicios • Reservación 	Razón
VARIABLE DEPENDIENTE Gestión de seguridad de la información. Apartado de operación de la norma ISO 27001:2014	Según Proenca & Borbinha (2018) las decisiones estratégicas de la organización para mantener la confidencialidad, disponibilidad e integridad de la información mediante la aplicación de procesos de gestión de riesgos. Apartado de la norma ISO, que contribuye en establecer un control sobre los	Según Proenca & Borbinha (2018) según las normas ISO sus dimensiones son: Planificación, implementación y control.	Planificación	<ul style="list-style-type: none"> • Eliminar, manipular, borrar datos • Accesos no autorizados • Vulneraciones de los programas 	Nominal
			Implementación	<ul style="list-style-type: none"> • Controles • Políticas 	Nominal
			Control	<ul style="list-style-type: none"> • Reducción o eliminación de amenazas 	Nominal

	procesos de registro de la información.				
--	---	--	--	--	--

Anexo 6: Cuestionario

Para identificar amenazas y establecer probabilidad de ocurrencia - marca con un aspa (x) según la escala de Likert:

Valor	Puntuación
Prácticamente imposible	1
Poco probable	2
Posible	3
Probable	4
Muy probable	5

AMENAZAS	PROBABILIDAD DE OCURRENCIA				
	1	2	3	4	5
Fuego					
Tormenta eléctrica, rayo					
Error de usuario					
Errores del administrador					
Alteración accidental de la información					
Destrucción de la información					
Fugas de la información					
Vulnerabilidades de los programas (software)					
Errores de mantenimiento /actualización de programas					
Errores de mantenimiento / actualización de equipos					
Indisponibilidad del personal por salud					
Manipulación de los registros de actividad					
Suplantación de la identidad del usuario					
Abuso de privilegios de acceso					
Difusión de software dañino					
Acceso no autorizado					
Modificación deliberada de información					
Inestabilidad de la línea de internet					
Manipulación de programas					
Manipulación de equipos					
Robo de equipos					
Corte del suministro eléctrico					
Condiciones inadecuadas de temperatura o humedad					
Degradación de los soportes de almacenamiento de la información					
Instalación de software no autorizado					

Anexo 7: Fichas de registro Pre-test

Investigador						
Empresa						
Dirección						
Fecha de inicio	02/01/2022					
Fecha de terminación	21/01/2022					
Variable	Formula					
Reportes	$ANA = \frac{RANA}{TAD} \times 100$ <p>Donde: ANA: Accesos No Autorizados TAD: Total de Accesos del Día RANA: Reporte de Accesos No Autorizados</p>					
Indicador					Medida	
Accesos no autorizados (PRE-TEST)					Porcentaje	
ITEM	FECHA	RANA	TAD	ANA %		
1	02/01/2022	13	20	65		
2	03/01/2022	10	18	56		
3	04/01/2022	15	20	75		
4	05/01/2022	10	19	53		
5	06/01/2022	13	18	72		
6	07/01/2022	15	17	88		
7	08/01/2022	10	20	50		
8	09/01/2022	11	18	61		
9	10/01/2022	15	19	79		
10	11/01/2022	13	20	65		
11	12/01/2022	10	17	59		
12	13/01/2022	16	18	89		
13	14/01/2022	13	19	68		
14	15/01/2022	10	20	50		
15	16/01/2022	15	22	68		
16	17/01/2022	10	17	59		
17	18/01/2022	10	18	56		
18	19/01/2022	15	17	88		
19	20/01/2022	13	17	76		
20	21/01/2022	16	17	94		
	TOTAL	253	371			
	PROMEDIO			68		

Anexo 8: Fichas de registro Re-test

Investigador					
Empresa					
Dirección					
Fecha de inicio	01/02/2022				
Fecha de terminación	20/02/2022				
Variable	Formula				
Reportes	$ANA = \frac{RANA}{TAD} \times 100$ <p>Donde: ANA: Accesos No Autorizados TAD: Total de Accesos del Día RANA: Reporte de Accesos No Autorizados</p>				
Indicador					Medida
Accesos no autorizados (RE-TEST)					Porcentaje
ITEM	FECHA	RANA	TAD	ANA %	
1	01/02/2022	15	20	75	
2	02/02/2022	14	18	78	
3	03/02/2022	13	20	65	
4	04/02/2022	14	19	74	
5	05/02/2022	10	18	56	
6	06/02/2022	15	17	88	
7	07/02/2022	14	20	70	
8	08/02/2022	10	17	59	
9	09/02/2022	15	18	83	
10	10/02/2022	14	19	74	
11	11/02/2022	10	20	50	
12	12/02/2022	15	19	79	
13	13/02/2022	14	18	78	
14	14/02/2022	10	17	59	
15	15/02/2022	14	20	70	
16	16/02/2022	13	18	72	
17	17/02/2022	10	18	56	
18	18/02/2022	10	19	53	
19	19/02/2022	14	17	82	
20	20/02/2022	13	17	77	
	TOTAL	257	369		
	PROMEDIO			70	

Anexo 9: Fichas de registro Post-test

Investigador							
Empresa							
Dirección							
Fecha de inicio	01/03/2022						
Fecha de terminación	20/03/2022						
Variable	Formula						
Reportes	$ANA = \frac{RANA}{TAD} \times 100$ <p>Donde: ANA: Accesos No Autorizados TAD: Total de Accesos del Día RANA: Reporte de Accesos No Autorizados</p>						
Indicador					Medida		
Accesos no autorizados (POST-TEST)					Porcentaje		
ITEM	FECHA	RANA	TAD	ANA %			
1	01/03/2022	2	15	13			
2	02/03/2022	3	14	21			
3	03/03/2022	1	10	10			
4	04/03/2022	0	10	0			
5	05/03/2022	2	10	20			
6	06/03/2022	3	14	21			
7	07/03/2022	4	15	27			
8	08/03/2022	2	12	17			
9	09/03/2022	1	11	9			
10	10/03/2022	1	10	10			
11	11/03/2022	3	15	20			
12	12/03/2022	0	14	0			
13	13/03/2022	0	13	0			
14	14/03/2022	1	10	10			
15	15/03/2022	3	11	27			
16	16/03/2022	2	10	20			
17	17/03/2022	1	10	10			
18	18/03/2022	1	10	10			
19	19/03/2022	3	14	21			
20	20/03/2022	2	14	14			
	TOTAL	35	247				
	PROMEDIO			14			

Anexo 10: Fichas de registro Pre-test

Investigador							
Empresa							
Dirección							
Fecha de inicio	02/01/2022						
Fecha de terminación	21/01/2022						
Variable	Formula						
Reportes	$EBMD = \frac{EMBDNR}{TMDD} \times 100$ <p>Donde: EBMD: Manipulación de Datos TMDD: Total de Manipulación de datos del día EMBDNR: Eliminar, Manipular, Borrar Datos No reconocidos</p>						
Indicador					Medida		
Eliminar, manipular, borrar, datos (PRE-TEST)					Porcentaje		
ITEM	FECHA	EMBDNR	TMDD	EBMD%			
1	02/01/2022	10	20	50			
2	03/01/2022	15	25	60			
3	04/01/2022	10	20	50			
4	05/01/2022	13	22	59			
5	06/01/2022	10	23	43			
6	07/01/2022	10	24	42			
7	08/01/2022	11	25	44			
8	09/01/2022	15	20	75			
9	10/01/2022	10	20	50			
10	11/01/2022	10	25	40			
11	12/01/2022	13	20	65			
12	13/01/2022	10	25	40			
13	14/01/2022	10	20	50			
14	15/01/2022	10	20	50			
15	16/01/2022	13	22	59			
16	17/01/2022	11	23	48			
17	18/01/2022	11	23	48			
18	19/01/2022	10	20	50			
19	20/01/2022	10	20	50			
20	21/01/2022	10	20	50			
	TOTAL	233	439				
	PROMEDIO			51			

Anexo 11: Fichas de registro Re-test

Investigador							
Empresa							
Dirección							
Fecha de inicio	01/02/2022						
Fecha de terminación	20/02/2022						
Variable	Formula						
Reportes	$EBMD = \frac{EMBDNR}{TMDD} \times 100$ <p>Donde: EBMD: Manipulación de Datos TMDD: Total de Manipulación de datos del día EMBDNR: Eliminar, Manipular, Borrar Datos No reconocidos</p>						
Indicador					Medida		
Eliminar, manipular, borrar, datos (RE-TEST)					Porcentaje		
ITEM	FECHA	EMBDNR	TMDD	EBMD%			
1	01/02/2022	15	22	68			
2	02/02/2022	10	23	43			
3	03/02/2022	14	24	58			
4	04/02/2022	10	22	45			
5	05/02/2022	10	20	50			
6	06/02/2022	10	25	40			
7	07/02/2022	14	20	70			
8	08/02/2022	15	24	63			
9	09/02/2022	10	20	50			
10	10/02/2022	10	22	45			
11	11/02/2022	10	23	43			
12	12/02/2022	14	24	58			
13	13/02/2022	10	20	50			
14	14/02/2022	10	22	45			
15	15/02/2022	15	27	56			
16	16/02/2022	14	25	56			
17	17/02/2022	10	20	50			
18	18/02/2022	14	26	54			
19	19/02/2022	10	22	45			
20	20/02/2022	15	24	63			
	TOTAL	240	455				
	PROMEDIO			53			

Anexo 12: Fichas de registro Post-test

Investigador				
Empresa				
Dirección				
Fecha de inicio		01/03/2022		
Fecha de terminación		20/03/2022		
Variable		Formula		
Reportes		$EBMD = \frac{EMBDNR}{TMDD} \times 100$		
Indicador		Medida		
Eliminar, manipular, borrar, datos (POST-TEST)		Porcentaje		
		Donde: EBMD: Manipulación de Datos TMDD: Total de Manipulación de datos del día EMBDNR: Eliminar, Manipular, Borrar Datos No reconocidos		
ITEM	FECHA	EMBDNR	TMDD	EBMD%
1	01/03/2022	3	22	14
2	02/03/2022	5	23	22
3	03/03/2022	4	24	17
4	04/03/2022	1	22	5
5	05/03/2022	0	20	0
6	06/03/2022	2	25	8
7	07/03/2022	4	20	20
8	08/03/2022	2	24	8
9	09/03/2022	3	20	15
10	10/03/2022	1	22	5
11	11/03/2022	5	23	22
12	12/03/2022	0	24	0
13	13/03/2022	2	20	10
14	14/03/2022	2	22	9
15	15/03/2022	3	27	11
16	16/03/2022	5	25	20
17	17/03/2022	3	20	15
18	18/03/2022	5	26	19
19	19/03/2022	0	22	0
20	20/03/2022	2	24	8
		TOTAL	52	455
		PROMEDIO		11

Anexo 13: Fichas de registro Pre-test

Investigador						
Empresa						
Dirección						
Fecha de inicio	01/01/2022					
Fecha de terminación	21/01/2022					
Variable	Formula					
Reportes	$CI = \frac{CINE}{CID} \times 100$ <p>Donde: CI: Control Informático CINE: Control Informático No Eliminado CID: Control Informático del día</p>					
Indicador					Medida	
Control informático (PRE-TEST)					Porcentaje	
ITEM	FECHA	CINE	CID	CI %		
1	02/01/2022	3	10	30		
2	03/01/2022	5	10	50		
3	04/01/2022	4	8	50		
4	05/01/2022	3	9	33		
5	06/01/2022	5	10	50		
6	07/01/2022	4	8	50		
7	08/01/2022	5	7	71		
8	09/01/2022	4	9	44		
9	10/01/2022	5	8	63		
10	11/01/2022	5	7	71		
11	12/01/2022	4	9	44		
12	13/01/2022	5	9	56		
13	14/01/2022	5	7	71		
14	15/01/2022	4	9	44		
15	16/01/2022	5	9	56		
16	17/01/2022	5	10	50		
17	18/01/2022	5	8	38		
18	19/01/2022	4	7	71		
19	20/01/2022	5	10	40		
20	21/01/2022	5	8	50		
	TOTAL	87	172			
	PROMEDIO			51		

Anexo 14: Fichas de registro Re-test

Investigador						
Empresa						
Dirección						
Fecha de inicio	01/02/2022					
Fecha de terminación	20/02/2022					
Variable	Formula					
Reportes	$CI = \frac{CINE}{CID} \times 100$ <p>Donde: CI: Control Informático CINE: Control Informático No Eliminado CID: Control Informático del día</p>					
Indicador					Medida	
Control informático (RE-TEST)					Porcentaje	
ITEM	FECHA	CINE	CID	CID %		
1	01/02/2022	6	8	75		
2	02/02/2022	4	10	40		
3	03/02/2022	6	9	67		
4	04/02/2022	5	10	50		
5	05/02/2022	4	10	40		
6	06/02/2022	3	9	33		
7	07/02/2022	4	10	40		
8	08/02/2022	4	10	40		
9	09/02/2022	5	8	63		
10	10/02/2022	4	10	40		
11	11/02/2022	4	9	44		
12	12/02/2022	4	10	40		
13	13/02/2022	4	10	40		
14	14/02/2022	3	8	38		
15	15/02/2022	6	10	60		
16	16/02/2022	4	9	44		
17	17/02/2022	3	10	30		
18	18/02/2022	5	8	63		
19	19/02/2022	4	10	40		
20	20/02/2022	5	9	56		
	TOTAL	87	187			
	PROMEDIO			47		

Anexo 15: Fichas de registro Post-test

Investigador						
Empresa						
Dirección						
Fecha de inicio	01/03/2022					
Fecha de terminación	20/03/2022					
Variable	Formula					
Reportes	$CI = \frac{CINE}{CID} \times 100$ <p>Donde: CI: Control Informático CINE: Control Informático No Eliminado CID: Control Informático del día</p>					
Indicador					Medida	
Control informático (POST-TEST)					Porcentaje	
ITEM	FECHA	CINE	CID	CI %		
1	01/03/2022	1	8	13		
2	02/03/2022	2	9	22		
3	03/03/2022	1	9	11		
4	04/03/2022	1	7	14		
5	05/03/2022	1	9	11		
6	06/03/2022	0	8	0		
7	07/03/2022	0	7	0		
8	08/03/2022	0	8	0		
9	09/03/2022	0	7	0		
10	10/03/2022	1	8	13		
11	11/03/2022	1	8	13		
12	12/03/2022	1	8	13		
13	13/03/2022	1	9	11		
14	14/03/2022	2	7	29		
15	15/03/2022	0	8	0		
16	16/03/2022	0	8	0		
17	17/03/2022	2	7	29		
18	18/03/2022	2	8	25		
19	19/03/2022	2	9	22		
20	20/03/2022	1	8	13		
	TOTAL	19	160			
	PROMEDIO			12		

Anexo 16: Metodología de Desarrollo XP

- Fase de Planificación

- Modelo de Negocio Actual

El hotel el Puerto – La Libertad. actualmente no cuenta con un sistema que le permita gestionar los clientes que llegan al establecimiento, mucho menos tiene políticas de seguridad para el manejo de esta información, por lo que tiene varias brechas de seguridad y no tiene un correcto manejo de la información de los clientes.

Tabla 16: Modelo de negocio actual

<p>EL PROBLEMA</p>	<p>CON RESPECTO AL PROCESO</p> <ul style="list-style-type: none">• Actualmente la empresa no cuenta con sistema de clientes que acuden al hotel, además de asignación de habitaciones y servicios a ellos y genera deficiencia en estos procesos:• Gestión de clientes <p>La empresa no tiene un sistema que guarde el registro de clientes que visitan el hotel, además de guardar su información, no existe políticas de seguridad para el manejo de esta información, lo cual genera que se pueda perder mucha información o que personas no adecuadas tengan acceso a esta información.</p> <ul style="list-style-type: none">• Asignación de habitaciones y servicios <p>El registro de habitaciones y servicios a los clientes se hace a través de cuadernos, lo que genera que se pueda perder información, no registro de visitas o servicios. Además, complica al acceso del historial de información, cruce de información para el área contable. Otro problema es que no hay control de</p>
-------------------------------	--

	quien registra la información, y los eventos que cada encargado hizo durante su turno.
AECTA	<ul style="list-style-type: none"> • Clientes. • Encargados de la atención. • Misma empresa.
EL IMPACTO	<ul style="list-style-type: none"> • Brechas grandes de seguridad para la información de los clientes que visitan el hotel. • Perdida de información por diferentes factores. • Control inadecuado de los registros de visitas y servicios. • Demora en la búsqueda de información histórica.
SOLUCIÓN EXITOSA	<ul style="list-style-type: none"> • Mejorar la gestión de clientes. • Implementación de políticas de seguridad. • Mejorar el registro de visitas y servicios de los clientes. • Disminuir el tiempo de ejecución en los procesos. • Disminuir riesgos respecto al manejo de la información.

- Requerimientos funcionales
 - Gestión de usuarios
 - Gestionar cuentas de usuario
 - Gestionar roles
 - Gestionar contraseña
 - Gestión de habitaciones
 - Registro y edición de habitaciones
 - Gestión de tipo de habitaciones
 - Gestión de precios de habitaciones
 - Gestión de clientes
 - Registro y edición de clientes.
 - Gestión de servicios

- Gestión de tipo de servicios
 - Registro y edición de servicios
 - Gestión de precios de servicios
- Gestión de reservas
 - Gestión de habitaciones reservadas
 - Gestión de mantenimiento de habitaciones
- Gestión de pagos
 - Tipo de pago
- Gestión de reportes
 - Reporte de visitas
 - Reporte de ingresos
 - Reporte de inicios de sesión
 - Reporte de actividad
- Requerimientos no funcionales
 - Seguridad de contraseñas encriptas
 - Seguridad de complejidad de contraseñas
 - URL protegidas
 - Generación de token para procesos en la página
 - Usabilidad
 - Performance
- Reglas de negocio

Esta aplicación web consiste en un sistema que permite que las personas que trabajan en el hotel El Puerto de la Libertad puedan gestionar las visitas al establecimiento e información de los clientes bajo parámetros de seguridad.

Existen 3 tipos de usuario en la plataforma, el primero es el administrador que tiene acceso a toda la web y módulos de esta, luego está el supervisor, que tiene permisos para gestionar la creación de habitaciones y servicios, además de ver el reporte de ingresos y visitas. En tercer lugar, está el recepcionista que se encarga de la reserva de habitaciones y registro de clientes principalmente.

El entrar al sistema el usuario debe autenticarse con su nombre de usuario y contraseña, según su rol asignado, se mostrarán las opciones que le corresponda.

Al ingresar, para todos los usuarios van a tener de primera portada el dashboard principal de reserva de habitaciones. Esto debe estar organizado por pisos y se debe diferenciar entre las habitaciones disponibles, ocupadas o en mantenimiento, además de tener filtros para distinguirlas. Este módulo principal será utilizado principalmente por los recepcionistas, quienes se encargarán de registrar a los clientes al llegar al hotel, además del tiempo de estancia y el tipo de habitación que elijan.

Existirá un módulo de clientes, en donde se podrán registrar a los clientes en base a sus datos personales, pero este formulario también estará disponible al momento de registrar la reserva, para registrar un cliente u obtener información de algún cliente registrado previamente, además de poder registrar acompañantes.

Debe haber un módulo para los tipos de habitaciones, y también establecer las tarifas que maneja cada tipo.

Para los servicios habrá un módulo para registrar los tipos de servicios, los servicios disponibles y sus precios.

Todo esto servirá para que en el dashboard principal se pueda reservar las habitaciones con los precios establecidos y agregar los servicios que requiera el cliente. Finalmente se tendrá el módulo de pagos, con boleta o factura y con el tipo de pago que cancele el cliente, al finalizar la visita del cliente, quedará en estado de mantenimiento hasta que se termine la limpieza de la habitación. Para los usuarios existirá un módulo para crear, editarlos o eliminar, además de seleccionar su rol. Además, debe haber 4 reportes, de visitas, ingresos, inicios de sesión y actividad en la página.

- Priorización de requerimientos funcionales

Tabla 17: Priorización de requerimiento funcionales

N	Requerimiento	Prioridad
1	RF1. Inicio de sesión	Alta
2	RF2. Administración de cuentas de usuario	Alta
3	RF3. Asignación de permisos	Alta
4	RF4. Administración de habitaciones	Media
5	RF5. Administración de tipo de habitación	Media
6	RF6. Administración de clientes	Alta

7	RF7. Administración de servicios	Media
8	RF8. Administración de tipo de servicios	Media
9	RF9. Módulo de reservas	Alta
10	RF10. Registro de reserva	Media
11	RF11. Módulo de pagos	Media
12	RF12. Reporte de visitas	Media
13	RF13. Reporte de ingresos por fecha	Media
14	RF14. Reporte de inicio de sesión	Alta
15	RF15. Reporte de actividad en la web	Alta

○ Identificación de los actores

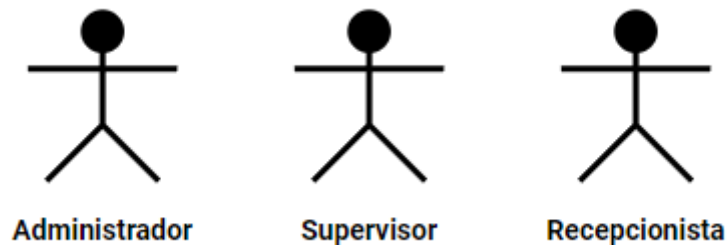


Figura 27: Actores

Tabla 18: Actores del negocio

Administrador	Se encarga de administrar usuarios para acceder al sistema y tener acceso a todos los módulos del sistema.
Supervisor	Se encarga de la gestión de las habitaciones y servicios, precios y tipos, además de poder ver el reporte de ingresos y visitas.
Recepcionista	Es el encargado de hacer las reservas de habitaciones al llegar los clientes, además de registrar la información de los clientes y tener reportes de visitas.

○ Diagramas de caso de uso del negocio

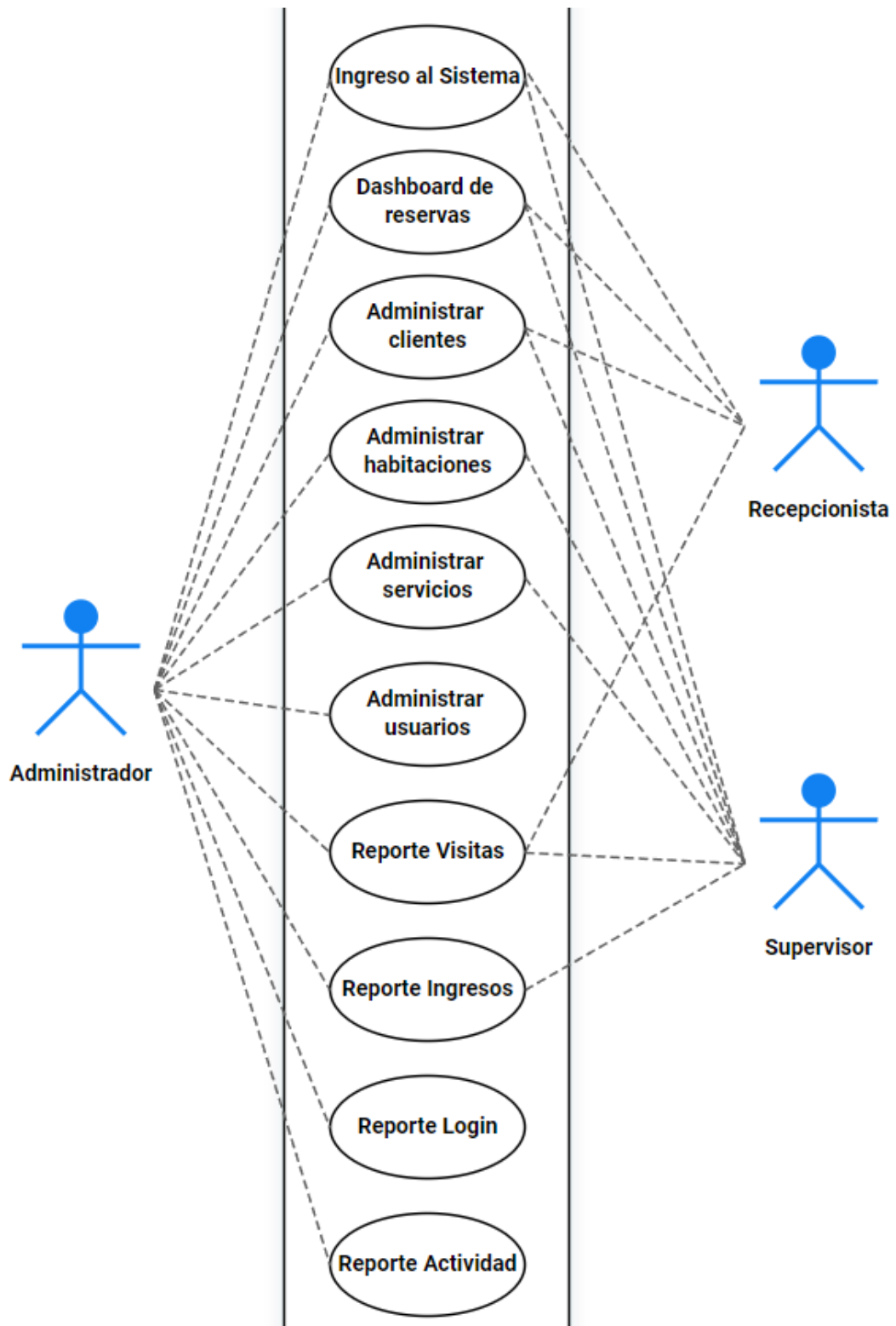


Figura 28: Diagrama de caso de uso del negocio

- Modelo del negocio
 - Escenarios
 - Escenario: Gestionar Usuario

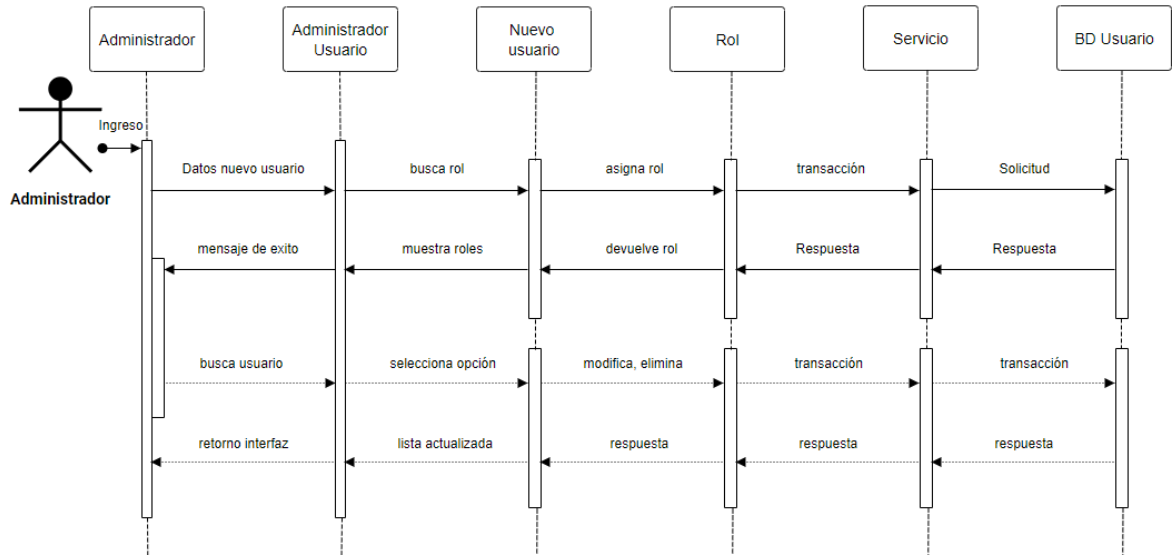


Figura 29: Gestionar usuario

- Escenario: Gestionar Cliente

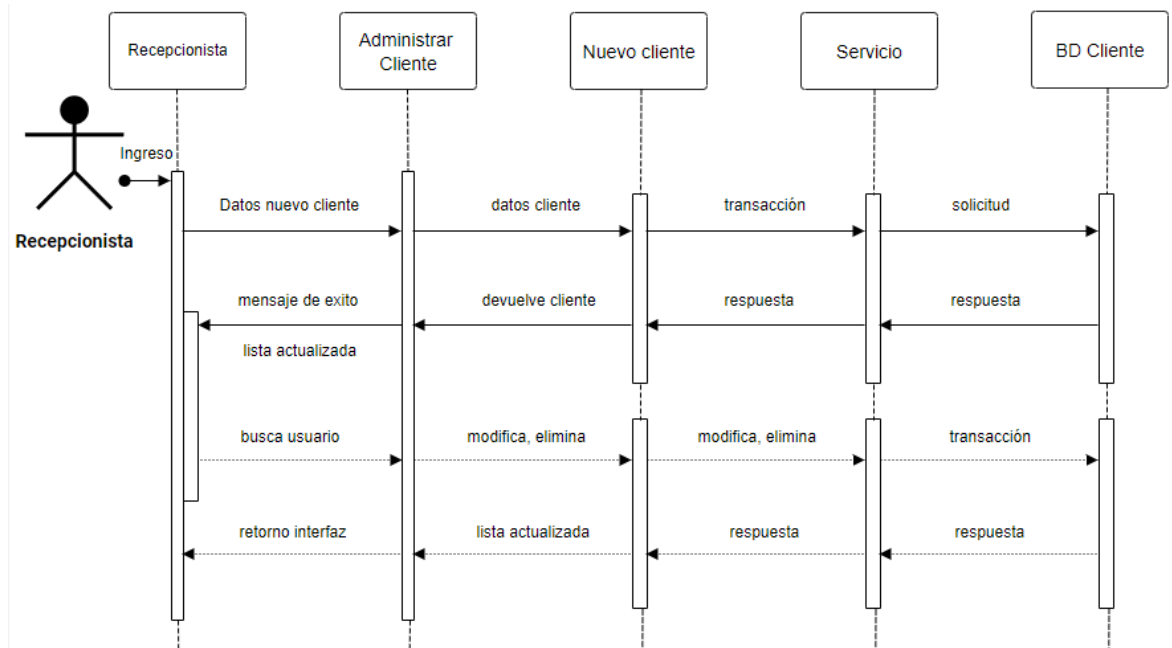


Figura 30: Gestionar Cliente

○ Diagramas de caso de uso del requerimiento (Sistema)

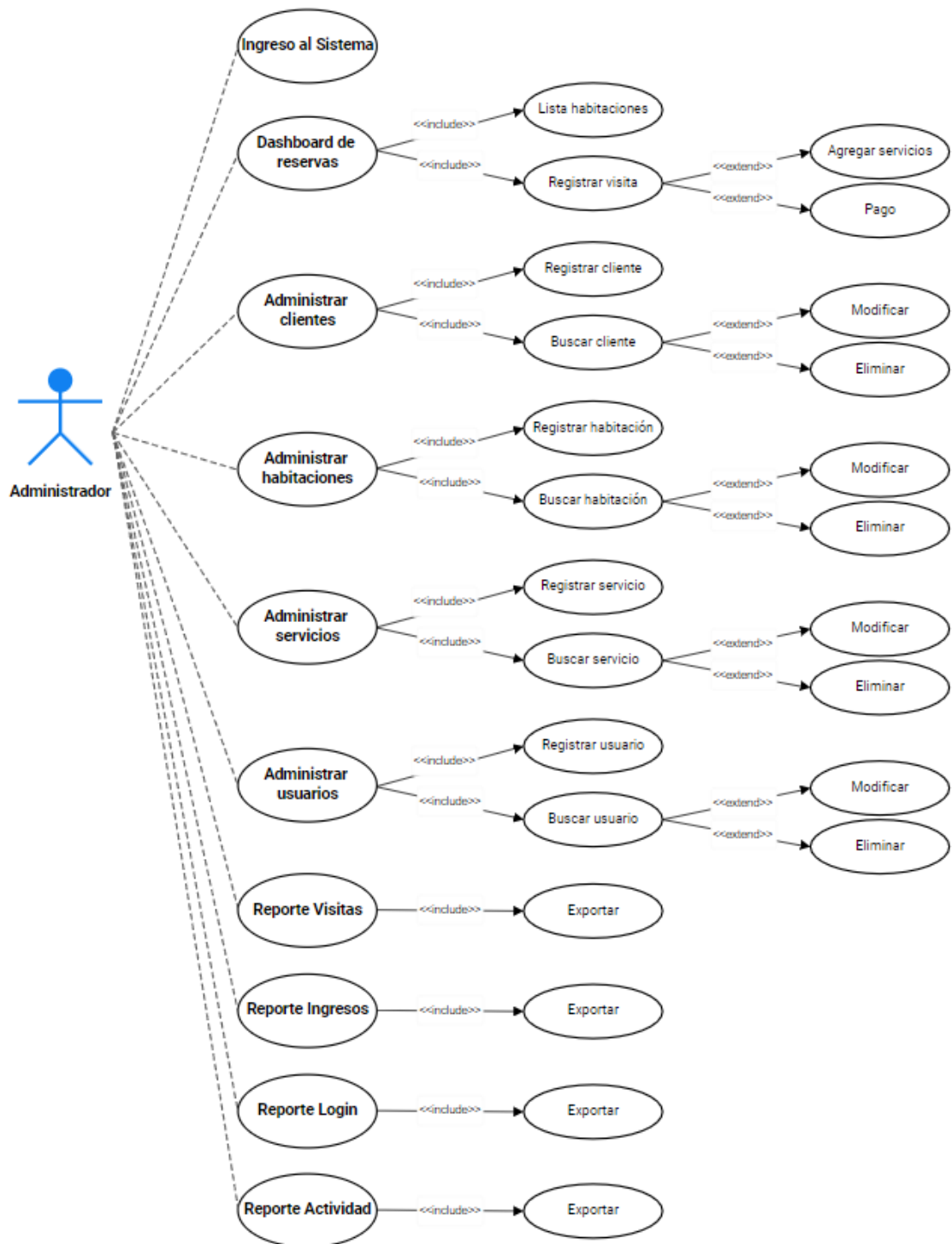


Figura 31: Diagrama de caso de uso del requerimiento Gestión del Administrador

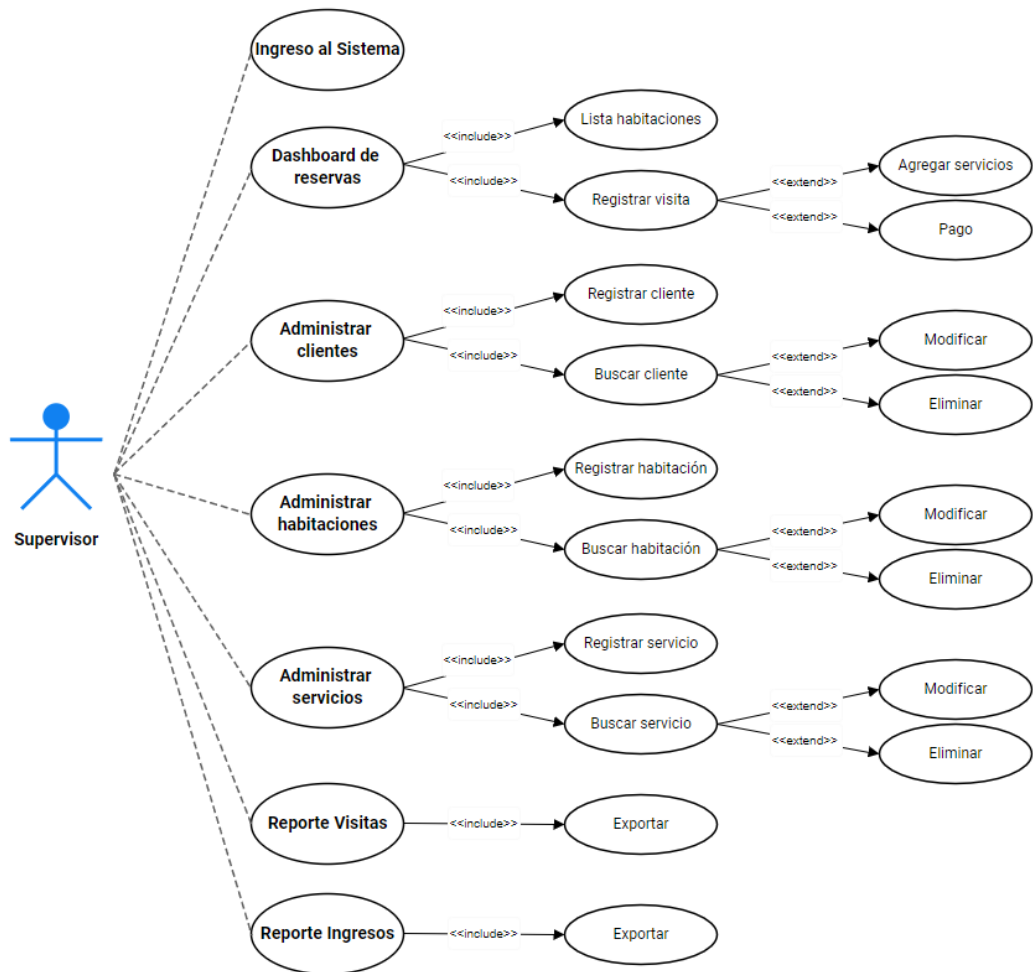


Figura 32: Diagrama de caso de uso del requerimiento Gestión del Supervisor

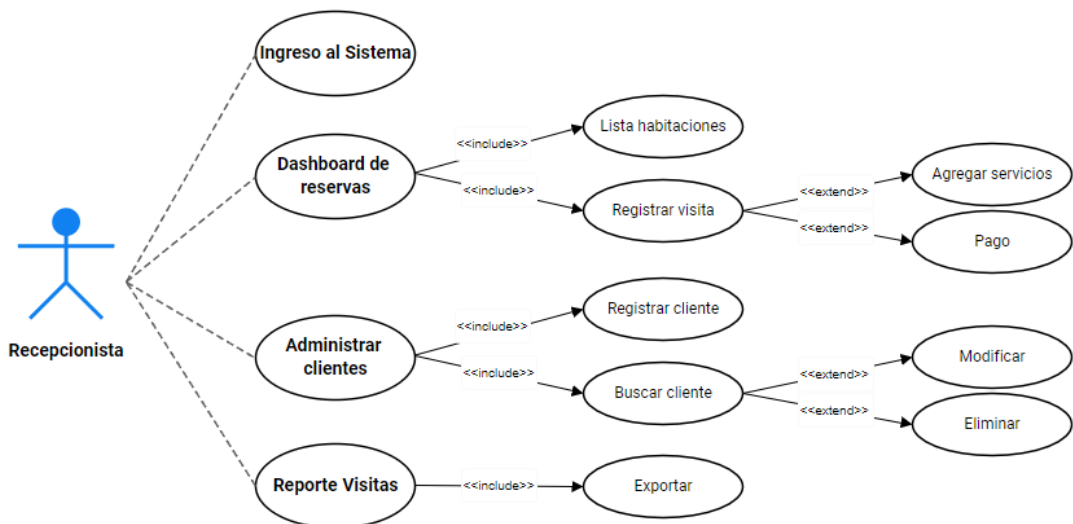


Figura 33: Diagrama de caso de uso del requerimiento Gestión del Recepcionista

○ Historias de usuario

N	Historias de Usuario	Prioridad	Riesgo	Iteración
1	RF1. Acceso y cierre del sistema	Alta	Alta	1
2	RF2. Administración de cuentas de usuario	Alta	Media	1
3	RF3. Asignación de permisos	Alta	Alta	1
4	RF4. Administración de habitaciones	Media	Media	1
5	RF5. Administración de tipo de habitación	Media	Media	1
6	RF6. Administración de clientes	Alta	Media	1
7	RF7. Administración de servicios	Media	Media	1
8	RF8. Administración de tipo de servicios	Media	Media	1
9	RF9. Módulo de reservas	Alta	Media	2
10	RF10. Registro de reserva	Media	Media	2
11	RF11. Módulo de pagos	Media	Media	2
12	RF12. Reporte de visitas	Media	Media	2
13	RF13. Reporte de ingresos por fecha	Media	Media	2
14	RF14. Reporte de inicio de sesión	Alta	Alta	2
15	RF15. Reporte de actividad en la web	Alta	Alta	2

○ Plan de iteraciones

▪ Primera iteración

N	Historias de Usuario	Prioridad	Riesgo	Iteración
1	RF1. Acceso y cierre del sistema	Alta	Alta	1
2	RF2. Administración de cuentas de usuario	Alta	Media	1
3	RF3. Asignación de permisos	Alta	Alta	1
4	RF4. Administración de habitaciones	Media	Media	1
5	RF5. Administración de tipo de habitación	Media	Media	1
6	RF6. Administración de clientes	Alta	Media	1
7	RF7. Administración de servicios	Media	Media	1
8	RF8. Administración de tipo de servicios	Media	Media	1

▪ Segunda iteración

N	Historias de Usuario	Prioridad	Riesgo	Iteración
9	RF9. Módulo de reservas	Alta	Media	2
10	RF10. Registro de reserva	Media	Media	2
11	RF11. Módulo de pagos	Media	Media	2
12	RF12. Reporte de visitas	Media	Media	2
13	RF13. Reporte de ingresos por fecha	Media	Media	2
14	RF14. Reporte de inicio de sesión	Alta	Alta	2
15	RF15. Reporte de actividad en la web	Alta	Alta	2

- Fase de Diseño
 - Diseño Lógico

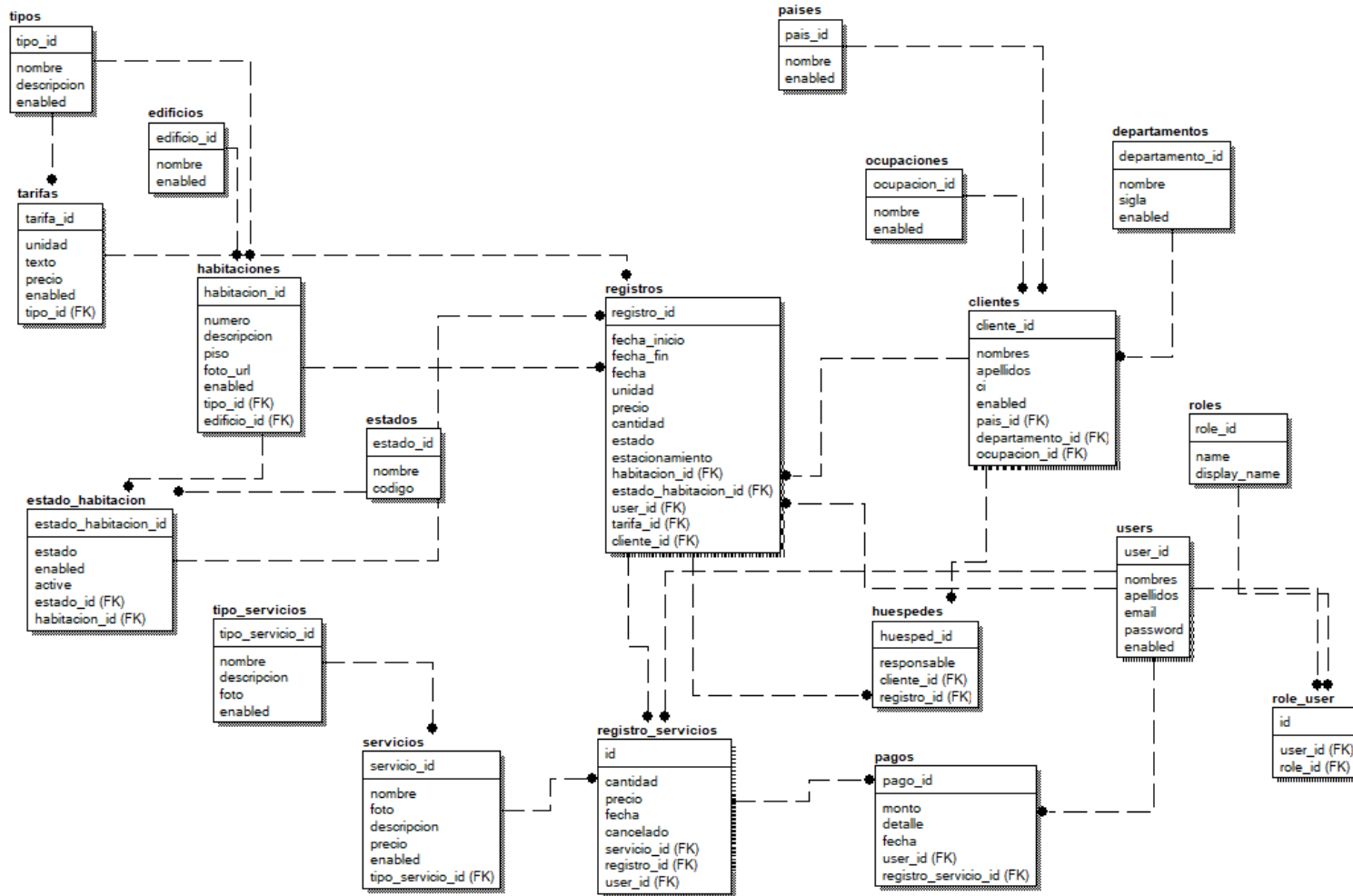


Figura 34: Diagrama del modelo lógico de la base de datos

Anexo 17: Sistema Hotelero



Figura 36: Login del sistema

The dashboard is titled 'EL PUERTO' and 'SISTEMA DE GESTION HOTELERA'. It displays a 'Lista Habitaciones' (Room List) with filters for 'Tipo' and 'Piso'. The room status summary shows: TODOS: 8, DISPONIBLE: 6, OCUPADO: 1, and MANTENIMIENTO: 1. The room list is organized by floor: 'Piso: 1' has two 'INDIVIDUAL ESTANDAR' rooms (102 and 101); 'Piso: 2' has four rooms: 'DOBLE ESTANDAR' (201), 'INDIVIDUAL ESTANDAR' (202), 'TRIPLE ESTANDAR' (203), and 'DOBLE' (204); 'Piso: 3' has two rooms: 'CUADRUPLE ESTANDAR' (301) and 'MATRIMONIAL' (302). Each room card includes an edit icon and a lock icon.

Figura 37: Dashboard principal




1 cliente ————— 2 huesped ————— 3 tarifa

D.N.I / Carnet de Extranjería

Nombres


Apellidos

Fecha de nacimiento



Celular

Estado Civil



Nacionalidad

Cerrar



Figura 38: Modulo de reserva

Lista de Servicios + Nuevo Servicio

#	Nombre	Descripcion	Precio	Tipo	Activo	Accion
1	COCA COLA 2LT	Coca Cola 2Lt	7	SNACK	<input checked="" type="checkbox"/>	
2	PARQUEO POR HORA	Parqueo por hora	8	PARQUEO	<input checked="" type="checkbox"/>	
3	OREOS	Oreo clásicas	1	SNACK	<input checked="" type="checkbox"/>	
4	INCA KOLA PERSONAL	600ml	3	BEBIDAS	<input checked="" type="checkbox"/>	
5	AGUA CIELO 1LT	Cielo de 1 Lt	3	BEBIDAS	<input checked="" type="checkbox"/>	
6	INCA KOLA	Inca Kola 600ml	2	BEBIDAS	<input checked="" type="checkbox"/>	

Figura 39: Lista de servicios

Lista de Habitaciones

[+ Nueva Habitación](#)

Buscar:

ejemplo (N° Habitación, descripción)

Tipo Habitación:

Seleccionar todos

#	# Habitación	Descripción	piso	Tipo	Activo	Acción
1	302	1 cama doble grande	3	MATRIMONIAL	<input checked="" type="checkbox"/>	
2	301	4 camas individuales	3	CUADRUPLE ESTANDAR	<input checked="" type="checkbox"/>	
3	204	1 cama doble	2	DOBLE	<input checked="" type="checkbox"/>	
4	203	1 cama individual y 1 cama doble	2	TRIPLE ESTANDAR	<input checked="" type="checkbox"/>	
5	202	1 cama individual	2	INDIVIDUAL ESTANDAR	<input checked="" type="checkbox"/>	
6	101	1 cama individual	1	INDIVIDUAL ESTANDAR	<input checked="" type="checkbox"/>	
7	102	1 cama individual	1	INDIVIDUAL ESTANDAR	<input checked="" type="checkbox"/>	
8	201	2 camas individuales	2	DOBLE ESTANDAR	<input checked="" type="checkbox"/>	

Figura 40: Lista de habitaciones

Reporte Diario de Clientes

[📄 Generar PDF](#)

27/03/2022

Seleccionar Todos:

Habitación	Nombre Completo	Nacionalidad	Edad	Profesión	D.N.I	Procedencia	Entrada	Salida	Seleccionar
201	ARMANDO ROJAS Salio	PERU	36	SIN OCUPACION	7167312		24-03-2022 11:34	27-03-2022 19:24	<input type="checkbox"/>
101	RENATO CABRERA Ingreso	PERU	26	SIN OCUPACION	71528969		27-03-2022 18:28	27-03-2022 20:03	<input type="checkbox"/>
101	RENATO CABRERA Salio	PERU	26	SIN OCUPACION	71528969		27-03-2022 18:28	27-03-2022 20:03	<input type="checkbox"/>
204	ARMANDO ROJAS Ingreso	PERU	36	SIN OCUPACION	7167312		27-03-2022 18:31	28-03-2022 12:00	<input type="checkbox"/>

Figura 41: Reporte Diario de Visitas

Logs de acceso

Buscar:

ejemplo (usuario o fecha)

[Generar archivo Excel](#)

#	Fecha de acceso	Hora de acceso	Usuario
1	15/05/2022	04-05-22 GMT-5	RENATO RENATO
2	08/05/2022	07-50-43 GMT-5	RENATO RENATO
3	26/04/2022	10-45-25 GMT-5	ADMIN DOS
4	26/04/2022	10-44-35 GMT-5	RENATO RENATO

Figura 42: Reporte de Inicios de sesión

Logs de acciones

Buscar: Generar archivo Excel

#	Fecha de acceso	Hora de acceso	Detalle	Usuario
1	26/04/2022	10-44-42 GMT-5	Habilito {servicio_id:8,nombre:"INCA KOLA",foto:null,descripcion:"Inca Kola 600ml",precio:"2",enabled:true,tipo_servicio_id:5}	RENATO RENATO
2	26/04/2022	10-19-21 GMT-5	Creo un {nombre:"INCA KOLA",descripcion:"Inca Kola 600ml",precio:"2",enabled:false,tipo_servicio_id:"5",servicio_id:8}	ADMIN DOS
3	26/04/2022	10-13-06 GMT-5	Habilito {id:6,nombres:"ADMIN",apellidos:"DOS",nombre_completo:"ADMIN DOS",ci:"71528899",celular:"989718923",nickname:null,username:"Admin2",email:"admin2@gmail.com",email_verified_at:null,"enabled":true,"registrado":3,"sucursal_id":2,"created_at":"2022-04-27T02:13:02.000000Z","updated_at":"2022-04-27T02:13:02.000000Z"};	RENATO RENATO
4	26/04/2022	10-13-02 GMT-5	Creo un {nombres:"ADMIN",apellidos:"DOS",nombre_completo:"ADMIN DOS",ci:"71528899",celular:"989718923",username:"Admin2",email:"admin2@gmail.com",sucursal_id:"2","registrado":3,"enabled":false,"updated_at":"2022-04-27T02:13:02.000000Z","created_at":"2022-04-27T02:13:02.000000Z",id:6}	RENATO RENATO

Figura 43: Reporte de acciones en la aplicación web

```
Route::middleware('auth:api')->get('/user', function (Request $request) {
    return $request->user();
});
Route::post('token', 'ApiController@login');
Route::get('ocupaciones/habilitados', 'OcupacionController@showEnabled');
Route::get('paises/habilitados', 'PaisController@showEnabled');

Route::group(['middleware' => 'auth:api'], function () {
    Route::post('users/update-password', 'UserController@validar');
    Route::get('users/roles', 'UserController@showAllRoles');
    Route::get('users/habilitar/{id}', 'UserController@enabled');

    Route::get('tipo-servicios/habilitar/{id}', 'TipoServicioController@enabled');
    Route::get('tipo-servicios/habilitados', 'TipoServicioController@showEnabled');
    Route::get('tipo_habitaciones/habilitar/{id}', 'TipoHabitacionController@enabled');
    Route::get('tipo_habitaciones/habilitados', 'TipoHabitacionController@showEnabled');
    Route::get('servicios/habilitar/{id}', 'ServicioController@enabled');
    Route::get('servicios/habilitados', 'ServicioController@showEnabled');
    Route::get('servicios/habilitados/tipo/{id}', 'ServicioController@showEnabledByTipo');
    Route::post('servicios/add', 'ServicioController@addServices');
    Route::get('ocupaciones/habilitar/{id}', 'OcupacionController@enabled');
    Route::get('paises/habilitar/{id}', 'PaisController@enabled');
    Route::get('departamentos/habilitar/{id}', 'DepartamentoController@enabled');

    Route::get('habitaciones/habilitar/{id}', 'HabitacionController@enabled');
    Route::get('habitaciones/pisos', 'HabitacionController@pisos');
    Route::get('habitaciones/listado', 'HabitacionController@listado');
    Route::get('habitaciones/disponibles', 'HabitacionController@disponibilidad');
    Route::get('habitaciones/datos/{id}', 'HabitacionController@showData');
    Route::get('registros/listar_servicios_alquiler/{id}', 'ServicioController@showByRegistro');
    Route::post('habitaciones/registran', 'RegistroController@store');
    Route::post('registros/aumentar', 'RegistroController@aumentar');
    Route::get('registros/servicios/{id}', 'RegistroController@showRS');
    Route::delete('registros/servicios/{id}', 'RegistroController@destroyRS');
    Route::post('registros/editar', 'RegistroController@editarRegistro');
    Route::put('registros/{id}', 'RegistroController@update');
    Route::delete('registros/{id}', 'RegistroController@destroy');
    Route::post('registros/servicios', 'RegistroController@storeServices');
```

Figura 44: Rutas protegidas

```

.env
1 APP_NAME=Laravel
2 APP_ENV=local
3 APP_KEY=base64:Y5sLkSVRqfch7izRFuf67Z9K64Bquvf1a3DrBaYH6s8=
4 APP_DEBUG=true
5 APP_URL=http://localhost
6
7 LOG_CHANNEL=stack
8
9 DB_CONNECTION=mysql
10 DB_HOST=127.0.0.1
11 DB_PORT=3306
12 DB_DATABASE=hoteldb2
13 DB_USERNAME=root
14 DB_PASSWORD=xiaomi2022
15
16 BROADCAST_DRIVER=log
17 CACHE_DRIVER=file
18 QUEUE_CONNECTION=sync
19 SESSION_DRIVER=file
20 SESSION_LIFETIME=120
21
22 REDIS_HOST=127.0.0.1
23 REDIS_PASSWORD=null
24 REDIS_PORT=6379

```

Figura 45: Laravel Passport

```

@Component({
  selector: 'app-lista-habitacion',
  templateUrl: './lista-habitacion.component.html',
  styleUrls: ['./lista-habitacion.component.css']
})
export class ListaHabitacionComponent extends BasePaginateClass {
  habitaciones: Habitacion[];
  modalOptions: NgbModalOptions = {};
  tipoHabitaciones: any[];
  busquedaForm: FormGroup;
  totalPaginacion: any = 0;
  labelPisoBloque: any = JSON.parse(localStorage.getItem('credentials')).user
    .sucursal.estructura;

  // loadingScroll: boolean;
  // disableScroll = false;
  // paginate: Paginated;

  constructor(
    private formBuilder: FormBuilder,
    private modalService: NgbModal,
    public habitacionService: HabitacionService,
    public alertSwal: AlertSwalService,
    public tipoHabitacionService: TipoHabitacionService
  ) {
    super(habitacionService);
    this.createBusquedaForm();
    this.list();
  }
}

```

Figura 46: Listado de habitaciones

```

@Component({
  selector: 'app-list-cliente',
  templateUrl: './list-cliente.component.html',
  styleUrls: ['./list-cliente.component.css']
})
export class ListClienteComponent extends BasePaginateClass {
  modalOptions: NgbModalOptions = {};
  BuscarForm = new FormControl('', []);
  url = environment.imgUrl2;
  currentSearchTerm = '';
  constructor(
    private modalService: NgbModal,
    public clienteService: ClienteService,
    public alertSwal: AlertSwalService
  ) {
    super(clienteService);
    this.list();

    this.BuscarForm.valueChanges.subscribe(term => {
      this.loadingScroll = true;
      this.currentSearchTerm = term;
      this.clienteService
        .getAllCliente(
          term
        )
        .subscribe((paginate: any) => {
          // this.paginate = paginate.data;
          this.dataPaginate = paginate.data;
          this.paginate = paginate;
          console.log('buscando listo', paginate);
          this.loadingScroll = false;
          // this.updateCategorias(cajas);
        });
    });
  }
}

```

Figura 47: Listado de clientes

```

createForm() {
  this.clienteForm = this.formBuilder.group({
    nombres: [
      '',
      [Validators.required, Validators.pattern('[0-9a-zA-ZñÑáéíóúÁÉÍÓÚx ]*')]
    ],
    apellidos: [
      '',
      [Validators.required, Validators.pattern('[0-9a-zA-ZñÑáéíóúÁÉÍÓÚx ]*')]
    ],
    ci: ['', [Validators.pattern('[0-9a-zA-ZñÑáéíóúÁÉÍÓÚx ]*')]],
    celular: ['', [Validators.pattern('[0-9 ]*')]],
    pais: [
      '',
      [Validators.required, Validators.pattern('[0-9a-zA-ZñÑáéíóúÁÉÍÓÚx ]*')]
    ],
    departamento_id: [
      '',
      [Validators.pattern('[0-9a-zA-ZñÑáéíóúÁÉÍÓÚx ]*')]
    ],
    fecha_nac: ['', Validators.required],
    ocupacion_id: [
      '',
      [Validators.pattern('[0-9a-zA-ZñÑáéíóúÁÉÍÓÚx ]*')]
    ],
  ],
}

```

Figura 48: Creación de cliente


```

@Component({
  template: `
    <div class="row">
      <div class="col-12">
        <div class="card">
          <div class="card-body text-center">
            <p class="display-3">Panel de {{ role }}</p>
            <p class="h3">
              Bienvenido <strong>{{ username }}</strong>
            </p>
          </div>
        </div>
      </div>
    </div>
    <router-outlet></router-outlet>
  `,
  styles: ['']
})
export class DashboardComponent implements OnInit {
  currentUser: any;
  username: string;
  role: any;
  email: string;
  id: number;

  // currentUserSubscription: Subscription;
  constructor(private authService: AuthenticationService) {
    this.currentUser = this.authService.credentials.user;
    this.username = this.currentUser.username;
    this.email = this.currentUser.email;
    this.id = this.currentUser.id;
    this.role = this.currentUser.roles[0].display_name;
    // console.log(this.currentUser.roles[0].display_name);
    // this.formGroup.patchValue({user_id: this.userId});
  }

  ngOnInit(): void {}
}

```

Figura 49: Dashboard principal

Anexo 18: Certificado de Validez
TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres de Experto: Raúl André Lino Jara
 Título y/o Grado: Ingeniero de computación y sistemas
 Fecha: 07/02/2014

DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN
 DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO
 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD

Nombre del Instrumento: Cuestionario para identificar amenazas y probabilidad de
 ocurrencias para el sistema hotelero que gestiona la información de los clientes, basado
 en el apartado de operación de la norma ISO 27001:2014

Indicadores	Criterios	Deficiente 0%- 20%	Regular 21%- 40%	Bueno 41%- 60%	Muy Bueno 61%- 80%	Excelente 81%- 100%
Claridad	Está formado con el lenguaje					x
Objetividad	Está expresado con el lenguaje apropiado					x
Organización	Está adecuado al avance de la ciencia y la tecnología					x
Suficiencia	Comprende los aspectos de cantidad y calidad					x
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico					x
Consistencia	Está basado en aspectos técnicos, científicos acordes a la tecnología adecuada					x
Coherencia	Entre los índices indicadores y dimensiones					x
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr					x
Pertinencia	El instrumento es adecuado al tipo de investigación					x
PROMEDIO						

Aplicabilidad:

El instrumento puede ser aplicado (x)
 El instrumento debe ser mejorado (x)



Firma de Experto

Observaciones:

EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres de Experto: Raúl André Lino Jara
 Título y/o Grado: Ingeniero de computación y sistemas
 Fecha: 07/02/2014

TÍTULO DE TESIS:

DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN
 DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO
 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante unas series de preguntas marcando un valor en las columnas. Así mismo, le exhortamos en la correcta determinación de la metodología en la correcta determinación de la metodología para el desarrollo de un **Sistema hotelero para gestionar la información de los clientes, basados en el apartado de operación de la norma ISO 27001:2014, para el Puerto hotel-La Libertad**, si hubiese algunas sugerencias:

ÍTEM	PREGUNTAS	Metodologías			
		RUP	XP	SCRUM	OBSERVACIONES
1	Sistema ordenado para el diseño, implementación y documentación orientado a objetos.		3		
2	Sistema con pruebas e iteraciones en las que se pueda ir perfeccionando progresivamente.		3		
3	Sistema en el que se diseña bases y plantillas de acuerdo a la necesidad		3		
4	Proceso ordenado y gradual en fases de diseño, construcción y entrega.		3		
5	Maneja una arquitectura establecida partiendo de pequeños trabajos		3		
TOTAL					

Evaluar con la siguiente calificación:

1. Malo 2. Regular 3. Bueno



Firma de Experto

Sugerencias: La metodología que ha obtenido una mayor calificación es XP

TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres de Experto: Ubidia Hoyos César Manuel
 Título y/o Grado: Ingeniero de Computación y Sistemas
 Fecha: 28/11/2008

TÍTULO DE TESIS:

DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN
 DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO
 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD

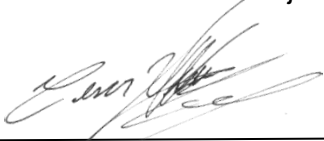
Nombre del Instrumento: Cuestionario para identificar amenazas y probabilidad de
 ocurrencias para el sistema hotelero que gestiona la información de los clientes, basado
 en el apartado de operación de la norma ISO 27001:2014

Indicadores	Criterios	Deficiente 0%-20%	Regular 21%- 40%	Bueno 41%- 60%	Muy Bueno 61%- 80%	Excelente 81%- 100%
Claridad	Está formado con el lenguaje				x	
Objetividad	Está expresado con el lenguaje apropiado				x	
Organización	Está adecuado al avance de la ciencia y la tecnología				x	
Suficiencia	Comprende los aspectos de cantidad y calidad				x	
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico				x	
Consistencia	Está basado en aspectos técnicos, científicos acordes a la tecnología adecuada				x	
Coherencia	Entre los índices indicadores y dimensiones				x	
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr				x	
Pertinencia	El instrumento es adecuado al tipo de investigación				x	
PROMEDIO						

Aplicabilidad:

El instrumento puede ser aplicado (x)

El instrumento debe ser mejorado ()



Firma de Experto

Observaciones:

_____ _____ _____

EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres de Experto: Ubidia Hoyos César Manuel

Título y/o Grado: Ingeniero de Computación y Sistemas

Fecha: 28/11/2008

TÍTULO DE TESIS:

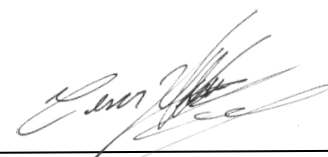
DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante unas series de preguntas marcando un valor en las columnas. Así mismo, le exhortamos en la correcta determinación de la metodología en la correcta determinación de la metodología para el desarrollo de un **Sistema hotelero para gestionar la información de los clientes, basados en el apartado de operación de la norma ISO 27001:2014, para el Puerto hotel-La Libertad**, si hubiese algunas sugerencias:

ÍTEM	PREGUNTAS	Metodologías			
		RUP	XP	SCRUM	OBSERVACIONES
1	Sistema ordenado para el diseño, implementación y documentación orientado a objetos.		3		
2	Sistema con pruebas e iteraciones en las que se pueda ir perfeccionando progresivamente.		3		
3	Sistema en el que se diseña bases y plantillas de acuerdo a la necesidad		3		
4	Proceso ordenado y gradual en fases de diseño, construcción y entrega.		3		
5	Maneja una arquitectura establecida partiendo de pequeños trabajos		3		
TOTAL					

Evaluar con la siguiente calificación:

1. Malo 2. Regular 3. Bueno



Firma de Experto

Sugerencias: La metodología que ha obtenido una mayor calificación es XP

TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y nombres de Experto: MAROCHO CAIRO FABRICIO

Título y/o Grado: INGENIERO DE SISTEMAS

Fecha: 05/12/2012

TÍTULO DE TESIS:

DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD

Nombre del Instrumento: Cuestionario para identificar amenazas y probabilidad de ocurrencias para el sistema hotelero que gestiona la información de los clientes, basado en el apartado de operación de la norma ISO 27001:2014

Indicadores	Criterios	Deficiente 0%-20%	Regular 21%- 40%	Bueno 41%- 60%	Muy Bueno 61%- 80%	Excelente 81%- 100%
Claridad	Está formado con el lenguaje					x
Objetividad	Está expresado con el lenguaje apropiado					x
Organización	Está adecuado al avance de la ciencia y la tecnología					x
Suficiencia	Comprende los aspectos de cantidad y calidad					x
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico					x
Consistencia	Está basado en aspectos técnicos, científicos acordes a la tecnología adecuada					x
Coherencia	Entre los índices indicadores y dimensiones					x
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr					x
Pertinencia	El instrumento es adecuado al tipo de investigación					x
PROMEDIO						

Aplicabilidad:

El instrumento puede ser aplicado (X)

El instrumento debe ser mejorado ()



Firma de Experto

Observaciones:

<hr style="border: 0; border-top: 1px solid black; margin-bottom: 5px;"/> <hr style="border: 0; border-top: 1px solid black; margin-bottom: 5px;"/> <hr style="border: 0; border-top: 1px solid black; margin-bottom: 5px;"/>

**EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE
TABLA DE EVALUACIÓN DE EXPERTOS**

Apellidos y nombres de Experto: MAROCHO CAIRO FABRICIO
Título y/o Grado: INGENIERO DE SISTEMAS
Fecha: 05/12/2012

TÍTULO DE TESIS:

DESARROLLO DE UN SISTEMA HOTELERO PARA GESTIONAR LA INFORMACIÓN DE LOS CLIENTES, BASADO EN EL APARTADO DE OPERACIÓN DE LA NORMA ISO 27001:2014, PARA EL PUERTO HOTEL-LA LIBERTAD

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante unas series de preguntas marcando un valor en las columnas. Así mismo, le exhortamos en la correcta determinación de la metodología en la correcta determinación de la metodología para el desarrollo de un **Sistema hotelero para gestionar la información de los clientes, basados en el apartado de operación de la norma ISO 27001:2014, para el Puerto hotel-La Libertad**, si hubiese algunas sugerencias:

ÍTEM	PREGUNTAS	Metodologías			
		RUP	XP	SCRUM	OBSERVACIONES
1	Sistema ordenado para el diseño, implementación y documentación orientado a objetos.		3		
2	Sistema con pruebas e iteraciones en las que se pueda ir perfeccionando progresivamente.		3		
3	Sistema en el que se diseña bases y plantillas de acuerdo a la necesidad		3		
4	Proceso ordenado y gradual en fases de diseño, construcción y entrega.		3		
5	Maneja una arquitectura establecida partiendo de pequeños trabajos		3		
TOTAL					

Evaluar con la siguiente calificación:

1.Malo 2. Regular 3. Bueno



Firma de Experto

Sugerencias: La metodología que ha obtenido una mayor calificación es XP

Anexo 19: Carta de autorización



CARTA DE AUTORIZACION

Yo, Guillermo Rojas Hernandez identificado con DNI 10608875 Gerente General de la empresa GYN negocios inmobiliarios SA con RUC 20600271432.

Certifica:

Que el Sr. RENATO SAMUEL CABRERA CHUMBE identificado con DNI 71528969 y Sr. GILMER ARMANDO ROJAS RETT identificado con DNI 75792113, cuenta con el permiso de la empresa para el desarrollo de su trabajo de investigación y elaboración de prototipos en las instalaciones de la empresa.

Dicha investigación podrá realizarlo solo hasta la terminación del desarrollo de la tesis en el ciclo académico que corresponda a la carrera de Ingeniería de sistemas de la universidad Cesar Vallejo año 2022.

Se expide el presente certificado a petición del interesado para fines que estime conveniente.

Lima, martes 15 de marzo 2022.

GUILLERMO ROJAS HERNANDEZ