



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**SISTEMA WEB BASADO EN LA ISO/IEC 27001 PARA LA GESTIÓN DE LA
INFORMACIÓN EN LA EMPRESA P.A PERÚ S.A.C.**

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas**

AUTORES:

Cahuana Prado Angel Cesar (ORCID: 0000-0002-5665-8165)

Cahuana Roman Alexander Elin (ORCID: 0000-0002-2996-9953)

ASESORA:

Mag. MENENDEZ MUERAS, ROSA (ORCID: 0000-0002-0767-1849)

LÍNEA DE INVESTIGACIÓN:

Sistema de Información y Comunicaciones

LIMA - PERÚ

2021

DEDICATORIA

Primeramente, agradecer a dios por habernos permitido seguir y no dejarnos caer en mal camino, por darnos salud y estabilidad, de darnos la fuerza de seguir adelante y no dejarnos derrumbar tan fácil por la avaricia.

A nuestros padres que fueron el pilar de todo éxito, a la vez nuestro motor y motivo, que siempre estuvo con nosotros a pesar de todo las alta y bajas que había en nuestro camino, agradecer a las personas que de una otra forma nos ayudó.

Agradecimiento

Agradezco a dios por la realización de este proyecto, a mi compañero por estar siempre con el compromiso en este trabajo, agradecer a los profesores por su gran enseñanza a lo largo de todo este tiempo, por siempre exigirnos al máximo, y estar siempre pendiente de nosotros, darnos una enseñanza de calidad.

A la universidad por estar siempre a nuestra disposición en cualquier de nuestro requerimiento como estudiante, y orientarnos con su abundante talle

Índice de contenido

Dedicatoria	i
Agradecimiento	ii
I. INTRODUCCIÓN	9
II. MARCO TEÓRICO	13
III. MÉTODOLÓGÍA.....	26
3.1. Tipo y diseño de investigación	26
3.2. Variables y operacionalización.....	26
3.3. Población, muestra y muestreo.....	26
3.4. Técnicas e instrumentos de recolección de datos	27
3.5. Procedimientos.....	29
3.6. Método de análisis de datos.....	31
3.7. Aspectos éticos	34
IV. RESULTADOS	35
V. DISCUSIÓN	56
VI. CONCLUSIONES	58
VII. RECOMENDACIONES	59
REFERENCIA	60
ANEXO.....	63

Índice de figuras

Tabla 1. Técnicas E Instrumentos De Recolección De Datos.....	27
Tabla 2. Valides y confiabilidad	25
Tabla 3. Estadísticos descriptivos sobre la dimensión 1: Confiabilidad.....	30
Tabla 4. Estadísticos descriptivos sobre la dimensión 2: Integridad	31
Tabla 5. Estadísticos descriptivos sobre la dimensión 3: Disponibilidad	32
Tabla 6. Estadísticos descriptivos sobre la variable: Seguridad de información	33
Tabla 7. Prueba de normalidad de Shapiro-Wilk sobre la dimensión 1: Confiabilidad	35
Tabla 8 Prueba de normalidad de Shapiro-Wilk sobre la dimensión 2: Integridad	37
Tabla 9. Prueba de normalidad de Shapiro-Wilk sobre la dimensión 3: Disponibilidad	39
Tabla 10. Prueba de normalidad de Shapiro-Wilk sobre la variable Seguridad de información	41
Tabla 11. Prueba de Wilcoxon sobre la hipótesis específica 1	44
Tabla 12. Prueba ^a de Wilcoxon sobre la hipótesis específica 2	45
Tabla 13. Prueba ^a de Wilcoxon sobre la hipótesis específica 3	46
Tabla 12 Prueba de Wilcoxon sobre la hipótesis general	47

Índice de figuras

Figura 1. Promedios sobre los porcentajes de reportes confidenciales entregados correctamente.....	31
Figura 2. Promedios sobre los porcentajes de reportes integrados generados	32
Figura 3. Promedios sobre los porcentajes de reportes entregados en el plazo establecido	33
Figura 4. Promedios sobre los porcentajes de los valores de seguridad de información	34
Figura 5 Histograma con curva de distribución normal de los reportes confidenciales entregados correctamente en el pre test.....	36
Figura 6. Histograma con curva de distribución normal de los reportes confidenciales entregados correctamente en el pos test.....	36
Figura 7. Histograma con curva de distribución normal de los reportes integrados generados en el pre test.....	38
Figura 8. Histograma con curva de distribución normal de los reportes integrados generados en el post test.....	38
Figura 9. Histograma con curva de distribución normal de los reportes entregados en el plazo establecido en el pre test.....	40
Figura 10. Histograma con curva de distribución normal de los reportes entregados en el plazo establecido en el post test.....	40
Figura 11. Histograma con curva de distribución normal sobre la seguridad de información en el pretest.....	42
Figura 12. Histograma con curva de distribución normal sobre la seguridad de información en el post test	42
Figura 13. Prueba de Wilcoxon sobre la hipótesis específica 1	44
Figura 14 Prueba de Wilcoxon sobre la hipótesis específica 2	45
Figura 15. Prueba de Wilcoxon sobre la hipótesis específica 3	47
Figura 16. Prueba de Wilcoxon sobre la hipótesis general	48

Resumen

En el actual proyecto ha adquirido el objetivo de aprender el efecto de la ejecución de un sistema web basado en la ISO/IEC 27001 para la gestión de la seguridad de la información en la empresa P.A PERÚ S.A.C. la exploración ejecutada es de tipo aplicada, con diseño experimental de tipo preexperimental. La localidad fue formada por 30 reportes frecuentes de información en un tiempo de un mes. Se aplicó un procedimiento de selección de datos la indagación y se trajo como herramienta la ficha de registro. Las consecuencias de este ensayo corroboran que la ejecución del sistema web tuvo un resultado real para la gestión de la seguridad de la información; respectivamente a los indicadores de reportes entregados en el plazo establecido, reportes integrados formados y reporte confidenciales entregados discretamente.

Se ha estipulado que el “Proporción de reportes confidenciales cedidos educadamente” tuvo un incremento, sin el sistema la media fue de 71.89 % y con uso del sistema la media fue de 96.89 %, recibiendo un incremento de 25.00% de satisfacción para los usuarios con los reportes confidenciales.

Se ha fijado que el “Proporción de reportes completados generados”, sin el software web la media es de 69.11 %, pero con uso del software la media es de 96.44 %, percibiendo una mejora de 27.33% de satisfacción para los usuarios con los reportes íntegros.

Se ha manifestado que el “Proporción de reportes cedidos en el plazo determinado” tuvo un incremento, sin el sistema la media fue de 79.44% y con uso del sistema la media es de 96.00%, lográndose mero mejoramiento de 16.56% de satisfacción para los usuarios con los reportes entregados.

Palabras clave: Sistema web, Gestión de la seguridad de la información e indicadores de porcentaje

Abstract

In this project has acquired the objective of learning the effect of the execution of a web system based on ISO / IEC 27001 for the management of information security in the company P.A PERÚ S.A.C. The exploration carried out is of an applied type, with an experimental design of a pre-experimental type. The town was formed by 30 frequent reports of information in a period of one month. A data selection procedure was applied to the inquiry and the registration form was brought as an instrument. The consequences of this test corroborate that the execution of the web system had a real result for the management of information security; respectively to the indicators of reports delivered within the established deadline, integrated reports formed and confidential reports delivered correctly.

It has been stipulated that the "Proportion of confidential reports transferred politely" had an increase, without the system the average was 71.89% and with use of the system the average was 96.89%, receiving an increase of 25.00% of satisfaction for users with confidential reports.

It has been established that the "Proportion of completed reports generated", without the web software the average is 69.11%, but with the use of the software the average is 96.44%, perceiving an improvement of 27.33% in satisfaction for users with the reports intact.

It has been stated that the "Proportion of reports transferred within the determined period" had an increase, without the system the average was 79.44% and with use of the system the average is 96.00%, achieving a mere improvement of 16.56% of satisfaction for the users with the delivered reports.

Keywords: Web system, Information security management and percentage indicators

I. INTRODUCCIÓN

En la actualidad, muchas empresas a diario se enfrentan con muchos riesgos e inseguridad que pueden ser procedentes de focos diversos tanto como internos y externo de una empresa. Esto nos dice que los diligentes de estudio de las empresas, uno de sus productos más importantes, se localizan trazados o asociados a riesgos y peligros que explotan una profunda tipología de debilidades. (Isotools, 2020).

Entre los bienes que se puede ganar en una empresa que implemente SGSI; se obtendrá la mención del marca de los riesgos, garantías de prolongación del negocio basado en la aceptación de planes de contingencias; mejorar la imagen de la organización y los aumentos del valor productivo de la organización y el rubro (esan 2019)

En el año 2018 se registraron más de 21000 ataques de cibernéticos en el país. Esto quiere decir que al día se hizo más de 60 ataques. Según una encuesta de Óptica Networks, las empresas que sufrieron con ataques fueron mediana y grandes empresas, solo el 30% de ellas fueron realizado un diagnóstico sobre vulnerabilidad de su sistema informático. (Gestion 2018)

La norma ISO 27001, es un modelo internacional que puede certificar todos los procesos de una empresa en el mejor manejo de la seguridad de la investigación (SGSI). Las empresas que logre certificase, están con la capacidad de poder demostrar a sus clientes potenciales y actuales, la capacidad de proteger la información bajo un sistema de gestión que pueda cumplir con todas la de seguridad con la norma internacional. (Optical Network, 2019)

El eje principal de la ISO 27001 es resguardar la confiabilidad, integridad y disponibilidad de toda la investigación en una empresa. Esto lo hace con la finalidad de describir cuales son los puntos frágiles de los problemas que se localizan en el medio del proceso (evaluar los riesgos que hay en la actualidad) y luego se definirá lo que es inevitable para poder evitar que estas dificultades se produzcan (tratamiento de cualquier riesgo que puede haber). (Advisera, 2020)

Existe tres pilares de la seguridad de la investigación, que ayudan a la empresa

tener la información muy resguardado, una información muestra su importancia de valor que puede aportar para una formación, la integridad y disponibilidad de la información para sacarle el enorme rendimiento con el nimio conflicto. La información puede ser representada con valores que puede ser numérico, medidas, texto, documentaciones en bruto, la investigación es un valor único de esos datos, es lo que hace la diferencia con la competencia u otras organizaciones. (Romero, 2018) Según Romero (2018) en su libro nos indica que la Disponibilidad es uno de los tres pilares de la información, esta dicha información debe ser utilizable solo para los interesados quien lo necesita o lo use en una emergencia, si la información es muy tediosa para un usuario, no estaría ayudando en la disponibilidad inmediata para requerir alguna información. (Romero, 2018).

La integridad es la segunda columna de la seguridad, nos indica que la información debe estar asegurada, quiere decir que no se puede perder si se ve comprometida voluntaria, una de las prevenciones es monitorear el tráfico de red para reducir el riesgo de posibilidad de que un usuario interno o externo pueda descargar un virus que pueda afectar la información que manejan. Verificar que pendrive introducen a un computador etc. (Romero, 2018)

Confidencialidad, en este punto consiste en que la información que será compartida solo tendrá que acceder los usuarios autorizados por el jefe, ni un personal que no tenga autorización no podrá acceder a la información, es necesario que cada uno tenga un usuario diferente para poder tener un mejor monitoreo de información. (Romero, 2018)

En términos muy práctico, el dominio es una trayectoria virtual que es identifica como la apariencia de internet en una individuo o empresa, que sirve a dirección hacia una zona web, así como para poder crear cuentas personales para empresa que todo será alojado en su servidor local. (Godaddy, 2020)

En la empresa PA PERU SAC tiene como principal actividad de la ingeniería, infraestructura y construcción de obras tales como, minería, Eléctricas, mecánicas, telecomunicaciones, gas natural, etc. Esta empresa nace hace dieciséis años (16 años) atrás en Bogotá - Colombia se creó PROFESIONALES ASOCIADOS, en la fecha es una de las empresas muy jóvenes emprendedoras que da soluciones y aportes a la ingeniería, que genera beneficio con el menor impacto ambiental en la zona de construcción.

En ese momento se da un giro al negocio apostando por invertir en el PERU, por lo cual se creó el nombre de PA PERU SAC lo cual es la representante de matriz de PROFESIONALES ASOCIADOS LTDA. Quien da soporte y garantiza los trabajos que

se va a realizar, con lo más altos estándares de calidad en la ejecución.

En la actualidad hay dos tipos de lugar de trabajo en la empresa PA PERU SAC que son: en campo y oficina, en el presente trabajo que se va a realizar donde abarcaremos en lugar de trabajo de oficina, es ahí donde se comete muchas incidencias porque se perpetra vulnerabilidad de información, en el área de externas es donde se realizan todo el plano de construcción y es allí donde se maneja volúmenes información que en otras áreas.

En el tiempo actual la empresa PA PERU SAC no tiene un buen proceso de gestionar la información, esto debido a que cualquier usuario puede ingresar a este masivo información y por falta de la confiabilidad de la información es por eso que es uno de los problemas que está afrontando la empresa en el área de externas, además de que no tiene una integridad de información, esto debido que cualquier usuario, sin restricción, pueda acceder y eliminar cualquier información que se pueda encontrar, no hay seguridad de información, cabe resaltar que toda esta información esta guardada en un PC local lo cual que no permite una disponibilidad inmediata para los usuario con permisos puedan ingresar, los reportes que se elaboran **confidencial** a diario son un promedio de 40 al día, lo cual 20 reportes salen con éxito, siendo un promedio del 50%, además de los repostes **integral** se hacen un total de 50 al día que con éxito nos arroja 20 reportes, que representa un 40% del total Y por último los reportes de **disponibilidad** que consiste con 40 reportes al día que con éxito nos agarra 30 reportes, que representa un 75% en total, debido a esta gran problemática se propuso hacer un Sistemas Web para la Gestionar la seguridad de la información utilizando la ISO/IEC 27001, con el fin de mejorar y ayudar todos los procesos de seguridad de la información, contribuir con el trabajo y el respaldo de la información, para así mismo pueda ayudar con la gestión de la información.

Como problema general se consideró: ¿Cómo influye la usencia sin un Sistemas Web para la gestión de la seguridad de la información utilizando la ISO/IEC 27001 en la empresa PA PERU SAC? Como problema específico se consideró: ¿Cómo afecta la ausencia de **confiabilidad** sin un Sistemas Web para la gestión de la seguridad de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC?

¿Cómo afecta la ausencia de **integridad** sin un Sistemas Web para la gestión de la seguridad de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC?

¿Cómo afecta la ausencia de **disponibilidad** sin un Sistemas Web para la gestión de la seguridad de la información utilizando la ISO/IEC 27001 para la empresa PA PERU

SAC?

Por lo tanto, esta investigación se justificará con los siguientes aspectos: el en aspecto teórico, puesto que se contractará los resultados de esta con las derivaciones obtenidos en informes encontrados, los cuales indicaran que la implementación de un Sistema Web para la gestión de la información utilizando ISO/IEC 27001 para la empresa PA PERU SAC. De igual modo, demostrará metodológicamente por la preparación y utilización de mecanismos de recaudación de datos tales como cuestionarios, fichas de registro y observación, mismos que utilizarán para registrar la investigación sobre los procesos de la compañía, misma que se logrará después de la cuidado de un pre-test y pos-test, así mismo, el ensayo se demostrará de forma práctica, pues como resultado de la igual se implementará una Sistema Web para la gestión de la seguridad de la información utilizando ISO/IEC 27001 que buscará resolver los problemas hallados en la compañía, finalmente, la investigación se justificará de forma tecnológica, pues como producto de esta se obtendrá una a Sistema Web para la gestión de la seguridad de la información utilizando ISO/IEC 27001 adaptado a la realidad de la compañía, así con el propósito de mejorar y gestionar la seguridad de la información utilizando la ISO/IEC 27001. Como objetivo general se consideró: Determinar la mejora de un Sistemas Web para gestión de la seguridad de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC. Como objetivos específicos identificar el efecto de un Sistema web en la integridad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU

S.A.C., identificar el efecto de un Sistema web en la confiabilidad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la compañía P.A PERU S.A.C., e identificar el resultado de un Sistema web en la disponibilidad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

II. MARCO TEÓRICO

En la investigación de Castillo (2018), en su trabajo de investigación “Ejecución De Un Gobierno Web De Misión Documentaria En La Concejo Distrital De Pararin-Provincia Recuay-Departamento De Ancash,2017”, con su principal objetivo de ejecutar la realización de un gobierno web de Gestión Documentaria en la Concejo Distrital de Pararin-Provincia Recuay-Departamento de Ancash,2017; para optimizar el nivel y disposición de atención al interesado, se realizó mediante el tipo de busca cuantitativa, de tipo descriptiva, de diseño no experimental de tajo transversal. Además, se usó un informe integrado por 2 dimensiones en el cual detallaban con 10 consultas cada uno, que sirvió para analizar a una población de 21 colaboradores y la muestra es de 21 colaboradores. Este trabajo se terminó a solicitar a perfeccionar la altura y calidad de la atención a los beneficiarios a través de un gobierno web para que le sea útil, eficiente, renovado y que además reduzca los cosechas de proceso y solicitud.

La investigación de Berrio (2016), en su compromiso de tesis “Metodología para la valoración del cometido de revisiones en sistemas de misión de seguridad de la información sobre la norma ISO/IEC 27001”, con su principal objetivo de desarrollar unos métodos para la evaluación del empuje de los sistemas de misión de seguridad de la investigación basado en la norma ISO/IEC 27001, en la exploración a aplicado la técnica de Delphi. La población muestra un total de 7 personas, con un total de 7 muestras en el documento. Se concluyó que el establecimiento de software de dirección para la seguridad de sistematización solicita seguir la evaluación en tecnologías, el departamento de sistema establece un rol muy significativo, ya que aborda efectos metodológicos para la precaución y caracterización de amenazas interrelacionadas con el incremento de ataques de sistematización.

La investigación de Nieves (2017), en su trabajo de investigación “Diseño de un

sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013”, con su principal objetivo de elaborar un software de dirección para la seguridad de sistematización fundados en la medida ISO/IEC 27001:2013, la exploración contiene un prototipo cuantitativa y cualitativa. En cierre, la tesis da riesgo que inquietan a los eficaces programadores impalpables en las disímiles agencias de la fundación, esto sirvió para manifestar la poca sensatez del tema que origina dificultades en las programaciones que generan una relación con la confidencialidad, integridad y disponibilidad.

Según Arévalo (2015), Según la revista “Creación de un sistema de gestión de seguridad de información inferior a la ISO 27001: observación del riesgo de la información”, con su principal objetivo de estudiar el escenario actual y de identificar los rasgos de la actividad productora del municipio, su don empresarial, desarrollo científico y estructura de la tela lucrativa, la investigación es de tipo descriptiva. Se concluyó que la zona tiene el reto de lograr una senda de incremento sostenido y creciente, que le asegure niveles superiores y logre aumentar la inversión productiva, la procreación de empleo y optimizar la calidad de vida para sus poblaciones.

La investigación de Nacipucha (2019), según la tesis titulada “Estudio Y Diseño Para Un Tipo De Gestión De Seguridad De La Información Basados En Normas ISO/IEC27001:2013 Para La Sociedad Artehogar En La Ciudad De Guayaquil”. Con su principal objetivo de trazar un tipo de método de gestión de la Seguridad de Investigación mediante la afán de la Norma Mundial ISO/IEC 27001: 2013 para la empresa ArteHogar S.A. en la ciudad de Guayaquil. Determinar el ambiente actual relativo a seguridad de la indagación dentro de la empresa. Observar y tramitar los riesgos en seguridad de la encuesta de la empresa. La población fue el todo el personal que hace dicha labor en la realización del software. La indagación es aplicada, con nivel aclaratorio y de diseño de investigación experimental del tipo preexperimental. Se concluyó que: A partir de la indagación elaborada en la empresa ArteHogar con analogía al

contexto presente de la seguridad de la encuesta, se obtuvo un modelo de cometido en base a la norma ISO27001:2013, con la proposito de resguardar la información de los peligros a los cuales no se localiza exenta.

Esta investigación de Aquino, Martínez y Sorto (2017), con la tesis titulada “Manual de Disposición, Ordenación de un Sistema de Gestión y Monitoreo de Redes Sistematizaciones para Pequeñas y Medianas Compañías en e l Salvador utilizando establecimiento de un programa libre”. Con su principal objetivo de diseñar un Manual de Disposición, Ordenación de un Sistema de Gestión y Monitoreo de Redes Sistematizaciones para Pequeñas y Medianas Compañías en El Salvador, utilizando establecimiento de un programa libre. La población fue el todo el personal que hace dicha labor en la realización del software. La indagación es aplicada, con nivel aclaratorio y de diseño de busca experimental del ejemplar preexperimental. Luego del estudios de datos se perfeccionó que en base a cada una de las fases del proceso de averiguación para la presente tesina, se determinó que es trascendental tener implementado un sistema de mandato y monitoreo en una red LAN en una PYMES y que esto proporciona la administración de la misma, y en este campo empresarial de las PYMES, quienes por ser compañías con utilidades algo limitadas y que estas son enfocadas a materias primas y/o servicios precisos para mantenerse en el mercado, invierten poco en la ejecución de un programa de computador de monitoreo, por Los gastos que les puede representar una inversión en este rubro.

La investigación de Meneses, Ramírez, Merchan y Suarez (2016), con la tesis titulada “Boceto Del Sistema De Gestión De Seguridad De La Investigación SGSI fundado En El Estándar ISO 27001, Para Los Conocimientos Tolerados Por El Área De gobiernos En La Cámara De Comercio De Aguachica, Cesar”. El objetivo ordinario, Diseñar el Sistema de Gestión de Seguridad de la Investigación basado en el estándar ISO 27001, para los Métodos Soportados por el Espacio de Sistemas en la Cámara de Comercio de Aguachica, Cesar. La población fue el todo el personal que hace dicha labor en la realización del

software. La investigación es aplicada, con nivel explicativo y diseño de averiguación experimental del tipo preexperimental. Luego del estudio de fichas se concluyó que la ejecución de los métodos e instrumentos de recopilación de investigación, se perfeccionó y se evidenció la escasez que existe en la Cámara de Comercio de Aguachica, de darle un método mejor a la investigación que se maneja en cada uno de los métodos llevados por los clases de la institución; mediante la ejecución de normas que regularicen, estandaricen y certifiquen la confidencialidad, integridad y disponibilidad.

La investigación de Molano (2017), con la tesis titulada “Estrategia Para Hacer 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”. Con su principal objetivo de asemejar la mejor táctica en el proceso de culminación de un Gobierno de Gestión de Seguridad de la Investigación fundadas en la norma ISO 27001 en el espacio de TI para la compañía Market Mix. La población fue el todo el personal que hace dicha labor en la realización del software. La indagación es aplicada, con nivel explicativo y diseño de exploración experimental del tipo preexperimental. Luego de la observación de datos se perfeccionó que. El objetivo de naciente compromiso de nivel era asemejar una táctica para la ejecución de un Gobierno de Gestión de Seguridad de la Indagación para el espacio de TI de la compañía Market Mix, después de haber escogido las herramientas que aprobaron la valoración del estado presente del área de TI, los datos obtenidos se ejecutaron y aprobaron que se igualara la mejora habilidad que se debe desplegar paso a paso con el desenlace de cometer con los objetivos de esta.

En la investigación de Bermúdez y Bailón (2015), con la tesis Estudios en seguridad sistematización y seguridad de la investigación apoyado en la estándar ISO/IEC 27001 Gobiernos de misión de seguridad de la investigación dirigido a una compañía de valores financieros. El objetivo general, Analizar los técnicas críticos de Credigestión proporción a las gestiones de seguridad correctas para avalar la confidencialidad, integridad y disponibilidad de la

información, mediante la formulación encargos de seguridad y controles basados en la Norma ISO/IEC 27001. La investigación fue tipo descriptiva, con un nivel explicativo y de croquis de investigación práctico del tipo preexperimental. Luego de la observación de datos se concluyó que el análisis elaborado demuestra que los eficaces de información de las espacios estimadas críticas y la situación actual de la compañía con respecto a la seguridad de la investigación, evidencia potencial listos de riesgo, los cuales muestran a la investigación perjuicios, hurto o transformaciones que pueden hacer un impacto perjudicial dentro de las acciones del negocio.

En la investigación Guzmán (2015), en su encargo de investigación Metodología Para La Seguridad De Tecnología De Investigación Y Comunicaciones En La Clínica Ortega. Con su principal objetivo de establecer el nivel de importancia metodología de seguridad de tecnologías de investigación y comunicaciones que permita la continuidad de métodos de la clínica Ortega cuyos valores principales depende de la tecnología. La investigación fue de tipo descriptiva, con un nivel explicativo. Luego del examen de datos se concluyó que para el desarrollo del tipo de seguridad de tecnologías de información y comunicaciones se hubo en cuenta Normas sistemáticas y las representaciones del modelo ISO, además, se efectuó la evaluación financiera del mismo el cual ha sido tomado como reseña para considerar que el propósito metodologías de tecnologías de información y comunicaciones es económico factibles.

En la investigación Rak (2020), en su artículo Modeling Web Client and System Behavior, con su principal objetivo que es permitir una especificación del modelo jerárquico para reducir el tamaño del modelo. Este método es muy flexible y de bajo costo. Los resultados fueron experimentales mostrando que este método podría aplicarse a sistemas web más complejos. Se concluye que este trabajo propone un marco de ingeniería del desempeño del sistema web. El formalismo QPN se aplicó al desarrollo de una herramienta de software para que soportar el diseño del sistema.

En la investigación de Dotsenko, Illiashenko, kamenskyi y Kharchenko (2019), en el artículo de investigación Integrated Security Management System for Enterprises in Industry 4.0, con su principal objetivo de cumplir con los requisitos para la gestión de seguridad de las compañías que implementan los principios de la Industria 4.0. Estándares clave como ISO/IEC 7498, 15408, 18045, 20000, 27000 que han sido analizados para sugerir un enfoque en el desarrollo de la estructura integrada del sistema de gestión de seguridad y protección teniendo en cuenta las amenazas de intrusión en la información física y la señal espacios. Este compromiso se concluye que el sistema de gestión de seguridad empresarial corresponde al principio de construcción de los sistemas de control jerárquico basados sobre la integración de los canales correspondientes del sistema de control. Por el contenido de la ley de control, este sistema se refiere a los sistemas de control cibernético con retroalimentación, por lo que se puede describir con el aparato matemático apropiado.

En la investigación de Abazi (2020), en su trabajo de investigación “A Novel Approach For Information Security Risk Assessment Maturity Framework Based On ISO 27001”, con su objetivo de identificar la brecha entre la práctica y la teoría que luego se puede cerrar siguiendo un enfoque orientado al proceso. El estudio actual presenta un método que proporciona un lugar de partida para hacer cumplir la seguridad, una visión de seguridad común y un marco para priorizar acciones. En conclusión, este trabajo da un enfoque, modelo y solución para la conteo de conflictos de seguridad de la información especialmente para el sector bancario, las compañías de seguros y la industria de TI. Además, este enfoque explora algunas de las mayores brechas que tienen las organizaciones en la implementación de la seguridad.

En la investigación de Kim y Yoo (2019), en su artículo Estado actual e investigación sobre la vulnerabilidad web del sistema de control, con su principal objetivo de clasificar y comparar los elementos de vulnerabilidad web existentes para derivar los ataques de piratería web más probados contra el sistema de control desde el estado de vista del atacante. Los resultados de

este estudio es examinar la vulnerabilidad web del sistema con el control de Sistema web. En conclusión, por los intentos de conectarse a Internet ocurren constantemente, y cada empresa y organización dice que nuestro sistema de control es una red cerrada.

Según Aguirre (2018), en su tesis Gobierno web para la gestión de la seguridad de la investigación ordenada a la regla ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C - La Molina, con su principal justificación en determinar el resultado de un Sistema web en la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la compañía de productos informáticos - La Molina, esta investigación es aplicada, con diseño experimental del tipo pre experimental, con un total de su población de 30 reportes diarios. Este trabajo se concluyó al comprobar el porcentaje de reporte de ingresos creados formando uso de un software web en la gestión en seguridad de la investigación en la organización Servicios Informáticos S.A.C. ampliación, sin el software web se midió un porcentaje de 74.06% por con el uso del sistema web se midió 97.94%, logrando el aumento de 23.88%. En la investigación de Mirtsch, Kinne y Blind (2020), en su artículo Explorando la adopción del sistema internacional de misión de seguridad de la información estándar ISO/IEC 27001: Un análisis basado en minería web, con su principal objetivo de explorar la adopción de ISO/IEC 27001, sino también adoptando esta norma de otras formas, los resultados de esta investigación mostraron que este enfoque produce predicciones confiables y tiene el potencial de ser una adición valiosa y altamente rentable al conjunto existente de indicadores de innovación. En conclusión, se describe las limitaciones de este artículo y se discute la idoneidad de la minería web para explotar la adopción de ISO/IEC 27001 y sus estándares de sistema de gestión en general.

Según Huerta (2020), en su tesis Sistema de gestión de seguridad de la investigación para optimizar el proceso de gestión del riesgo de Coopsol Consultoría, 2019, con su principal objetivo en estimar la manera en que la ejecución del Sistema de Gestión de Seguridad de la Investigación hacer caer

la balanza en el proceso de gestión de peligro de Coopsol Consultoría, el prototipo de investigación es aplicada, con un total de población de 24 activos. Este trabajo se concluye mediante los resultados expuestos en la prueba estadística de Student con un valor total de 4,614 al asumir varianzas iguales en la comparación de medidas del Pretest y Post test.

Según Carrasco (2018), en su tesis Sistema web matrícula para Business Process Management de la Facultad de Ingenierías de la Universidad Privada Juan Pablo II, con su vital objetivo en mejorar significativamente el desarrollo de los procesos de matrícula de la Universidad Privada Juan Pablo II, el prototipo de indagación es empleada y el diseño cuasi experimental, con un total de población de 130. Este trabajo finaliza en su objetivo general, en el cual demuestra con el gobierno web de matrícula para BPM, la formación mejor significativamente.

En la investigación Saber (2019), en su artículo An Integrated Framework to Enruse Information Security Over the Internet, con su principal objetivo en proponer un recuadro para la seguridad de la información que proporciona un nuevo procedimiento y estrategia para la gestión de la seguridad de la información, el resultado de esta investigación se basa en proporcionar una solución integrada a los dificultades de seguridad de la información al incorporar tácticas y procedimientos metodológicos, en conclusión, a partir de las estrategias y procedimientos metodológicos incorporados junto con las múltiples técnicas de análisis matemático y lógico, el marco propuesto definitivamente podrá funcionar mucho mejor que los sistemas existentes para la seguridad de la investigación para el conjunto de datos o información dado.

Según Ohud y Nigel (2020) con el artículo Performance Modelling of the Impact of Cyber Attacks on a Web-based Sales System, con el objetivo de evitar temporal o permanentemente que los usuarios legítimos accedan a los recursos, el resultado de este artículo es en calcular el rendimiento de algunas acciones principales de Customer y en conclusión de este documento es en

presentar los modelos de desempeño del sistema de venta en web en dos escenarios, con o sin presencia de ataques de denegación de servicio.

Según Ključnikov, Mura, Sklenár (2019), con el artículo Information Security Management in SMES: Factors Of Success, con el principal objetivo de este trabajo fue de identificar los factores de éxito de la gestión de la seguridad de la investigación en el segmento de las pymes en Eslovaquia, el resultado de la investigación nos muestra que los controles de seguridad y la alta dirección de apoyo son los factores más importantes en general, mientras que el factor de conciencia organizacional es el más obvio e importante en el corto plazo, en conclusión el tema de la dirección de la seguridad de la investigación se vuelve de vital importancia, especialmente en el segmento de las chicas y medianas compañías.

Según Leiva (2016), con la tesis Diseño de un Sistema de Gestión de Seguridad de la Investigación basado en las Reglas ISO/IEC 27001 e ISO/IEC 27002 para resguardar los laborosos de investigación en el causa de abastecimientos de remedios de la Red de Salud de Lambayeque 2015, con su principal objetivo de contar con una organización de Hardware y Software que preserve la integridad y disponibilidad de la averiguación de software que elabora en la red concreto del malware, troyanos y otros virus que transgredan contra la integridad y disponibilidad de la investigación acumulada en pausas de trabajo y cualquier otro intermedio magnético, con tipo de investigación tecnológica formal, en conclusión se semejó

los conocimientos de oficio haciendo manejo del instrumento de BIZAGI y con la anotación BPMN 2.0 para los métodos de comisión de compra, repartimiento de medicinas, gestionar el control de calidad de alimentos, en el cual permitió establecer como se definiría nuestro gobierno de gestión de seguridad de la averiguación.

Según Sheikhpour y Modiri (2016), con el artículo A best approach for

integration of ITIL and ISO/IEC 27001 services for information security management, con su principal objetivo de explorar el pliego de la gestión de la seguridad de la investigación internamente de la gestión de bienes de ITIL y como ITIL e ISO/IEC 27001 están ordenados y puedan elaborar adyacentes para optimizar la gestión de seguridad de la información y se concluyó que la seguridad de la información detalla las actividades que se relacionan con la defensa de información de activos de construcción contra los riesgos de traspapelada, mal uso, publicidad o perjuicio.

Según Syreyshchikova, Pimenov y Liviu (2019), con el artículo Information Safety Process Development According to ISO 27001 for an Industrial Enterprise, con el objetivo principal de garantizar la continuación del negocio, mermar los riesgos comerciales y propagar el retorno de la adquisición y las procedencias comerciales, dando como resultado del trabajo que se ha realizado han sido aprobados e implementados en la empresa y tienen una importancia práctica significativa no solo para la empresa, sino también para el perfil de la industria en su conjunto. En conclusión, de esta investigación era el de diseñar, desarrollar y dominar el proceso de seguridad de la investigación de acuerdo con las necesidades de la ISO 27001 para las condiciones de la empresa industrial JSC "K".

Según Alqahtani, Almytlaq, Alomari y Mahmoud (2020), con el artículo Web Based System for Electronic and Electric Devices Maintenance, con el objetivo de elaborar una plataforma electrónica inteligente para elevar la calidad de vida de los individuos reduciendo el tiempo y esfuerzo invertido en el trabajo rutinario, dando como resultado que existe una gran categoría que necesita un sitio de mantenimiento que facilite el proceso de mantenimiento, y también hay categoría que busca brindar servicio de mantenimiento a los clientes con alta calidad y eficiencia.

Según Ramalingam, Arun, Anbazhagan (2018), con el artículo A Novel

Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM, con el objetivo de llegar a un IT- GRC optimizando mediante la introducción de un modelo matemático novedoso para optimizar la seguridad de la investigación mediante la ejecución de un IT-GRC optimizado mediante el método del Laboratorio de Evaluación y prueba de toma de decisiones (DEMATEL) y llegar a una Figura de Merito (FoM) optima, dando como resultados promedio al cumplir con el resultado deseable en la investigación, en conclusión los autores lograron resolver los problemas mencionados anteriormente que surgieron en las mediaciones cualitativas de los revisiones de seguridad que son inadecuados para medir la seguridad de los controles de seguridad.

Según Szczepaniuk, Rokicki y Klepacki (2020), con el artículo Information security assessment in public administration, con el objetivo de caracterizar y evaluar la gestión de la seguridad de la investigación de las unidades de la administración pública y definir las soluciones recomendadas que faciliten el aumento del nivel de seguridad de la investigación, estos resultados de la investigación permiten asumir que la entrega de seguridad de la investigación en la gestión pública requiere un enfoque sistémico que surge de la necesidad de una mejora permanente, en conclusión la seguridad de la investigación en la gestión pública debe percibirse en el contexto de la realización de las misiones de las instituciones y la entrega de la calidad suficiente de los servicios prestados, proporcionando simultáneamente atributos de seguridad de la información.

Según Pizzi (2020), con el artículo Cybersecurity and it's integration with safety for transport systems: not a formal fulfillment but an actual commitment, con el objetivo de mostrar que las vulnerabilidades de dispositivos y sistemas tecnológicos no deben descuidarse en el análisis de riesgos, dando como resultados obtenidos en los campos de la investigación que también pueden aplicarse a los sistemas de transporte ferroviaria, llegando a la conclusión que una ruta de ciberataque es compatible con el incidente ocurrido en el tren

regional italiano.

Según Özdemir (2019), con el artículo A Conceptual Model for a Metric Based Framework for the Monitoring of Information Security Tasks Efficiency, con el fin de corregir la eficacia y eficiencia de las tareas relacionadas con la seguridad, dando como resultado ofertas todas las cuales tiene un impacto directo o indirecto en la productividad del personal humano y las herramientas al tiempo que logran tareas relacionados con la seguridad, concluyendo en proporcionar una plataforma para la medición de la eficiencia de las tareas de seguridad para los usuarios humanos y las herramientas y dispositivos de seguridad.

Según Walkowiak, Kami (2017), según el artículo Influence of Data Delivery on Availability of Web Systems, con el objetivo de proponer un adaptador personalizado que corta el tiempo de carga inicial y, como resultado, aumentar la disponibilidad de un sistema web, en conclusión, el adaptador personalizado permite reducir la disponibilidad del sistema en comparación con GoldenGate. además, el uso del adaptador personalizado no requiere espacio adicional en el disco porque todo se realiza en la memoria.

Según Laínez (2015), con la obra Desarrollo de Software Ágil: Extreme Programming y Scrum.2ª Edición, la metodología XP es considerado una metodología ligera de desarrollo de software. Esta es catalogada como un sistema de experiencias que la entidad de desarrollos de software viene desarrollando para solventar las dificultades de entrega de software de calidad velozmente, y poder lograr los requisitos de negocio que eternamente cambian.

No obstante, la XP no se emplea a todos los ejemplos de planes, siendo más apropiado para los planes con dispositivos chicos o medianos, de 2 a 12 individuos, ya que al dividirlos en sub-proyectos independientes. Los proyectos extensos deben ser partidos en una Bpermanencia de unas tres semanas (Laínez, 2015, p.107).

Por otra parte, según Borborema (2007), con el informe Impacto da aplicada la

metodología XP en las organizaciones de desenvolvimiento del software, en el cual nos dice el uso de la XP debe ser realizado en empresas que priman los procesos dinámicos de desarrollo, basados en la asistencia del cliente y en el aprendizaje perene de todos los integrantes del equipo.

Según Anwer, Aftab, shah, shah y Waheed (2017), con el articulo Coparative Analysis of Two Popular Agile Process Models: Extreme Programming and Scrum en el cual define a las fases como:

La fase de planificación: Durante el período de planificación, las tareas se extraen de cuentas de usuarios y se describen en tarjetas de tareas.

La fase de diseño: El diseño simple es una gran practica de XP que refuerzo a diseñar la funcionalidad capital citada del sistema y evita detalles innecesarios. Se centra en las funciones que se necesitan actualmente.

La fase de codificación: La codificación la realizan dos programadores en la misma máquina. La idea detrás de la programación por pares es desarrollar software de admisión calidad a menor costo.

La fase de prueba: Después de completar cada tarea, el sistema se integra y se prueba. Puede suceder muchas veces al día. Esto reduce los dificultades de integración y adelanto la calidad del software.

III. METODOLOGÍA

3.1. Tipo y diseño de indagación Pauta

de investigación: Aplicada.

Diseño de indagación: experimental de grado pre-experimental.

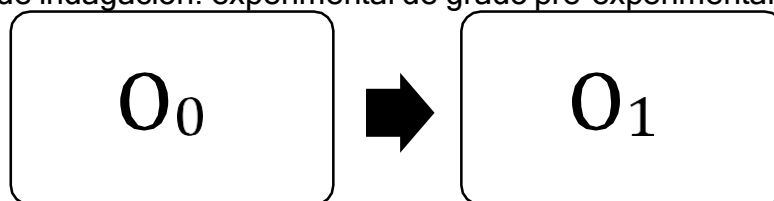


Figura 1. Diseño de investigación Fuente:

Elaborado por los autores

Donde:

O_0 : Seguridad de la información utilizando la ISO/27001 antes de la implementación de Sistema web para gestionar la información.

X : Sistemas Web

O_1 : Seguridad de la información utilizando la ISO/27001 después de la implementación de Sistema web para gestionar la información.

3.2. Variables y operacionalización

Variables

- Variable independiente: Sistema web
- Variable dependiente: Seguridad de información

3.3. Población, muestra y muestreo

Población

Para Lind, Marchal y Wathen (2008) definen la población como: “ligado de personas u objetos de ventaja o medidas logradas a partir de todos los individuos u objetos de beneficio” (p.7).

El presenta investigación cuenta con una población, siendo los mismos personales de la compañía de PA PERU SAC, en el área de externas, teniendo un aproximado de 23 colaboradores que manejan la información de manera directa, lo cual los colaboradores tienen un intervalo de edad de

22 a 28 años de la sucursal de lima.

Muestra

Para Lind, Marchal y Wathen (2008) definen la muestra como: la muestra “es una trozo o parte de la población de ventaja” (p. 7).

Nuestra muestra es similar a la población que viene a ser 23 colaboradores.

3.4. Técnicas e instrumentos de recolección de datos

Según Orellana (2015):” El registro de los datos alcanzados en la aplicación de los métodos de recolección constituye un aspecto sustancial dentro del trabajo de campo, ya que de estos datos depende la construcción, perspicacia o interpretación del ambiente en estudio. Para esta presente investigación se realizó con la ayuda de la siguiente técnica e instrumento, para tener una mejor precisión al momento de recolectar los datos.”

- OBSERVACION:

Según Rekalde (2015): “La reflexión se ha registrado a través de las notas de campo, de gobiernos categoriales procedente, y de la reparación de la realidad, para comenzar reiteradamente el ciclo con una nueva observación.”

Se tendrá que supervisar a cada usuario con la incidencia que pueda ocurrir durante el día de su trabajo, esto nos ayudara en cuanto incidencia al día ocurre, por usuario y quienes son los que comenten más fallas al día, además de cuánto tiempo de paralización se realizara cuando se cometerá estas incidencias.

C: Cuestionario “Comunicación Ascendente y Descendente”

Tabla 1. *Técnicas E Instrumentos De Recolección De Datos*

INDICADOR	TECNICA	INSTRUMENTO	FUENTES	INFORMANTES
-----------	---------	-------------	---------	-------------

Comunicación vertical ascendente	Encuesta	Cuestionario	Área de Externas	Trabajadores del área de Externas
Comunicación vertical descendente	Encuesta	Cuestionario	Área de Externas	Trabajadores del área de Externas

Validez y confiabilidad

Validez

Hernández (2018) manifiesta con respecto a la validez lo siguiente: la validez del participio se logra mediante las sentencias de peritos y al afirmar que las extensiones discretas por el herramienta sean definidas del universo o dominio de extensiones de las variables de utilidad (p.326)

Para poder establecer la eficacia de incluido del mecanismo de cosecha de datos la investigación, se realizó mediante la modalidad juicio de los expertos, del docente con el grado de poder validar, que fueron conformado por el siguiente experto.

Experto	Grado Académico	Instrumento
Jauregui Briceño Carlos	Magister	Aplicable
Menéndez Muera Rosa	Magister	Aplicable
Aradiel Castañeda Hilario	Magister	Aplicable

- ENCUESTA:

Según López (2016):” La búsqueda de los métodos de averiguación social de más abierto uso en los valores de la Sociología que ha propagarse el ámbito estricto de la averiguación científica, para cambiar en una actividad habitual de que todos

participamos tarde o temprano. Se ha generado el estereotipo de que la búsqueda es lo que hacen los sociólogos y que éstos son expertos .”

Las encuestas serán realizadas por el mismo personal de la empresa de PA PERU SAC del área de EXTERNAS que tiene una población de 23, lo cual nos arrojará un índice exacto de las incidencias que puede ocurrir en el trabajo, la encuesta tendrá pregunta sobre confiabilidad, disponibilidad e integridad.

- INSTRUMENTO:

- Libros.
- Artículos científicos.
- Tesis Cuestionarios.

3.5. Procedimientos

Para este inicio de investigación se tuvo que realizar con una entrevista al encargado del área EXTERNAS que es JOSE GARRIDO, para conocer a detalle las dificultades que están teniendo y las incidencias que ocurren a diario con esta información que nos brinda el encargado del área, para poder nosotros describir el estado actual de la realidad problemática además de poder conocer de cómo es el flujo de trabajo interno en el área

(CREACION, MODIFICACION DE PLANOS),
HABILITACIONES DE tubería y conexión, etc.). Para poder estar más involucrado con lo que ellos hacen a diario.

Una vez obtenida la entrevista con el encargado del área externas, JOSE GARRIDO y poder llegar a un acuerdo verbal procedió el a redactar la realidad problemática de la respectiva área, así mismo una vez redactada se procedió a determinar el objetivo de estudio y el campo de acción.

Así mismo se define el título de la investigación, definición de los objetivos de esta, se realizó el estudio la cantidad de la población actual del área externa y su respectivo muestra de estudio.

Así mismo en trabajo paralelo, se redactaron resaltante en la presente investigación, así como la preparación del instrumento de datos y los exteriores éticos, los aspectos administrativos los cuales contienen todos los recursos, finalmente ante la exposición de la investigación, se realizó la ensayo de originalidad de la investigación, a través de la herramienta Turnitin.

Luego se realizó el pre test para recolectar la dicha información cubierta el proceso de la seguridad de la información, lo cual hemos identificado 3 indicadores según la ISO/IEC 27001 que son: integridad, confiabilidad y disponibilidad.

Para poder tener resultado exacto y de manera óptima se elabora 3 instrumento de recolección de datos, un instrumento por cada indicador, cada uno de esto ha pasado por un proceso de evaluación, esto cuestionario respaldado por los trabajos anteriores que se encontró en tesis de otras universidades que son local, nacional e internacional.

Para el proceso de validación se consultó con experto en temas relacionados a la seguridad de información, para esta investigación se consideró que los experto fueron a través de video virtuales(zoom y meet), de cual se consideró que los expertos como mínimo estén titulados, de lo cual a través de estar conectados con los docentes se le enviaron a través del correo el avanza del proyecto(información general de la investigación), titulo, formulación del problema, objetivo y la matriz de la operalización de variables además que se envió la valides de los formatos de la validación de los indicadores. Después del primer envío del proyecto de investigación, se tuvo que levantar las observaciones que el mismo docente nos indicó, una vez levantada las observaciones se procedió a realizar el segundo envío. Finalmente, cuando ya no existían observaciones, los expertos descargaron los formatos de validación, los llenaron, los firmaron y los escanearon para enviarnos los de vuelta.

El proceso de confiabilidad, integridad y disponibilidad se realizó a través de dos métodos, uno de ellos fue en realizar los cuestionarios a base de las dimensiones, porque a través de este método se puede calcular el porcentaje de confiabilidad,

integridad y disponibilidad.

Este método se realiza, comprobando las validaciones hechas por los expertos, se cuentan las similitudes entre las validaciones y se dividen entre el número de expertos, de esa manera se pudo calcular la confiabilidad, disponibilidad e integridad.

Cabe resaltar, para que la entrevista sea de un acuerdo formal de hecho verbal con el encargado del área, este mismo firmo la carta de aceptación del sistema del instrumento en su compañía.

Para el progreso de Sistema web, se utilizará una metodología que es MVC (Modelo, Vista y Controlador) para la gestión de un sistema web esta metodología fue escogida porque se adapta más a lo propuesto por nosotros, y también una manera dinámica para los usuarios.

Se tendrá que realizar la creación de una base de datos que sea local, usaremos SQL Server 2018, la base de datos tendrá como pabla principal los usuarios, tipo de trabajo y cargo que tienen cada uno, para poder gestionar los procesos del área, así se podrá mejora en todo el aspecto y bajar el porcentaje de erros que tienen en la actualidad, lo principal es la integridad, confiabilidad y disponibilidad, según establecido por la norma internacional ISO/IEC 27001.

3.6. Método de análisis de datos

EL ensayo planteo la siguiente hipótesis especifico por cada indicador de esta dicha investigación. Estas son:

INDICADOR: Autenticación

H1: Sistemas Web basado en la ISO/IEC 27001 va a mejorar la autenticación de la seguridad de la información en la empresa PA PERU SAC en el área externa.

H0: Sistemas Web basado en la ISO/IEC 27001 no va a mejorar la autenticación de la seguridad de la información en la empresa PA

PERU SAC en el área externa.

Donde:

Aa: Autenticación antes de utilizar el Sistema Web basado en la ISO/IEC

27001 Ad: Autenticación después de utilizar el Sistema Web basado en la

ISO/IEC 27001

Hipótesis Nula H0: Un Sistema Web basado en la ISO/IEC 27001 no disminuirá la autenticidad en la empresa PA PERU SAC en el área de externas.

$$H_0 = A_a - A_d \geq 0$$

Hipótesis alternativa H1: Un Sistema Web basado en la ISO/IEC 27001 no disminuirá la autenticidad en la empresa PA PERU SAC en el área de externas.

$$H_1 = A_a - A_d < 0$$

INDICADOR: Integridad

H2: Sistemas Web basado en la ISO/IEC 27001 va a mejorar la protección de la seguridad de la información en la empresa PA PERU SAC en el área externa.

H0: Sistemas Web basado en la ISO/IEC 27001 no va a mejorar la protección de la seguridad de la información en la empresa PA PERU SAC en el área externa.

Donde:

Pa: La protección antes de utilizar el Sistema Web basado en la ISO/IEC

27001. Pd: La protección después de utilizar el Sistema Web basado en la ISO/IEC 27001.

Hipótesis Nula H0: Un Sistema Web basado en la ISO/IEC 27001 no disminuirá

la protección en la empresa PA PERU SAC en el área de externas.

$$H_0 = Pa - Pd \geq 0$$

Hipótesis alternativa H1: Un Sistema Web basado en la ISO/IEC 27001 no disminuirá la protección en la empresa PA PERU SAC en el área de externas.

$$H_2 = Pa - Pd < 0$$

INDICADOR: Acceso a la Información

H2: Sistemas Web basado en la ISO/IEC 27001 va a mejorar la Acceso a la información de la seguridad de la información en la empresa PA PERU SAC en el área externa.

H0: Sistemas Web basado en la ISO/IEC 27001 no va a mejorar la Acceso a la información de la seguridad de la información en la empresa PA PERU SAC en el área externa.

Donde:

Ala: Acceso a la información antes de utilizar el Sistema Web basado en la ISO/IEC 27001.

Ald: Acceso a la información después de utilizar el Sistema Web basado en la ISO/IEC 27001.

Hipótesis Nula H0: Un Sistema Web basado en la ISO/IEC 27001 no disminuirá la Acceso a la información en la empresa PA PERU SAC en el área de externas.

$$H_0 = Ala - Ald \geq 0$$

Hipótesis alternativa H2: Un Sistema Web basado en la ISO/IEC 27001 no disminuirá la Acceso a la información en la empresa PA PERU SAC en el área de externas.

$$H_2 = Ala - Ald < 0$$

3.7. Aspectos éticos

Para nuestra investigación se resguardará por las siguientes deferencias éticas:

- Se admite en totalidad la participación en la investigación.
- Se acatará la verdad de las consecuencias y de los datos entregados por los empleados de la empresa involucrada a la investigación.
- Se dará beneficio de las normas ISO para citar a los autores que fueron acabados para resguardar la presente investigación, mencionado en los informes bibliográficos.
- Se protegerá en discreción la investigación propia a lo que se obtuvo acceso a la compañía.

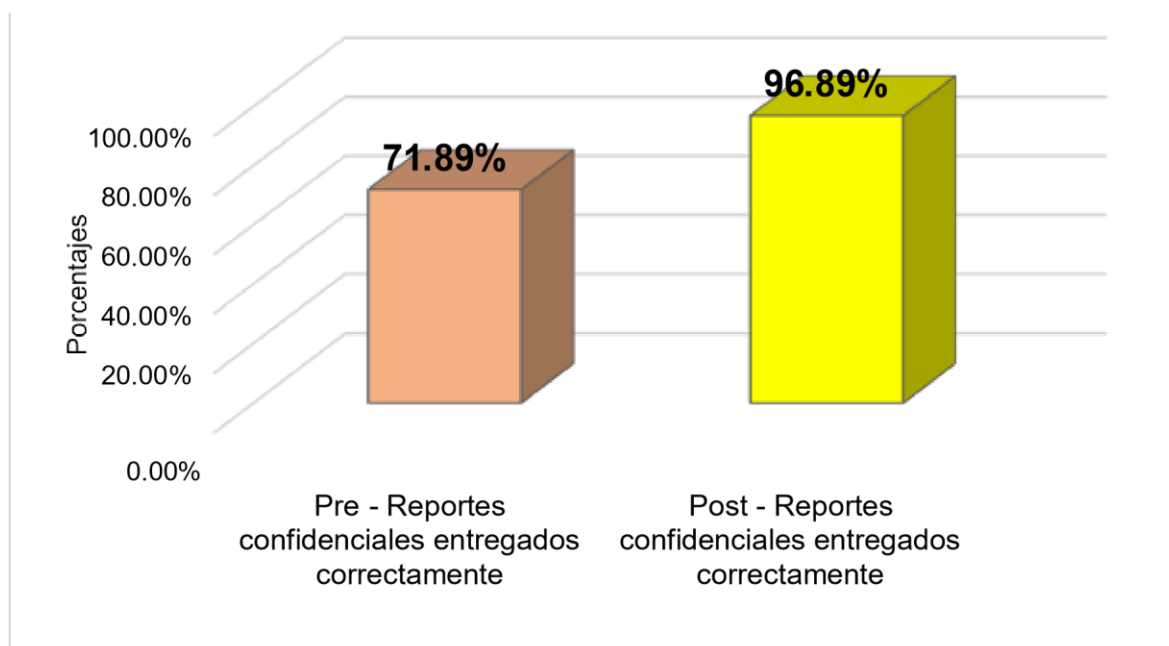
IV. RESULTADOS

Tabla 1. Estadísticos descriptivos sobre la dimensión 1: Confiabilidad

Dimensión 1: Confiabilidad	n	Media	Desviación E.	Mínimo	Máximo
Pre- Reportes confidenciales entregados correctamente	30	71,89	17,34	50,00	100,00
Post - Reportes confidenciales entregados correctamente		96,89	7,11	80,00	100,00
	30				

De acuerdo con la tabla se aprecia los estadísticos descriptivos sobre los porcentajes de reportes confidenciales cedidos educadamente antes y después de la implementación del Sistema web. De esta manera, el pre test tuvo una media de 71,89%. Mientras que en el post test hubo una media de 96,89%. De tal manera que hubo un aumento del 25,0% de reportes confidenciales entregados correctamente (ver figura 1). Por otro lado, la desviación estándar en el pre test fue de 17,34%; mientras que en el post-test fue de 7,11%. Por lo cual los porcentajes de reportes confidenciales entregados correctamente se fueron concentrando más con respecto a hacia su promedio. Por su parte, en el pre test el mínimo fue de 50,0% y el máximo de 100,0%; mientras que en el post test el mínimo fue de 80,0% y el máximo de 100,0%. De manera que se aprecia que el mínimo aumento en 30,0%.

Figura 1. Promedios sobre los porcentajes de reportes confidenciales entregados correctamente



Dimensión 1: Confiabilidad

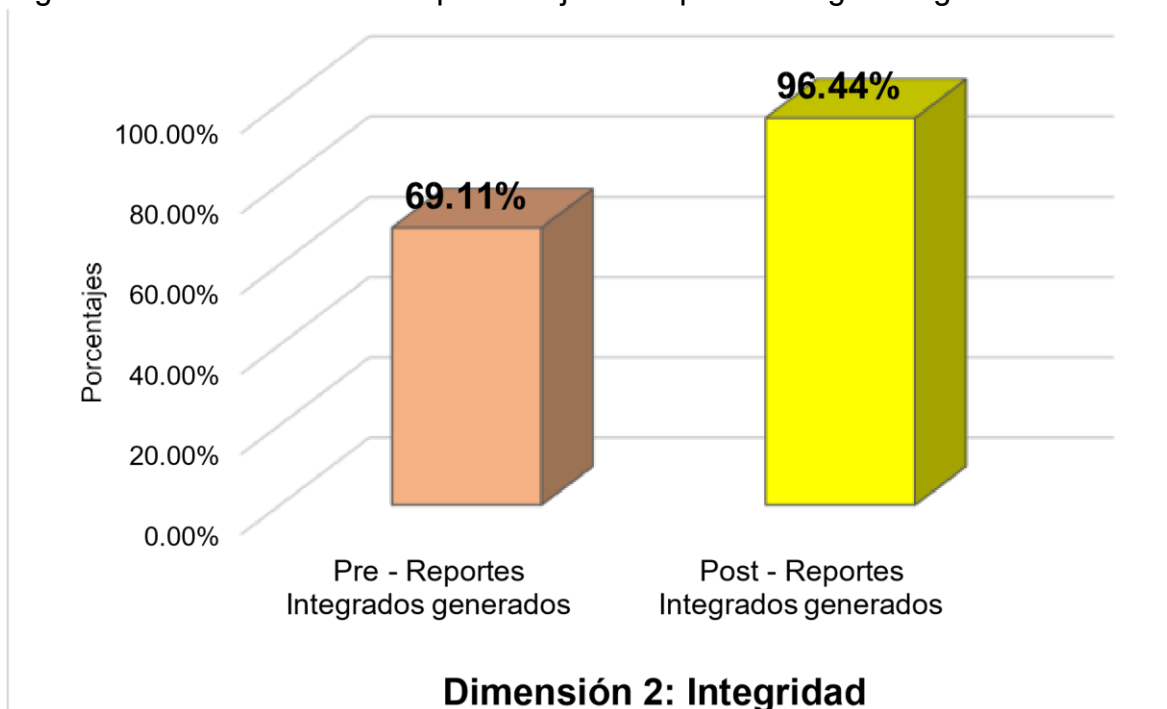
Tabla 2. Estadísticos descriptivos sobre la dimensión 2: Integridad

Dimensión 2: Integridad	n	Media	Desviación E.	Mínimo	Máximo
Pre - Reportes Integrados generados	30	69,11	14,98	40,00	100,00
Post - Reportes Integrados generados	30	96,44	7,27	80,00	100,00

En la tabla se muestra los detallados sobre los porcentajes de reportes integrados creados antes y después de la aplicación del Sistema web. De esta manera, el pre test tuvo una media de 69,11%. Mientras que en el post test hubo una media de 96,44%. De tal manera que hubo un aumento del 27,33% de reportes integrados generados (ver figura 2). Asimismo, la desviación estándar en el pre test fue de 14,98%; mientras que en el post test fue de 7,27%. Por lo cual los porcentajes de

reportes integrados generados se fueron concentrando más con respecto a hacia su promedio. Por otro lado, en el pretest el mínimo fue de 40,0% y el máximo de 100,0%; mientras que en el post test el mínimo fue de 80,0% y el máximo de 100,0%. Por lo cual se aprecia que el mínimo aumento en 40,0%.

Figura 2. Promedios sobre los porcentajes de reportes integrados generados



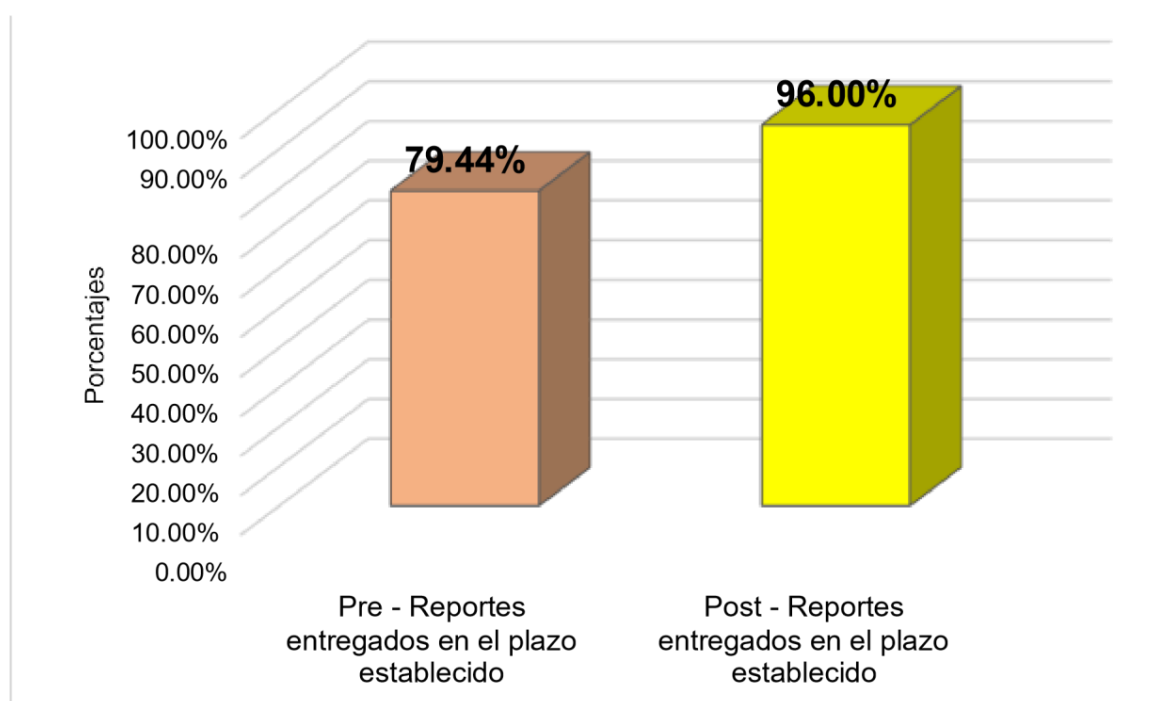
Dimensión 3: Disponibilidad	n	Media	Desviación E.	Mínimo	Máximo
Pre - Reportes entregados en el plazo establecido	30	79,44	14,81	50,00	100,00
Post - Reportes entregados en el plazo establecido	30	96,00	7,40	80,00	100,00

Tabla 3. Estadísticos descriptivos sobre la dimensión 3: Disponibilidad

Según la tabla se aprecia los estadísticos descriptivos sobre los porcentajes de reportes cedidos en el plazo establecido antes y después de la aplicación del Sistema web. De esta manera, el pre test tuvo una media de 79,44%. Mientras que en el post test hubo una media de 96,00%. De tal manera que hubo un aumento del 16,56% de

reportes entregados en el plazo establecido (ver figura 3). Por otro lado, la desviación estándar en el pre test fue de 14,81%; mientras que en el post test fue de 7,40%. Por lo cual los porcentajes de reportes entregados en el plazo establecido se fueron concentrando más con respecto a hacia su promedio. Por su parte, en el pre test el mínimo fue de 50,0% y el máximo de 100,0%; mientras que el post-test cuenta con el total de 80,0% y el máximo de 100,0%. De manera que se aprecia que el mínimo aumento en 30%.

Figura 3. Promedios sobre los porcentajes de reportes entregados en el plazo establecido



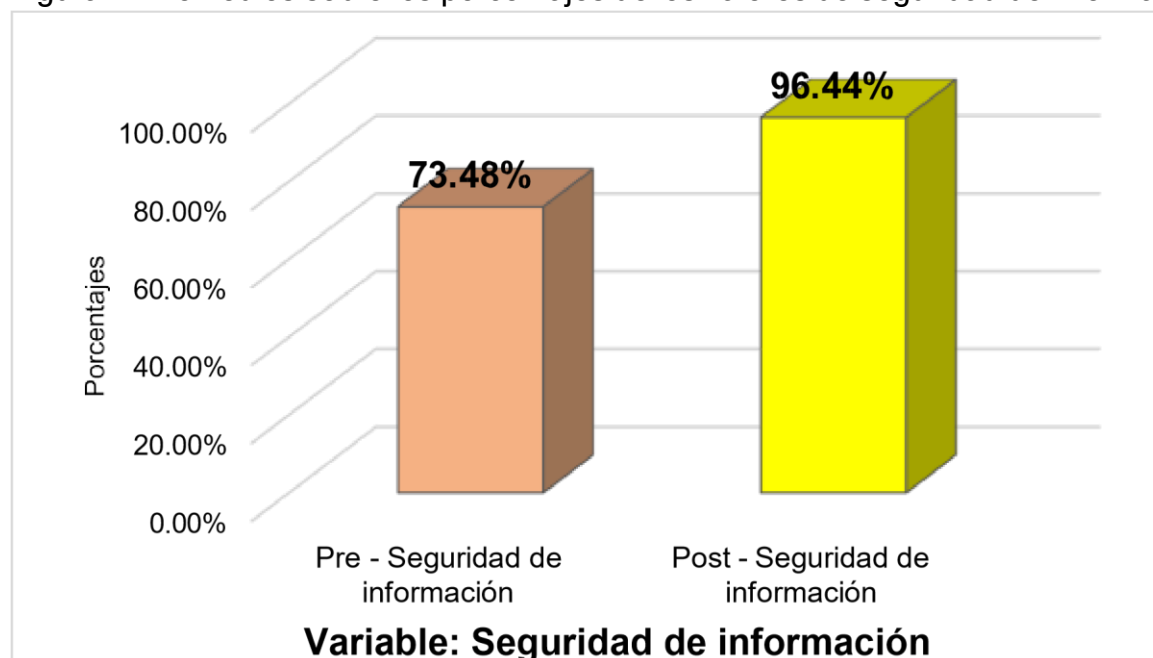
Dimensión 3: Disponibilidad

Tabla 4. Estadísticos descriptivos sobre la variable: Seguridad de información

Variable: Seguridad de información	n	Media	Desviación E.	Mínimo	Máximo
Pre - Seguridad de información	30	73,48	9,19	58,33	93,33
Post - Seguridad de información	30	96,44	5,27	83,33	100,00

De acuerdo con la tabla se aprecia los estadísticos descriptivos sobre los porcentajes de la variable Seguridad de encuesta antes y después de la implementación del Sistema web. De esta manera, el pre test tuvo una media de 73,48%. Mientras que en el post-test hubo una media de 96,44%. De tal manera que hubo un aumento del 22,96% sobre la seguridad de información (ver figura 4). Por otro lado, la desviación estándar en el pretest fue de 9,19%; mientras que en el post test fue de 5,27%. Por lo cual los porcentajes sobre la seguridad de información se fueron concentrando más con respecto a hacia su promedio. Por su parte, en el pre-test el mínimo fue de 58,33% y el máximo de 93,33%; mientras que en el post-test cuenta con un total de 83,33% y el máximo de 100,0%. De manera que se aprecia que el mínimo aumento en 25,0%; y el máximo aumentó en 6,67%.

Figura 4. Promedios sobre los porcentajes de los valores de seguridad de información



Prueba de hipótesis

Prueba de normalidad sobre la hipótesis específica 1

H1. No existe distribución normal en los porcentajes de reportes confidenciales entregados correctamente.

H0. Existe distribución normal en los porcentajes de reportes confidenciales entregados correctamente.

Nivel de significancia

0,05

Interpretaciones posibles

Si el Sig es menor a 0,05 la hipótesis nula es rechazada.

Si el Sig es mayor a 0,05 la hipótesis nula no es rechazada.

Prueba de Shapiro-Wilk

Tabla 5. Prueba de normalidad de Shapiro-Wilk sobre la dimensión 1: Confiabilidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre-Reportes confidenciales entregados correctamente	0,897	30	0,007
Post-Reportes confidenciales entregados correctamente	0,465	30	0,000

Dimensión 1: Confiabilidad

De acuerdo a la prueba de Shapiro-Wilk se muestra una significancia inferior a 0,05 para tanto el pre test como para el post test sobre los porcentajes de reportes confidenciales entregados correctamente. Ello indica que no coexiste distribución corriente en los porcentajes de reportes confidenciales transmitidos correctamente

antes y después de la aplicación del Sistema Web. A raíz de ello se debe aplicar la prueba de Wilcoxon para evaluar si el Sistema web mejora la integridad basada en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Figura 5. Histograma con curva de distribución normal de los reportes confidenciales entregados correctamente en el pre test

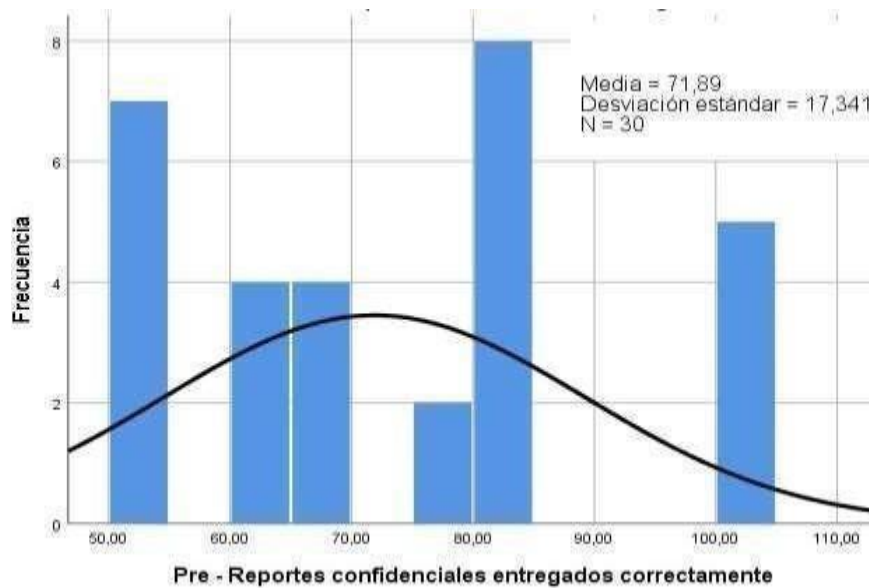
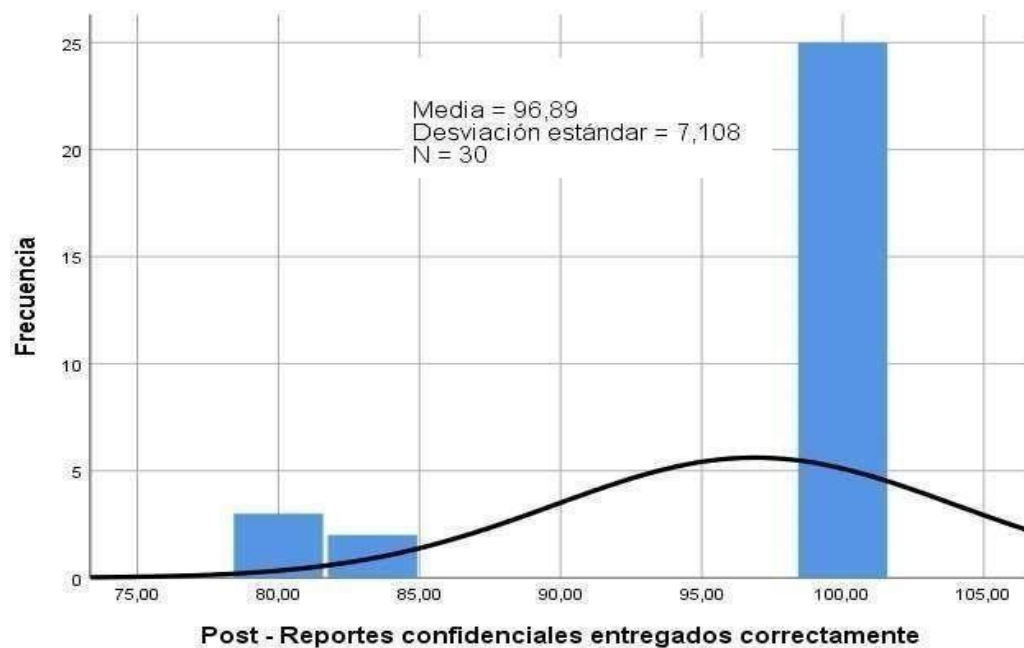


Figura 6. Histograma con curva de distribución normal de los reportes confidenciales entregados correctamente en el pos test



De acuerdo con los histogramas sobre la distribución de los porcentajes de reportes confidenciales transmitidos comedidamente antes y después de la aplicación del sistema web se aprecia que ambas distribuciones no siguen la curva de distribución normal. Por lo cual se debe aplicar la prueba de Wilcoxon para evaluar la hipótesis específica 1.

Prueba de normalidad sobre la hipótesis específica 2

H1. No existe distribución normal en los porcentajes de reportes integrados generados.

H0. Existe distribución normal en los porcentajes de reportes integrados generados.

Nivel de significancia

0,05

Interpretaciones posibles

Si el Sig es menor a 0,05 la hipótesis nula es rechazada.

Si el Sig es mayor a 0,05 la hipótesis nula no es rechazada.

Prueba de Shapiro-Wilk

Tabla 6. Prueba de normalidad de Shapiro-Wilk sobre la dimensión 2: Integridad

Dimensión 2: Integridad	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre - Reportes Integrados generados	0,952	30	0,187
Post - Reportes Integrados generados	0,512	30	0,000

Según la prueba de Shapiro-Wilk se evidencia una significancia superior a 0,05 para el pre test de los porcentajes de reportes integrados generados. Pero la significancia es inferior a 0,05 para el post test de los porcentajes de reportes integrados. Por lo que no existe distribución normal en los porcentajes de reportes integrados generados después de la implementación del Sistema Web. A raíz de ello se debe aplicar la prueba de Wilcoxon para evaluar si el Sistema web mejora la confidencialidad basada en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Figura 7. Histograma con curva de distribución normal de los reportes integrados generados en el pre test

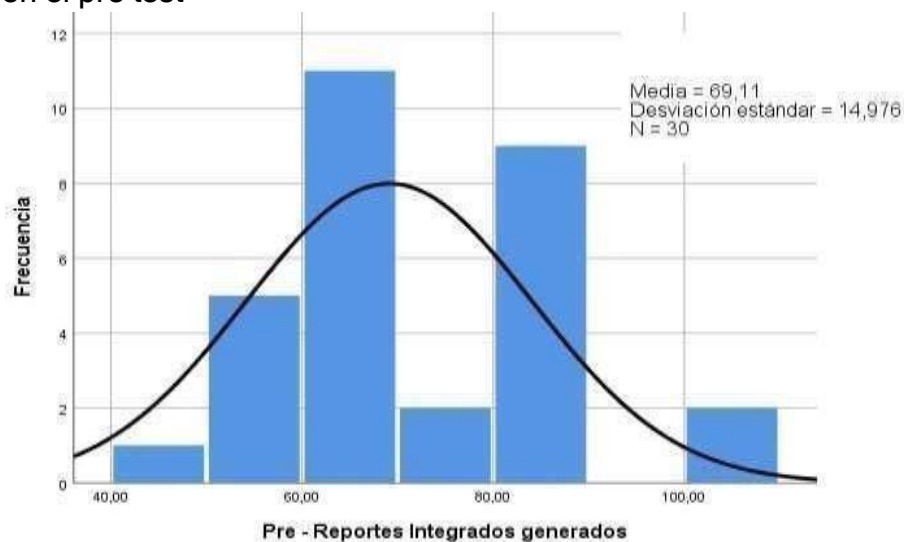
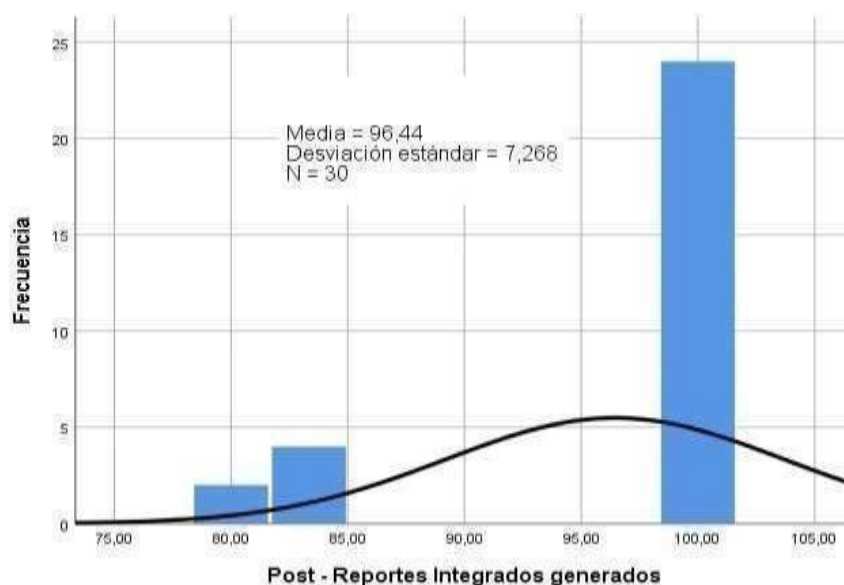


Figura 8. Histograma con curva de distribución normal de los reportes integrados generados en el post test



Según los histogramas sobre la distribución de los porcentajes de reportes integrados generados antes y después de la implementación del sistema web se aprecia que solamente en el pretest la distribución sigue la curva de normalidad. Por lo cual se debe aplicar la prueba de Wilcoxon para valorar la hipótesis específica 2.

Prueba de normalidad sobre la hipótesis específica 3

H1. No existe distribución normal en los porcentajes de reportes entregados en el plazo establecido.

H0. Existe distribución normal en los porcentajes de reportes entregados en el plazo establecido.

Nivel de significancia

0,05

Interpretaciones posibles

Si el Sig es menor a 0,05 la hipótesis nula es rechazada.

Si el Sig es mayor a 0,05 la hipótesis nula no es rechazada.

Prueba de Shapiro-Wilk

Tabla 7. Prueba de normalidad de Shapiro-Wilk sobre la dimensión 3: Disponibilidad

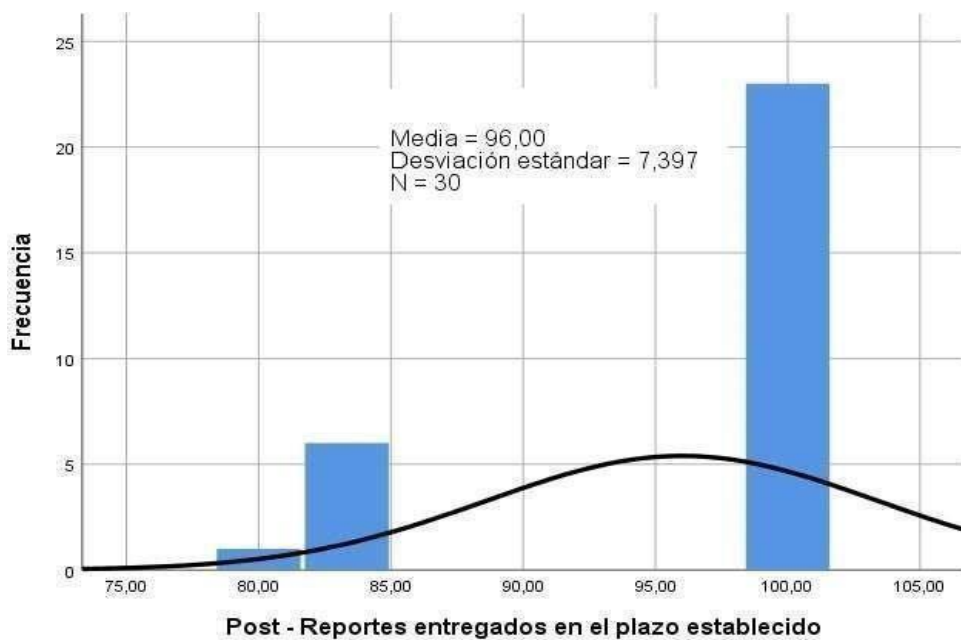
Dimensión 3: Disponibilidad	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre - Reportes cedidos en el plazo establecido	0,915	30	0,020
Post - Reportes cedidos en el plazo establecido	0,544	30	0,000

La prueba de Shapiro-Wilk muestra una significancia inferior a 0,05 para tanto el pre test como para el post test sobre los porcentajes de reportes entregados en el plazo establecido. Ello indica que no existe distribución normal en los porcentajes de reportes entregados en el plazo determinado antes y después de la aplicación del Sistema Web. A raíz de ello se debe aplicar la prueba de Wilcoxon para analizar si el Sistema web mejora la disponibilidad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Figura 9. Histograma con curva de distribución normal de los reportes entregados en el plazo establecido en el pre test.



Figura 10. Histograma con curva de distribución normal de los reportes entregados en el plazo determinado en el post test



Según los histogramas sobre la distribución de los porcentajes de reportes entregados en el plazo determinado antes y después de la aplicación del sistema web se aprecia que ambas distribuciones no siguen la curva de normalidad. Por lo cual se debe aplicar la prueba de Wilcoxon para evaluar la hipótesis específica 3.

Prueba de normalidad sobre la hipótesis general

H1. No existe distribución normal en los porcentajes sobre seguridad de información.

H0. Existe distribución normal en los porcentajes sobre seguridad de información.

Nivel de significancia

0,05

Interpretaciones posibles

Si el Sig es menor a 0,05 la hipótesis nula es rechazada.

Si el Sig es mayor a 0,05 la hipótesis nula no es rechazada.

Prueba de Shapiro-Wilk

Tabla 8. Prueba de normalidad de Shapiro-Wilk sobre la variable Seguridad de información

Variable: Seguridad de información	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pre- Seguridad de información	0,975	30	0,686
Post- Seguridad de información	0,705	30	0,000

De acuerdo con la prueba de Shapiro-Wilk se observa una significancia superior a 0,05 para el pre test de los porcentajes sobre seguridad de información. Pero la significancia es inferior de 0,055 para el post test de los porcentajes sobre seguridad de información. Por lo que no existe distribución normal en los porcentajes de seguridad de información después de la implementación del Sistema Web. A raíz de ello se debe aplicar la prueba de Wilcoxon para evaluar si el Sistema web mejora la gestión de la seguridad de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC.

Figura 11. Histograma con curva de distribución normal sobre la seguridad de información en el pretest

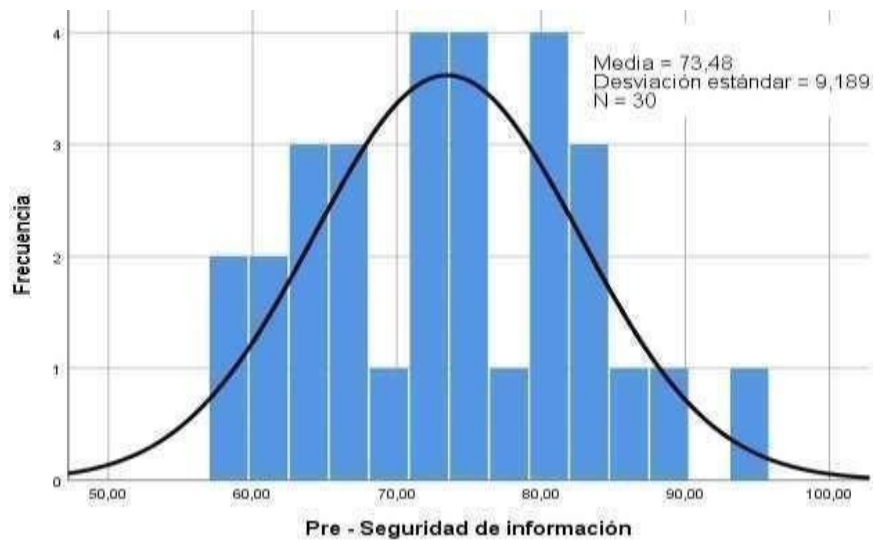
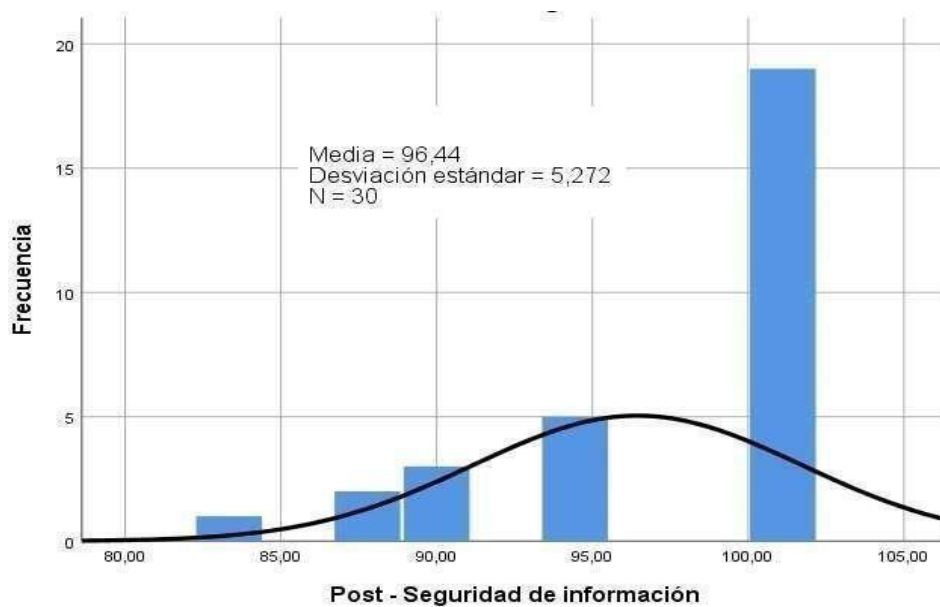


Figura 12. Histograma con curva de distribución normal sobre la seguridad de información en el post test



De acuerdo a los histogramas sobre la distribución de los porcentajes de seguridad de información antes y después de la implementación del sistema web se aprecia que solamente en el pre test la distribución sigue la curva de normalidad. De manera que se debe aplicar la prueba de Wilcoxon para valorar la hipótesis general.

Hipótesis específica 1

H1. El Sistema web mejora la integridad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

H0. El Sistema web no mejora la integridad fundado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Nivel de significancia

0,05

Interpretaciones posibles

Si el Sig es menor a 0,05 la hipótesis nula es rechazada.

Si el Sig es mayor a 0,05 la hipótesis nula no es rechazada.

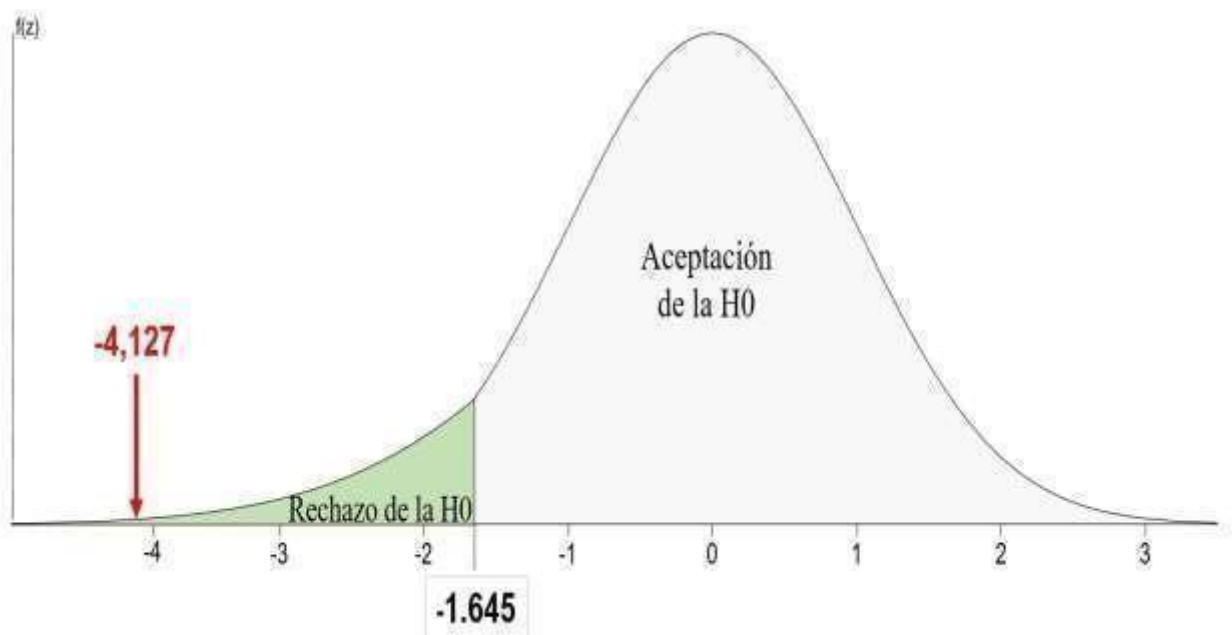
Prueba de Wilcoxon

Tabla 9. Prueba^a de Wilcoxon sobre la hipótesis específica 1

Post - Reportes confidenciales cedidos correctamente - Pre - Reportes confidenciales cedidos correctamente	
Z calculado -----	4,127 ^b
Sig. asintótica(bilateral)	0,000

-
- a. Evidencia de rangos con signo de Wilcoxon
 - b. Se basa en rangos perjudiciales.

Figura 13. Prueba de Wilcoxon sobre la hipótesis específica 1



El resultado de la prueba de Wilcoxon dio una significancia de 0,000. La cual es inferior a 0,05. Por lo cual se impugna la hipótesis nula. Ello se corrobora evaluando el valor de Z resultante, el cual fue de -4,127. Este resulta menor que el Z teórico de 1,645. Por lo cual, también se impugna la hipótesis nula, de manera que se permite indicar

que el Sistema web mejora la integridad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Hipótesis específica 2

H1. El Sistema web mejora la confidencialidad fundada en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

H1. El Sistema web no mejora la confidencialidad fundada en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Nivel de significancia
0,05

Interpretaciones posibles

Si el Sig es menor a 0,05 la hipótesis nula es rechazada.

Si el Sig es mayor a 0,05 la hipótesis nula no es rechazada.

Prueba de Wilcoxon

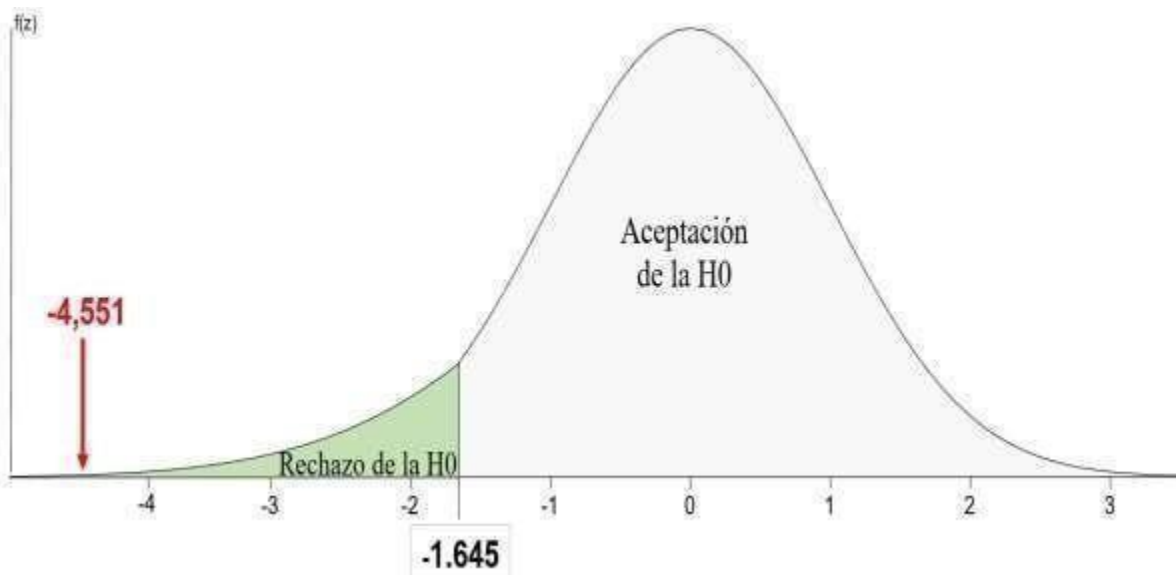
Tabla 10. Prueba^a de Wilcoxon sobre la hipótesis específica 2

	Post - Reportes Integrados generados - Pre - Reportes Integrados generados
Z calculado	-4,551 ^b
Sig. asintótica(bilateral)	0,000

a. Evidencia de rangos con signo de Wilcoxon

b. Se basa en rangos perjudiciales.

Figura 14. Prueba de Wilcoxon sobre la hipótesis específica 2



De acuerdo a la prueba de Wilcoxon dio una significancia de 0,000. La cual es inferior a 0,05. De manera que se impugna la hipótesis nula. Ello se corrobora evaluando el valor de Z resultante, el cual fue de -4,551. Este resulta menor que el Z teórico de 1,645. Por lo cual, también se impugna la hipótesis nula, de manera que se permite indicar que el Sistema web mejora la confidencialidad basada en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Hipótesis específica 3

H1. El Sistema web mejora la disponibilidad fundado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

H1. El Sistema web no mejora la disponibilidad fundado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Nivel de significancia
0,05

Interpretaciones posibles

Si el Sig es menor a 0,05 la hipótesis nula es rechazada.

Si el Sig es mayor a 0,05 la hipótesis nula no es rechazada.

Prueba de Wilcoxon

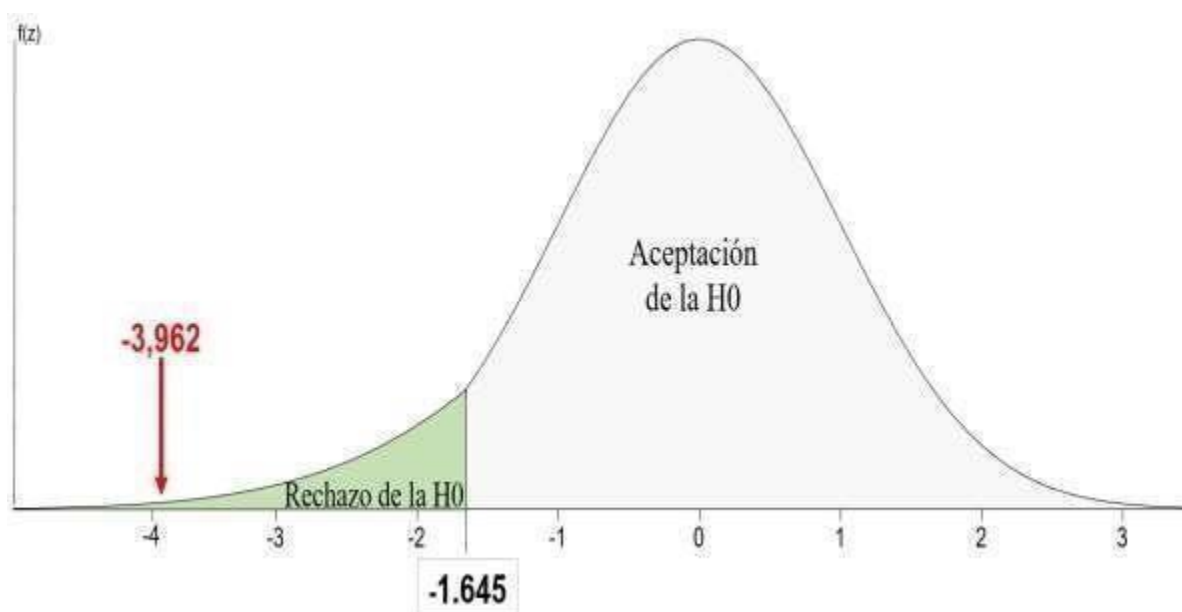
Tabla 11. Prueba de Wilcoxon sobre la hipótesis específica 3

	Post - Reportes cedidos en el plazo establecido - Pre - Reportes cedidos en el plazo establecido
Z calculado	-3,962 ^b
Sig. asintótica(bilateral)	0,000

a. Evidencia de rangos con signo de Wilcoxon

b. Se basa en rangos perjudiciales.

Figura 15. Prueba de Wilcoxon sobre la hipótesis específica 3



El ensayo de Wilcoxon arrojó una significancia de 0,000. La cual es inferior a 0,05. Por lo cual se impugna la hipótesis nula. Ello se corrobora evaluando el valor de Z resultante, el cual fue de -3,962. Este resulta menor que el Z teórico de -1,645. Por lo cual, también se impugna la hipótesis nula, de manera que se permite indicar que el Sistema web mejora la disponibilidad fundada en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

Hipótesis general

H1. El Sistema web mejora la gestión de la seguridad de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC.

H0. El Sistema web mejora la gestión de la seguridad de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC.

Nivel de significancia
0,05

Interpretaciones posibles

Si el Sig es menor a 0,05 la hipótesis nula es rechazada.

Si el Sig es mayor a 0,05 la hipótesis nula no es rechazada.

Prueba de Wilcoxon

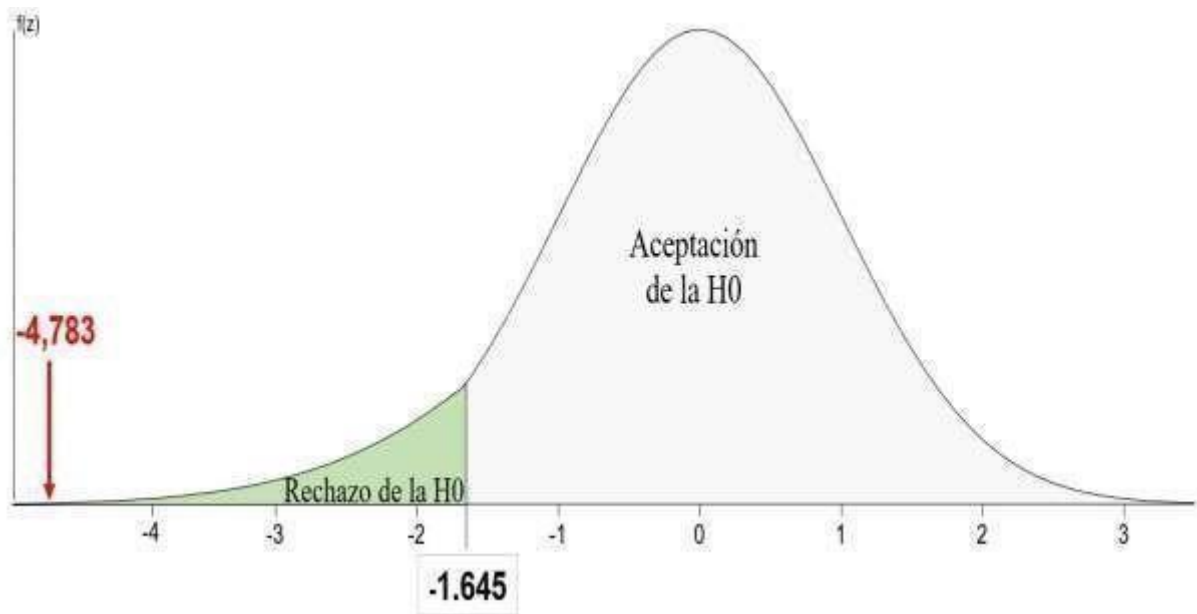
Tabla 12. Prueba^a de Wilcoxon sobre la hipótesis general

	Post - Seguridad de información - Pre - Seguridad de información
Z calculado	-4,783 ^b
Sig. asintótica (bilateral)	0,000

a. Evidencia de rangos con signo de Wilcoxon

b. Se basa en rangos perjudiciales.

Figura 16. Prueba de Wilcoxon sobre la hipótesis general



De acuerdo a la prueba de Wilcoxon dio una significancia de 0,000. La cual es inferior a 0,05. De manera que se impugna la hipótesis nula. Ello se corrobora analizando el valor de Z resultante, el cual fue de -4,783. Este resulta menor que el Z teórico de 1,645. Por lo cual, también se impugna la hipótesis nula, de manera que se permite indicar que el Sistema web mejora la disponibilidad fundada en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.

V. DISCUSIÓN.

Con las deducciones adquiridas en el presente ensayo se indagó y se equiparó el “% de reportes integrados generados”, el “% de reportes confidenciales cedidos correctamente” y “% de reportes entregados en el plazo establecido”, dando un antes y después de efectuar el Sistema web Basado En La ISO/IEC 27001 Para La Gestión De La Seguridad De La Información En La Sociedad P.A PERÚ S.A.C.

Estas conclusiones se asemejan con el ensayo de Nieves (2017), quien a través de su investigación logró un aumento significativo relacionando a las técnicas de gestión. También, se tiene la indagación que ha sido realizada por Arévalo (2015), quien también bosquejó un sistema de gestión alcanzando una mejora.

La participación de Reportes entregados en el plazo determinado, en el cálculo pre-test, la media logró un porcentaje de 79.44% y la ejecución del sistema web la media creció un 96.00%. Estos datos adquiridos muestran una constatación de discrepancia efectiva de 16.56%, en el cual reafirma que la ejecución del sistema se ha logrado incrementar el % de reportes cedidos en el plazo establecido al área externa de la compañía P.A PERÚ S.A.C.

Esta conclusión contrasta con el ensayo de Carrasco (2018), en el cual realizó mero sistema Web en la cual obtuvo un incremento en la eficacia del personal.

El porcentaje de reportes integrados creados, en el cálculo pre-test, la media consiguió un porcentaje de 69.11 % y con la ejecución del sistema web la media incrementó a 96.44 %. Las consecuencias obtenidas muestran una discrepancia efectiva de 27.33%, en la cual se ratifica que con la ejecución del sistema se da un aumento del % de reportes integrados generados al área externa de la compañía P.A PERÚ S.A.C.

Esto tomamos en el ensayo del autor Molano (2017), con relación a los reportes íntegros demuestran a través de un sistema de gestión de la seguridad de la información permita reconocer los peligros o vulnerabilidad que amenaza la empresa, logrando obtener al final un análisis del estado actual de la empresa y así poder pronunciar los encargos que deben estar conforme a la normativa vigente.

El porcentaje de reportes confidenciales cedidos correctamente, en la medición pre-test,

la media consiguió un porcentaje de 71.89 % y con la ejecución del sistema la media tuvo una crecida de 96.89 %. Las consecuencias obtenidas muestran que existe una oposición efectiva de 25.00 %, por lo que se puede ratificar que con la ejecución del sistema se ha alcanzado crecer el % de reportes íntimos entregados correctamente al área externa de la compañía P.A PERÚ S.A.C.

Esto se cogerá del ensayo de Aguirre (2018) con respecto a los reportes íntimos, en el cual demostró que su sistema web respalda a concentrar la información, de manera que los reportes confidenciales se realizan de manera eficaz.

VI. CONCLUSIONES

Las apreciaciones finales son:

1. Se ha estipulado que el “Proporción de reportes confidenciales cedidos educadamente” aplicando un sistema web basado en la ISO/IEC 27001 para la gestión de la seguridad de la investigación en la compañía P.A Perú S.A.C. tuvo un incremento, sin el sistema la media fue de 71.89 % y con uso del sistema la media fue de 96.89 %, recibiendo un incremento de 25.00% de satisfacción para los usuarios con los reportes confidenciales.
2. Se ha fijado que el “Proporción de reportes completados generados” aplicando un sistema web basado en la ISO/IEC 27001 para la gestión de la seguridad de la investigación en la sociedad P.A Perú S.A.C. tuvo un incremento, sin el software web la media es de 69.11 %, pero con uso del software la media es de 96.44 %, percibiendo una mejora de 27.33% de satisfacción para los usuarios con los reportes íntegros.
3. Se ha manifestado que el “Proporción de reportes cedidos en el plazo determinado”, empleando un sistema web basado en la ISO/IEC 27001 para la gestión de la seguridad de la información en la sociedad P.A Perú S.A.C. tuvo un incremento, sin el sistema la media fue de 79.44% y con uso del sistema la media es de 96.00%, lográndose mero mejoramiento de 16.56% de satisfacción para los usuarios con los reportes entregados.

VII. RECOMENDACIONES

En este proyecto podemos ver la importancia de realizar un sistema web para la empresa PA PERU SAC, así ayudando a los usuarios en su gestión de información en la empresa tales como: subir información, saber quiénes fueron los protagonistas de la información que subieron o descargaron, adicionar fecha de entrega, quienes entran al sistema (la hora y fecha que ingresan).

1. poder implementar un módulo de sugerencia donde se le envíe al administrador como una notificación, además de una alerta de aviso cuando las tareas o actividades se van terminar en el tiempo establecido por el administrador de sistema.
2. Se sugiere que para lograr los resultados estadístico más minuciosos se puede pensar extender el periodo de ensayos, para obtener resultados precisos.
3. Se sugiere tomar como muestras cada quincenal, porque constantemente ingresa nuevo personal y se retiran, los usuarios rotan constantemente y es inexacto la cantidad de la muestra.
4. Se recomienda que se habrá un cuadro de dialogo si está conforme con el producto usando el nivel de satisfacción del NPS.

III. REFERENCIA.

- Nieves, A. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013". (Tesis de grado). Institución Universitaria Politécnico Gran colombiano, Colombia.
- Abazi, Blerton.2020. A Novel Approach for Information Security Risk Assessment Maturity Framework Based on ISO 27001. (Tesis de grado). Cornvinus University of Budapest.
- DOTSENJO, Sergiy, ILLIASHENKO, Oleg, KHARCHENKO, Vyacheslav, KAMENSKYI, Sergii, 2019. Integrated Security Management System for Enterprise in Industry 4.0. Published since 1998. Ukraine. Information & Security, vol. 43, no. 3, pp. 294-304. ISSN 0861-5160(print), ISSN 1314-2119(online).
- Holmes, L.; LaHurd, A.; Wasson, E.; McClarin, L.; Dabney, K. Racial and Ethnic Heterogeneity in the Association Between Total Cholesterol and Pediatric Obesity. Int. J. Environ. Res. Public Health 2016, 13, 19. Disponible en: <https://www.mdpi.com/1660-4601/13/1/19>
- CASTILLO PEÑA, Gerardo. Implementación De Un Sistema Web De Gestión Documentaria En La Municipalidad Distrital De Pararin-Provincia RecuayDepartamento De Ancash; 2017. Perú: Universidad Católica Los Ángeles De Chimbote. 2017.
- Arévalo Ascanio, J. G., Bayona Trillos, R. A., & Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información. Revista Tecnura, 19(46), 123-134.doi: 10.14483/udistrital.jour.tecnura.2015. 4.a10
- Bermúdez Molina, Kelly, Bailón Sánchez, Edber. (2015). Análisis En Seguridad Informático Y Seguridad De La Información Basado En La Norma ISO/IEC 27001 - Sistemas De Gestión De Seguridad De La Información Dirigido A Una Empresa De Servicios Financieros. (tesis de grado). Universidad Politécnica Salesiana Sede Guayaquil. Ecuador.
- Nacipucha Cumbe, Julio Cesar. (2019). Análisis Y Diseño Para Un Modelo De Gestión De Seguridad De La Información Basados En Normas ISO/IEC 27001:2013 Para La Empresa ARTEHOGAR En La Ciudad De Guayaquil. (tesis de grado). Universidad de Guayaquil. Ecuador.
- Aquino Quiñonez. J, Martínez Lara, K, Sorto Chávez, A. (2017). Manual de Instalación, Configuración de un Sistema de Gestión y Monitoreo de Redes Informáticas para Pequeñas y Medianas Empresas en El Salvador, utilizando software libre. (tesis de grado). Universidad Tecnológica de El Salvador. El Salvador.

- Guzmán Pacheco, G. (2015). Metodología para la Seguridad de Tecnología de Información y Comunicaciones en la Clínica Ortega. (tesis de grado de Magister). Universidad Nacional del Centro del Perú. Perú.
- Berrio López, J. (2016). Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001. (tesis de grado). Universidad Nacional de Colombia. Colombia.
- Meneses Martínez, A, Ramírez Camargo, E, Merchan Villalba, M, Suarez De La Cruz, Y. (2016). Diseño Del Sistema De Gestión De Seguridad De La Información SGSI Basado En El Estándar Iso 27001, Para Los Procesos Soportados Por El Área De Sistemas En La Cámara De Comercio De Aguachica, Cesar. (tesis de grado). Universidad Francisco de Paula Santander Ocaña. Colombia.
- Uno. Kim HH, Yoo J. Estado actual e investigación sobre la vulnerabilidad web del sistema de control. La Revista Coreana de Comercio Electrónico [Internet]. 31 de mayo de 2019; 24 (2): 15-27. Disponible en: <https://doi.org/10.7838/JSEBS.2019.24.2.015>
- Aguirre, J. (2018). Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C-La Molina. (Tesis para obtener el título profesional de Ingeniería de Sistemas). Universidad César Vallejo, Perú.
- Mirtsch, M., Kinne, J. y Blind, K., "Exploración de la adopción de la norma ISO / IEC 27001 del sistema de gestión de seguridad de la información internacional: un análisis basado en la minería web", en IEEE Transactions on Engineering Management, doi: 10.1109 / TEM. 2020.2977815. Disponible: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9082865&isnumber=4429834>
- Huerta, C. (2020). Sistema de gestión de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019. (Tesis para obtener el grado académico). Universidad Cesar Vallejo. Perú
- Carrasco, R. (2018). Sistema web de matrícula para Business Process Management de la Facultad de Ingenierías de la Universidad Privada Juan Pablo II (Tesis para optar el grado académico de Maestro en Gestión de Tecnologías de Información). Universidad Cesar Vallejo. Perú
- Saber, Mohamed & Arnous, Reham. (2019). An Integrated Framework to Ensure Information Security Over the Internet. International Journal of Computer Applications. Volumen. 178, Pages 13-15, ISSN 0975-887, disponible en: 10.5120/ijca2019919117
- Almutairi, Ohud, Thomas, Nigel, Performance Modelling of the Impact of Cyber Attacks on a Web-based Sales System, Electronic Notes in Theoretical Computer Science, Volumen 353,2020, Pages --- 5-20, ISSN1571-0661, disponible en: <http://www.sciencedirect.com/science/article/pii/S1571066120300712>
- Leiva.R (2016). Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015. (Tesis para obtener el título profesional de Ingeniería de

Sistema). Universidad Nacional Pedro Ruiz Gallo. Perú

- Sheikhpour, Razieh & Modiri, Nasser, A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. Indian Journal of Science and Technology. (2016). 5. 2170-2176, ISSN 0974-6846, disponible en: 10.17485/ijst/2012/v5i3.1.
- Nelli V. Syreyshchikova, Danil Yu. Pimenov, Tadeusz Mikolajczyk, Liviu Moldovan. Information Safety Process Development According to ISO 27001 for an Industrial Enterprise, Procedia Manufacturing, Volumen 32, 2019, Pages 278-285, ISSN 2351-9789, disponible en: <https://doi.org/10.1016/j.promfg.2019.02.215>
- Alqahtani, Rawan, Alqahtani, Fai, Almutlaq, Fay, Alomari, Yazan. Web Based System for Electronic and Electric Devices Maintenance. International Journal of Applied Engineering Research. Reseaech India Publications. vol.15, num.8, pp. 804-811. ISSN 0973-4562
- Dharmalingam Ramalingam, Shivasankarappa Arun, Neelamegam Anbazhagan. A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM, Procedia Computer Science, Volume 134, 2018, Pages 365-370, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2018.07.197>
- Szczepaniuk, Edyta, Szczepaniuk, Hubert, Rokicki, Tomasz, Klepacki, Bogdan, Information security assessment in public administration, Computers & Security, Volume 90, 2020, 101709, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2019.101709>
- Pizzi, Giorgio. Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment, Transportation Research Procedia, Volume 45, 2020, Pages 250-257, ISSN 2352-1465, <https://doi.org/10.1016/j.trpro.2020.03.014>
- Özdemir Sönmez, Ferda. A Conceptual Model for a Metric Based Framework for the Monitoring of Information Security Tasks' Efficiency, Procedia Computer Science, Volumen 160, 2019, Pages 181-188, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2019.09.459>
- Walkowiak, Tomasz, Kamiński, Wojciech. Influence of Data Delivery on Availability of Web Systems, Procedia Engineering, Volumen 178, 2017, Pages 223-232, ISSN 1877-7058, <https://doi.org/10.1016/j.proeng.2017.01.102>.

Anexo 3.

□ Anexo 3.1: Matriz de operacionalización de variables

Tabla 1. Matriz de operacionalización de variables

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Independiente: Sistema Web	Son aquellas aplicaciones de software que puede utilizarse accediendo a un servidor web a través de internet o de una intranet mediante un navegador.	Herramienta que permita mejorar la seguridad de información en la empresa PAC PERU SAC.			Razón
Dependiente: Seguridad de Información	Es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesto. (Baca. 2016)	Proceso en el cual se controla la: confidencialidad, integridad, disponibilidad	Confidencialidad	% Reportes confidenciales entregados correctamente	
			Integridad	% Reportes Integrados generados	
			Disponibilidad	% Reportes entregados en el plazo establecido	

Fuente: elaboración propia de los autores.

□ Anexo 3.2: Indicadores de variables

Tabla 2. Indicadores de variables

OBJETIVO ESPECÍFICO	INDICADOR	DESCRIPCIÓN	TÉCNICA / INSTRUMENTO	TIEMPO EMPLEADO	MODO DE CÁLCULO
Identificar el efecto de un Sistema web en la confidencialidad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.	% Reportes confidenciales entregados correctamente	Este indicador sirve para mejorar la confidencialidad de información de la empresa	Ficha de registro	Diario	$\text{Valor} = \frac{\% \text{ Reportes confidenciales Entregados Correctamente}}{\text{Reportes confidenciales entregados correctamente}} * 100$
Identificar el efecto de un Sistema web en la integridad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.	% Reportes Integrados generados	Este indicador sirve para proteger la integridad de la empresa	Ficha de registro	Diario	$\text{Valor} = \frac{\% \text{ Reportes Integros generados}}{\text{Reportes Integros generados}} * 100$
Identificar el efecto de un Sistema web en la disponibilidad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C	% Reportes entregados en el plazo establecido	Este indicador sirve para aumentar la disponibilidad de la información, a los usuarios con permiso.	Ficha de registro	Diario	$\text{Valor} = \frac{\% \text{ Reportes entregados en el plazo establecido}}{\text{Reportes entregados en el plazo establecido}} * 100$

Fuente: elaboración propia de los autores.

Anexo 4. Instrumentos de recolección de datos

DIMENSION: DISPONIBILIDAD

¿La información se encuentra disponible a la disposición que uno requiere?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿La información en donde se guarda se Encuentra activa en todo momento?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- Parcialmente de Acuerdo ()
- d. Totalmente de acuerdo ()

¿Se cuenta en todo momento con la disponibilidad de la información?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿Cuenta con una información de respaldo por si se llegara a borrar la información?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿El tiempo de recuperación de un sistema ante una incidencia es rápido?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

DIMENSION: INTEGRIDAD

¿Cada usuario realiza el cambio de contraseña?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿Cuentan con antivirus correcto para la integridad de datos?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿La empresa P.A PERU S.A.C realiza capacitaciones de ataques de virus?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿La documentación en físico que usted maneja se encuentra resguardado?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿Se realiza el bloqueo automático cuando se deja me usar?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

DIMENSION: CONFIDENCIALIDAD

¿La empresa P.A PERU S.A.C cuenta con políticas de seguridad de información?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿La empresa P.A PERU S.A.C capacita a los trabajadores del área externa sobre la política de información?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿La empresa P.A PERU S.A.C capacita a sus trabajadores sobre la calificación de los activos de información y su importancia?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿Hacen respaldo de información?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

¿Existen accesos restringidos en el área para ceder la información?

- a. Totalmente en desacuerdo ()
- b. Parcialmente en desacuerdo ()
- c. Indiferente ()
- d. Parcialmente de Acuerdo ()
- e. Totalmente de acuerdo ()

MATRIZ DE CONSISTENCIA

Titulo: Sistema Web Basado en la ISO/IEC 27001 para la gestión de la información en la empresa P.A Perú S.A.C.

Problema	Objetivos	Hipótesis	Variable	Dimensiones	Indicador	Metodología
PG: ¿Cómo influye la ausencia de un Sistemas Web para la gestión de la información utilizando la ISO/IEC27001 en la empresa PA PERU SAC?	Determinar la mejora de un Sistemas Web para gestión de la seguridad de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC.	Implementar un sistema web para la gestión de la seguridad de información basado en la ISO/IEC 27001, mejorando la confiabilidad integridad y disponibilidad de la información	Independiente: Sistema Web			Tipo de investigación: Aplicada Diseño de la investigación: Experimental Pre-experimental
PE1: ¿Cómo afecta la ausencia de confiabilidad de un Sistemas Web para la gestión de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC?	Identificar el efecto de un Sistema web en la confiabilidad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C.	Implementar un sistema web para la gestión de seguridad de información basado en la ISO/IEC 27001 mejorando la confiabilidad en la empresa PA PERÚ SAC	Dependiente: Seguridad de Información	confiabilidad	$\frac{\% \text{ Reportes confidenciales Entregados Correctamente}}{\text{Reportes confidenciales entregados correctamente}} \times 100$ <p style="text-align: center;">Valor= _____ *100</p> <p style="text-align: center;">Total de reportes</p>	Técnica Fichaje Instrumento Ficha de registro
PE2: ¿Cómo afecta la ausencia de integridad de un Sistemas Web para la gestión de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC?	Identificar el efecto de un Sistema web en la integridad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C...	Implementar un sistema web para la gestión de seguridad de información basado en la ISO/IEC 27001 mejorando la integridad en la empresa PA PERÚ SAC		Integridad	$\frac{\% \text{ Reportes integros generados}}{\text{Reportes integros generados}} \times 100$ <p style="text-align: center;">Valor= _____ *100</p> <p style="text-align: center;">Total de reportes</p>	Metodología aplicada Programación Extrema XP
PE2: ¿Cómo afecta la ausencia de disponibilidad de un Sistemas Web para la gestión de la información utilizando la ISO/IEC 27001 para la empresa PA PERU SAC?	Identificar el efecto de un Sistema web en la disponibilidad basado en la ISO/IEC 27001 para gestionar la seguridad de información en la empresa P.A PERU S.A.C...	Implementar un sistema web para la gestión de seguridad de información basado en la ISO/IEC 27001 mejorando la disponibilidad en la empresa PA PERÚ SAC		Disponibilidad	$\frac{\% \text{ Reportes entregados en el plazo establecido}}{\text{Reportes entregados en el plazo establecido}} \times 100$ <p style="text-align: center;">Valor = _____ * 100</p> <p style="text-align: center;">Total de reportes</p>	

Anexo 7. Autorización de aplicación del instrumento firmado por la entidad



Lima, 14 de diciembre de 2020

"P.A. PERU S.A.C"

SRES: UNIVERSIDAD CÉSAR VALLEJO

ATENCIÓN:

MS. DANIEL ORLANDO ANGELES PINILLOS

COORDINADOR DE LA ESCUELA DE INGENIERÍA DE SISTEMAS

MS. RICARDO MANUEL GUEVARA RUIZ

ASESOR DE PROYECTO DE INVESTIGACIÓN

PRESENTE

ASUNTO: AUTORIZACIÓN DEL PROYECTO DE INVESTIGACIÓN

Ante todo, reciban un cordial saludo y por medio de la presente hacer de su conocimiento que los alumnos Angel Cesar Cahuana Prado y Alexander Elin Cahuana Romari, estudiantes de la Escuela de Ingeniería de Sistemas, han sido aceptado satisfactoriamente para realizar su investigación en nuestra institución, la investigación a desarrollarse se denomina "Sistemas Web basado en la ISO/IEC 27001 para automatizar la seguridad de informaciones la empresa P.A PERU S.A.C".

Sin más a que hacer referencia,

Atentamente:

A handwritten signature in black ink, appearing to read "Hernan Moreno", is written over a horizontal line.

Hernan Moreno
Encargado del área de Sistemas

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	Dimensión: Confidencialidad	Si	No	Si	No	Si	No	
1	Indicadores: % Reporte confidenciales entregados correctamente <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes confidenciales entregados correctamente</p> <p>Valor= _____ *100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		
	Dimensión: Integridad	Si	No	Si	No	Si	No	
2	% Reportes integrados generados <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes Integros generados</p> <p>Valor= _____ *100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		
	Dimensión: Disponibilidad	Si	No	Si	No	Si	No	
3	% Reportes entregados en el plazo establecido <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes entregados en el plazo establecido</p> <p>Valor = _____ * 100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador. Dr./ Mg: Jauregui Briceno, Carlos DNI: 18122267

Especialidad del validador: Ing. de Computacion y Sistemas

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

..24.. de Junio del 2021

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



FIRMA DEL EXPERTO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	Dimensión: Confidencialidad	Si	No	Si	No	Si	No	
1	Indicadores: % Reporte confidenciales entregados correctamente <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes confidenciales entregados correctamente</p> <p>Valor= _____ *100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		
	Dimensión: Integridad	Si	No	Si	No	Si	No	
2	% Reportes integrados generados <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes Integros generados</p> <p>Valor= _____ *100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		
	Dimensión: Disponibilidad	Si	No	Si	No	Si	No	
3	% Reportes entregados en el plazo establecido <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes entregados en el plazo establecido</p> <p>Valor = _____ * 100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador. Dr./ Mg: MENENDEZ MUERAS, ROSA DNI:10246770
Especialidad del validador: Ingeniera de Sistemas

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

..... de diciembre del 2020

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	Dimensión: Confidencialidad	Si	No	Si	No	Si	No	
1	Indicadores: % Reporte confidenciales entregados correctamente <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes confidenciales entregados correctamente</p> <p>Valor= _____ *100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		
	Dimensión: Integridad	Si	No	Si	No	Si	No	
2	% Reportes integrados generados <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes Integros generados</p> <p>Valor= _____ *100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		
	Dimensión: Disponibilidad	Si	No	Si	No	Si	No	
3	% Reportes entregados en el plazo establecido <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Reportes entregados en el plazo establecido</p> <p>Valor = _____ * 100</p> <p style="text-align: center;">Total de reportes</p> </div>	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador. Dr./ Mg: ARADIEL CASTANEDA, HILARIO. DNI: 08576568

Especialidad del validador:

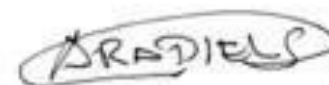
¹Pertinencia: El ítem corresponde al concepto teórico formulado.

.....30. de diciembre del 2020

²Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

³Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



FIRMA DEL

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: MENÉNDEZ MUERAS, ROSA

Título y/o Grado:

Doctor ... () Magister ...(X) Ingeniero () OtrosEspecifique. Fecha:

26/06/2021

TÍTULO DE TESIS

Sistema Web Basado en la ISO/IEC 27001 para la gestión de la información en la empresa P.A
Perú S.A.C.

Tabla de Evaluación de Expertos para la elección de la metodología
Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas con puntuaciones especificadas al final de la tabla.

Evaluar con la siguiente calificación:

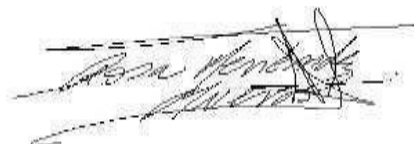
ITEMS	PREGUNTAS	MARCO DE TRABAJO AGIL			
		XP	SCRUM	KANBAN	OBSERVACIONES
1	Más enfocada en procesos	3	2	2	
2	Resultados Rápidos	3	3	2	
3	Desarrollo iterativo	3	3	3	
4	Capaz de adaptarse a cambios de requisitos	3	3	3	
5	Implementa las necesidades de la aplicación.	3	3	3	
	TOTAL	15	14	13	

1: Malo

2: Regular

3: Bueno

Sugerencias: _____



FIRMA DEL EXPERTO

EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: JALIREGUI BRICENO, CARLOS EDUARDO

Título y/o Grado:

Doctor ... () Magister ... (x) Ingeniero () Otros Especifique.

Fecha: 24 / 08 / 2021

TÍTULO DE TESIS

Sistema Web Basado en la ISO/IEC 27001 para la gestión de la información en la empresa P.A Perú S.A.C.

Tabla de Evaluación de Expertos para la elección de la metodología

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas con puntuaciones especificadas al final de la tabla.

ITEMS	PREGUNTAS	MARCO DE TRABAJO AGIL			
		XP	SCRUM	KANBAN	OBSERVACIONES
1	Más enfocada en procesos	3	2	1	
2	Resultados Rápidos	3	2	1	
3	Desarrollo iterativo	2	1	3	
4	Capaz de adaptarse a cambios de requisitos	2	3	1	
5	Implementa las necesidades de la aplicación.	3	2	1	
	TOTAL	13	10	7	

Evaluar con la siguiente calificación:

1: Malo

2: Regular

3: Bueno

Sugerencias: _____



FIRMA DEL EXPERTO

EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: ...ARADIEL CASTANEDA, HILARIO

Título y/o Grado:

Doctor ... Magister ... Ingeniero () Otros.....Especifique.

Fecha: 30 ___/___06___/___21___

TÍTULO DE TESIS

Sistema Web Basado en la ISO/IEC 27001 para la gestión de la información en la empresa P.A Perú S.A.C.

Tabla de Evaluación de Expertos para la elección de la metodología

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas con puntuaciones especificadas al final de la tabla.

ITEMS	PREGUNTAS	MARCO DE TRABAJO AGIL			
		XP	SCRUM	KANBAN	OBSERVACIONES
1	Más enfocada en procesos	1	3	2	
2	Resultados Rápidos	1	3	2	
3	Desarrollo iterativo	1	3	2	
4	Capaz de adaptarse a cambios de requisitos	1	3	2	
5	Implementa las necesidades de la aplicación.	1	3	2	
	TOTAL	5	15	10	

Evaluar con la siguiente calificación:

1: Malo

2: Regular

3: Bueno

Sugerencias: _____



Validación del Instrumento de Medición del Indicador: Margen Operacional

EVALUACIÓN DE METODOLOGÍA DE DESARROLLO DE SOFTWARE

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: **MENÉNDEZ MUERAS, ROSA**

Título y/o Grado:

Doctor ... Magister ... Ingeniero () Otros Especifique.

Fecha: 26/06/2021

TÍTULO DE TESIS

Sistema Web Basado en la ISO/IEC 27001 para la gestión de la información en la empresa P.A Perú S.A.C.

Tabla de Evaluación de Expertos para la elección de la metodología

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de preguntas con puntuaciones especificadas al final de la tabla.



ITEMS	PREGUNTAS	MARCO DE TRABAJO AGIL			
		XP	SCRUM	KANBAN	OBSERVACIONES
1	Más enfocada en procesos	3	2	2	
2	Resultados Rápidos	3	3	2	
3	Desarrollo iterativo	3	3	3	
4	Capaz de adaptarse a cambios de requisitos	3	3	3	
5	Implementa las necesidades de la aplicación.	3	3	3	
	TOTAL	15	14	13	

Evaluar con la siguiente calificación:

1: Malo

2: Regular

3: Bueno

Sugerencias: _____

FIRMA DEL EXPERTO

Ficha de Observación

FICHA DE OBSERVACIÓN	
Observador:	Cahuana Prado, Angel Cesar Cahuana Román, Alexander Elin
Empresa donde se investiga:	EMPRESA P.A PERÚ S.A.C.
Indicador Utilizado:	% Reportes confidenciales entregados correctamente
Periodo de la observación Pre test:	01/05/2021 - 31/05/2021
Periodo de la observación Pos test:	01/06/2021 - 31/06/2021

Informes diarios	PRETEST: Mayo 2021			POSTEST: Junio 2021		
	Reportes confidenciales entregados correctamente	Total de reportes	Resultados %	Reportes confidenciales entregados correctamente	Total de reportes	Resultados %
1	4	5	80.00	6	6	100.00
2	5	6	83.33	5	5	100.00
3	5	5	100.00	5	5	100.00
4	4	5	80.00	4	4	100.00
5	3	5	60.00	5	6	83.33
6	4	6	66.67	6	6	100.00
7	2	4	50.00	4	4	100.00
8	4	5	80.00	5	5	100.00
9	3	4	75.00	4	5	80.00
10	4	5	80.00	6	6	100.00
11	4	6	66.67	6	6	100.00
12	2	4	50.00	5	5	100.00
13	3	5	60.00	6	6	100.00
14	2	4	50.00	5	5	100.00
15	4	4	100.00	4	5	80.00
16	3	4	75.00	4	4	100.00
17	3	5	60.00	5	5	100.00
18	5	5	100.00	4	5	80.00
19	6	6	100.00	4	4	100.00
20	4	5	80.00	6	6	100.00
21	3	6	50.00	5	5	100.00
22	2	4	50.00	6	6	100.00
23	5	6	83.33	6	6	100.00
24	4	6	66.67	5	6	83.33
25	4	6	66.67	5	5	100.00
26	3	5	60.00	6	6	100.00
27	4	4	100.00	4	4	100.00
28	5	6	83.33	6	6	100.00
29	3	6	50.00	6	6	100.00
30	3	6	50.00	5	5	100.00
Promedio:	3.67	5.10	71.89	5.10	5.27	96.89

FICHA DE OBSERVACIÓN	
Observador:	Cahuana Prado, Angel Cesar Cahuana Román, Alexander Elin
Empresa donde se investiga:	EMPRESA P.A PERÚ S.A.C.
Indicador Utilizado:	% Reportes Integrados generados
Periodo de la observación Pre test:	01/05/2021 - 31/05/2021
Periodo de la observación Pos test:	01/06/2021 - 31/06/2021

Informes diarios	PRETEST: Mayo 2021			POSTEST: Junio 2021		
	Reportes Integrados generados	Total de reportes	Resultados %	Reportes Integrados generados	Total de reportes	Resultados %
1	4	6	66.67	5	5	100.00
2	4	5	80.00	5	5	100.00
3	4	5	80.00	4	5	80.00
4	3	5	60.00	6	6	100.00
5	4	5	80.00	5	6	83.33
6	3	5	60.00	6	6	100.00
7	4	4	100.00	5	5	100.00
8	5	6	83.33	5	5	100.00
9	4	6	66.67	4	5	80.00
10	4	4	100.00	4	4	100.00
11	3	4	75.00	5	5	100.00
12	2	4	50.00	6	6	100.00
13	2	5	40.00	5	6	83.33
14	3	5	60.00	5	5	100.00
15	2	4	50.00	4	4	100.00
16	5	6	83.33	4	4	100.00
17	4	5	80.00	5	6	83.33
18	3	5	60.00	3	3	100.00
19	4	6	66.67	5	5	100.00
20	5	6	83.33	5	5	100.00
21	4	6	66.67	6	6	100.00
22	3	4	75.00	5	5	100.00
23	4	6	66.67	5	6	83.33
24	2	4	50.00	3	3	100.00
25	2	4	50.00	5	5	100.00
26	4	5	80.00	4	4	100.00
27	2	4	50.00	5	5	100.00
28	3	5	60.00	6	6	100.00
29	5	6	83.33	3	3	100.00
30	4	6	66.67	5	5	100.00
Promedio:	3.50	5.03	69.11	4.77	4.97	96.44

FICHA DE OBSERVACIÓN	
Observador:	Cahuana Prado, Angel Cesar Cahuana Román, Alexander Elin
Empresa donde se investiga:	EMPRESA P.A PERU S.A.C.
Indicador Utilizado:	% Reportes entregados en el plazo establecido
Periodo de la observación Pre test:	01/05/2021 - 31/05/2021
Periodo de la observación Pos test:	01/06/2021 - 31/06/2021

Informes diarios	PRETEST: Mayo 2021			POSTEST: Junio 2021		
	Reportes entregados en el plazo establecido	Total de reportes	Resultados %	Reportes entregados en el plazo establecido	Total de reportes	Resultados %
1	4	5	80.00	5	5	100.00
2	5	5	100.00	5	5	100.00
3	3	5	60.00	4	5	80.00
4	4	5	80.00	6	6	100.00
5	5	6	83.33	5	6	83.33
6	3	4	75.00	6	6	100.00
7	5	6	83.33	5	5	100.00
8	5	6	83.33	5	6	83.33
9	5	6	83.33	6	6	100.00
10	4	4	100.00	5	5	100.00
11	2	4	50.00	5	5	100.00
12	3	4	75.00	6	6	100.00
13	4	5	80.00	5	6	83.33
14	5	5	100.00	5	5	100.00
15	3	4	75.00	4	4	100.00
16	6	6	100.00	4	4	100.00
17	5	5	100.00	5	6	83.33
18	4	5	80.00	6	6	100.00
19	5	6	83.33	5	5	100.00
20	3	6	50.00	5	5	100.00
21	4	6	66.67	6	6	100.00
22	3	4	75.00	5	5	100.00
23	4	6	66.67	5	6	83.33
24	3	4	75.00	6	6	100.00
25	3	4	75.00	5	5	100.00
26	3	5	60.00	5	6	83.33
27	4	4	100.00	6	6	100.00
28	5	5	100.00	6	6	100.00
29	5	6	83.33	5	5	100.00
30	3	5	60.00	5	5	100.00
Promedio:	4.00	5.03	79.44	5.20	5.43	96.00

**SISTEMA WEB BASADO EN LA ISO/IEC 27001
PARA LA GESTION DE LA INFORMACION EN
LA EMPRESA P.A PERÚ S.A.C. BAJO LA
METODOLOGIA XP**

Se mostrará a continuación como la solución de la propuesta el desarrollo del sistema webbasado en la ISO/IEC 27001 para la gestión de la información en la empresa P.A PERÚ S.A.C. a través de la Metodología XP que está dividida en 4 fases:

Fase 1: Planificar el sistema web

- Acta de reunión con el grupo de interés
Aquí se mostrará el modelo sin las firmas del acta de reunión, en los anexos se mostrarán las firmas con las actas de reunión establecidas en cada fecha.
- Historias de usuarios

HISTORIA DE USUARIO	
Número: 1	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz de Inicio de sesión	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 01
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario necesitamos iniciar sesión para ingresar al sistema web	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 2	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz Actividades	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario se visualiza la carga y la descarga de los archivos que realiza cada uno	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 3	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz Mis Archivos	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario se visualiza la carga y la descarga de los archivos que realiza cada uno	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 4	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz Archivos Recibidos	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario se visualiza la carga y la descarga de los archivos que realiza cada uno	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 5	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz de Usuarios	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario se visualiza la carga y la descarga de los archivos que realiza cada uno	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 6	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz Agregar Usuario	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario se visualiza la carga y la descarga de los archivos que realiza cada uno	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 7	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz Roles	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario se visualiza la carga y la descarga de los archivos que realiza cada uno	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 8	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz Agregar Roles	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario se visualiza la carga y la descarga de los archivos que realiza cada uno	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 9	Usuario: Administrador, Usuario
Nombre de la Historia: Interfaz Auditoria de Usuarios	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Bajo
Días estimados: 1 día	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario se visualiza la carga y la descarga de los archivos que realiza cada uno	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 10	Usuario: Administrador, Vendedor
Nombre de la Historia: Interfaz Auditoria de Archivos	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Medio
Días estimados: 2 días	Iteración asignada: 02
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador y usuario queremos visualizar todos los documentos que se viene subiendo por parte del usuario y el administrador	
Observaciones: El producto debe estar previamente registrado en la base de datos.	

HISTORIA DE USUARIO	
Número: 11	Usuario: Administrador, Vendedor
Nombre de la Historia: Interfaz Dashboards Indicadores	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Medio
Días estimados: 2 días	Iteración asignada: 01
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador queremos registrar los nuevos usuarios y ver estado de actividad	
Observaciones: El administrador y usuario deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 12	Usuario: Administrador, Vendedor
Nombre de la Historia: Interfaz Resultado en tabla	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Medio
Días estimados: 2 días	Iteración asignada: 01
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador dar permiso como creación eliminar etc.	
Observaciones: El administrador y vendedor deben estar previamente registrados en la base de datos.	

HISTORIA DE USUARIO	
Número: 13	Usuario: Administrador, Vendedor
Nombre de la Historia: Interfaz Cambiar contraseña	
Prioridad en Negocio: Alta	Riesgo en desarrollo: Medio
Días estimados: 2 días	Iteración asignada: 01
Programador responsable: Cahuana prado angel, Cahuana Roman Alexander	
Descripción: Como administrador dar permiso como creación eliminar etc.	
Observaciones: El administrador y vendedor deben estar previamente registrados en la base de datos.	

•Plan de iteración

ITERACIÓN	N° HISTORIA	NOMBRE DE LA HISTORIA
ITERACIÓN 1	1	Interfaz de Iniciar sesión
	2	Interfaz de Actividades
ITERACIÓN 2	3	Interfaz de Mis archivos
ITERACIÓN 3	4	Interfaz de Archivos Recibidos
ITERACIÓN 4	5	Interfaz de Usuario
ITERACIÓN 5	6	Interfaz de Agregar Usuario
ITERACIÓN 6	7	Interfaz de Roles
ITERACIÓN 7	8	Interfaz de Agregar Rol
ITERACIÓN 8	9	Interfaz de Auditoria de Usuarios
	10	Interfaz de Auditoria de Archivos
ITERACIÓN 9	11	Interfaz de Dashboard indicadores
	12	Interfaz de Dashboard Resultado en Tabla
ITERACIÓN 10	13	Interfaz de Cambiar Usuario

- Velocidad de Proyecto

N°	HISTORIA DE USUARIO	TIEMPO ESTIMADO (DÍAS)
1	Interfaz de Iniciar sesión	1
2	Interfaz de Actividades	1
3	Interfaz de Mis archivos	2
4	Interfaz de Archivos Recibidos	2
5	Interfaz de Usuario	1
6	Interfaz de Agregar Usuario	1
7	Interfaz de Roles	1
8	Interfaz de Agregar Rol	1
9	Interfaz de Auditoria de Usuarios	1
10	Interfaz de Auditoria de Archivos	1
11	Interfaz de Dashboard indicadores	1
12	Interfaz de Dashboard Resultado en Tabla	1
13	Interfaz de Cambiar Usuario	2

- Roles asignados

ROLES	RESPONSABLES
PROGRAMADOR	CAHUANA ROMAN, ALEXANDER ELIN
CLIENTE	PA PERU SAC
TESTER	CAHUANA ROMAN, ALEXANDER ELIN
TRACKER	CAHUANA PRADO, ANGEL CESAR
GESTOR	CAHUANA PRADO, ANGEL CESAR

Plan de entrega

N° HISTORIA	NOMBRE DE LA HISTORIA	ITERACIÓN	PRIORIDAD	DÍAS ESTIMADOS	FECHA INICIO	FECHA FIN
1	Interfaz de Iniciar sesión	1	Alta	1	2/06/2021	2/06/2021
2	Interfaz de Actividades	1	Alta	1	3/06/2021	3/06/2021
3	Interfaz de Mis archivos	2	Alta	2	4/05/2021	5/06/2021
4	Interfaz de Archivos Recibidos	3	Alta	2	7/06/2021	8/06/2021
5	Interfaz de Usuario	4	Alta	1	9/06/2021	9/06/2021
6	Interfaz de Agregar Usuario	5	Alta	1	10/06/2021	10/06/2021
7	Interfaz de Roles	6	Alta	1	11/06/2021	11/06/2021
8	Interfaz de Agregar Rol	7	Alta	1	12/06/2021	12/06/2021
9	Interfaz de Auditoria de Usuarios	8	Alta	1	14/06/2021	14/06/2021
10	Interfaz de Auditoria de Archivos	8	Alta	1	15/06/2021	15/06/2021
11	Interfaz de Dashboard indicadores	9	Alta	1	16/06/2021	16/06/2021
12	Interfaz de Dashboard Resultado en Tabla	9	Alta	1	17/06/2021	17/06/2021
13	Interfaz de Cambiar Usuario	10	Alta	2	18/06/2021	19/06/2021

Fase 2: Diseñar el sistema web

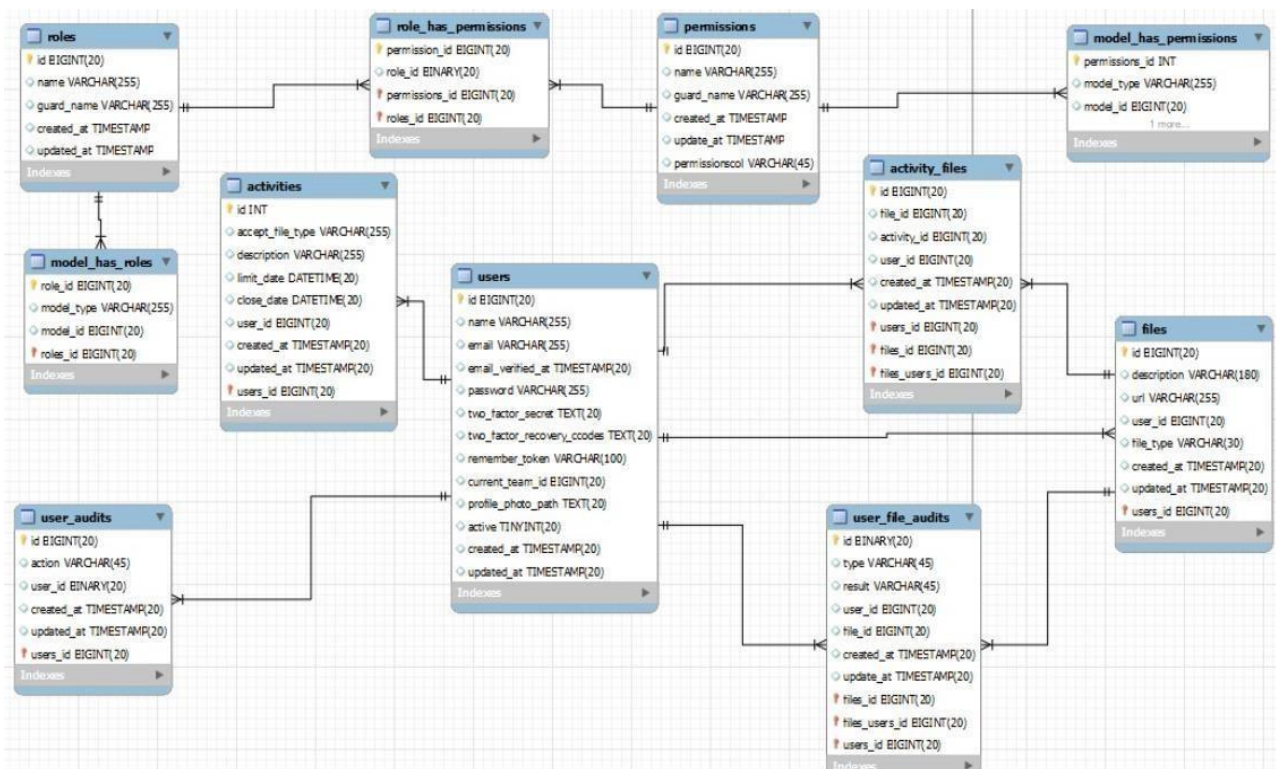
•Metáfora del sistema

El diseño del sistema web se va a realizar durante el desarrollo, donde se tendrá en cuenta todos los cambios y actualizaciones de los diseños, con la ayuda del diseño de CRC.

El sistema web estará enfocado en la gestión de la información en la empresa P.A PERUS.A.C, donde el objetivo principal es lograr la eficiencia en la gestión de los usuarios.

El sistema será desarrollado en el lenguaje de programación PHP, JavaScript y contará con el motor de base de datos MYSQL.

El modelo de base de datos estará desarrollado con la herramienta MYSQL, en la cual se importarán los datos de los prospectos, para las consultas de datos de catálogo de producto

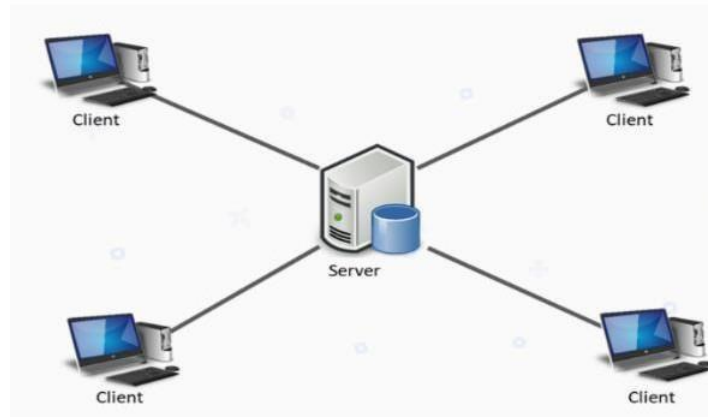


•Arquitectura del Sistema

El software adoptará una arquitectura de tres niveles, que no es más que una especialización de la arquitectura cliente-servidor donde la carga se divide en tres partes (o capas) con un reparto claro de funciones a continuación se definirá cómo se llevará a cabo este reparto:

- Una capa para la presentación (interfaz de usuario).
- Otra para el cálculo (donde se encuentra modelado el negocio)
- Y otra para el almacenamiento (persistencia). Una capa solamente tiene relación con la siguiente.

Figura 9. Arquitectura del sistema



•Tarjeta de CRC

ROLES	
Responsabilidades: Atributos: id_bigint name guard_name created_at updated_at	Colaboradores: Model_has_roles, Role_has_permissions
Operación: Crear Modificar	

PERMISOS

Responsabilidades:**Atributos:**

id_bigint
name
guard_name
created_at
updated_at
permissionscol

Colaboradores:

Role_has_permissions,
Model_has_permissions

Operación:

Crear
Modificar
eliminar

USUARIO

Responsabilidades:**Atributos:**

id_bigint
name
email_veritied_at
password
two_factor_secret
two_fator_recovery_ccodes
remember_token
current_team_id
profile_photo_path
active
created_at
update_at

Colaboradores:

Model_has_roles, Role_has_permissions

Operación:

Editar
Registro
Eliminar

FILE

Responsabilidades:**Atributos:**

id_bigint
description
url
user_id
file_type
created_at
updated_at
users_id

Colaboradores:

Activity_files, user_file_audits

Operación:

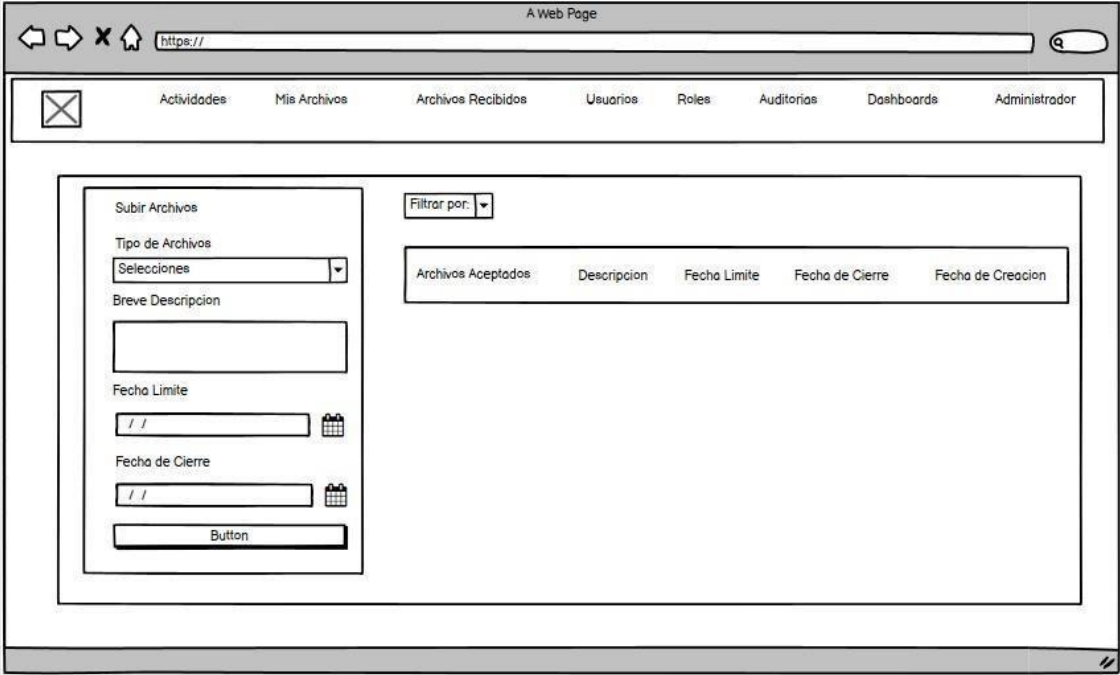
Crear
Descargar
cargar

User_file_audits	
Responsabilidades: Atributos: id_bigint type result user_id file_id created_at update_at file_id file_users_id users_id	Colaboradores: Users, user_file_audits
Operación: Crear Descargar cargar	

- Prototipos de entrega

Prototipo de Inicio de sesion

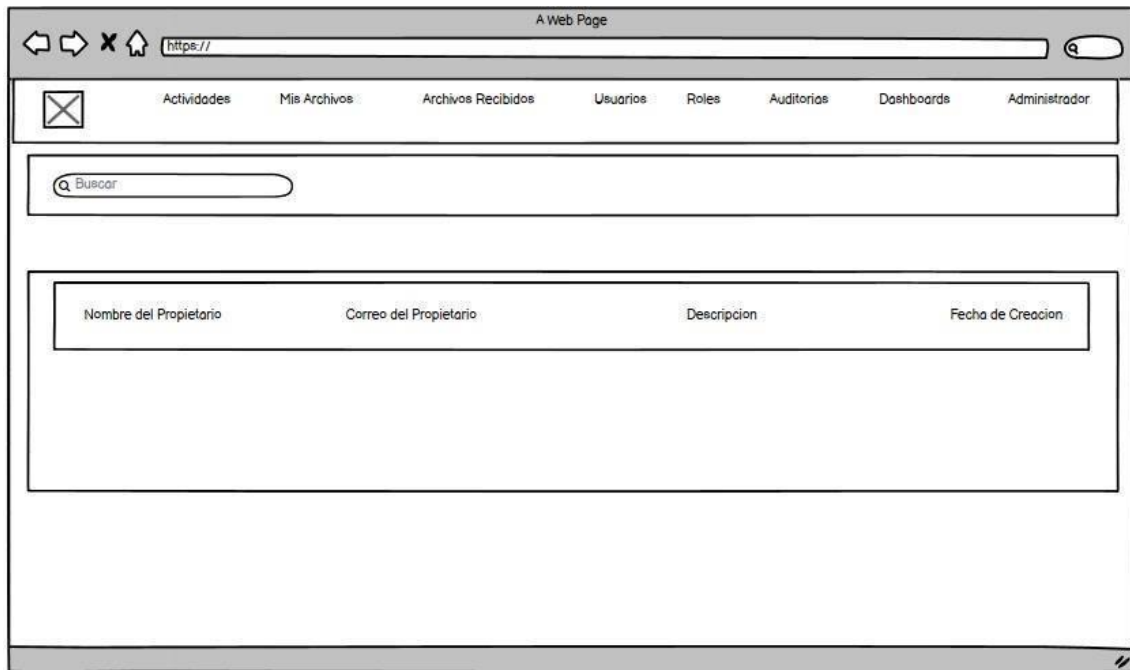
Prototipo de Actividades



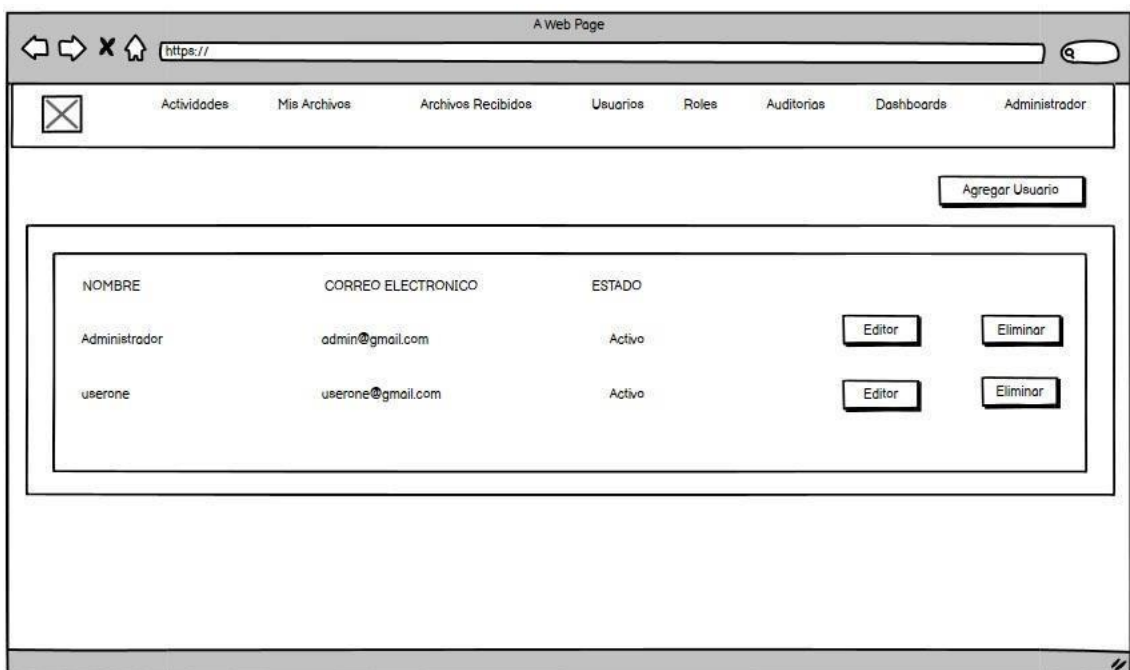
Prototipo Mis Archivos



Prototipo Archivos Recibidos



Prototipo de Usuarios



Prototipo Agregar Usuarios

A Web Page

https://

Actividades Mis Archivos Archivos Recibidos Usuarios Roles Auditorias Dashboards Administrador

Rol de Usuario
ComboBox

Nombre

Email

Contraseña

Confirmar Contraseña

Activo
Activo

Registro

Prototipo Roles

AGREGAR ROL

ID	NOMBRE		
2	USUARIO	Editor	Eliminar
1	Administrador	Editor	Eliminar

Prototipo Agregar Rol

A Web Page

https://

Actividades Mis Archivos Archivos Recibidos Usuarios Roles Auditorias Dashboards Administrador

Nombre del Rol

ROL

Permiso

<input type="checkbox"/> Ver Usuario	<input type="checkbox"/> Crear Usuarios	<input type="checkbox"/> Eliminar Usuario
<input type="checkbox"/> Ver Roles	<input type="checkbox"/> Crear Rol	<input type="checkbox"/> Eliminar Rol
<input type="checkbox"/> Ver Archivos	<input type="checkbox"/> Ver Archivos Recibidos	<input type="checkbox"/> Ver Auditoria

Eliminar

Prototipo Cambiar Contraseña

A Web Page

https://

Actividades Mis Archivos Archivos Recibidos Usuarios Roles Auditorias Dashboards Administrador

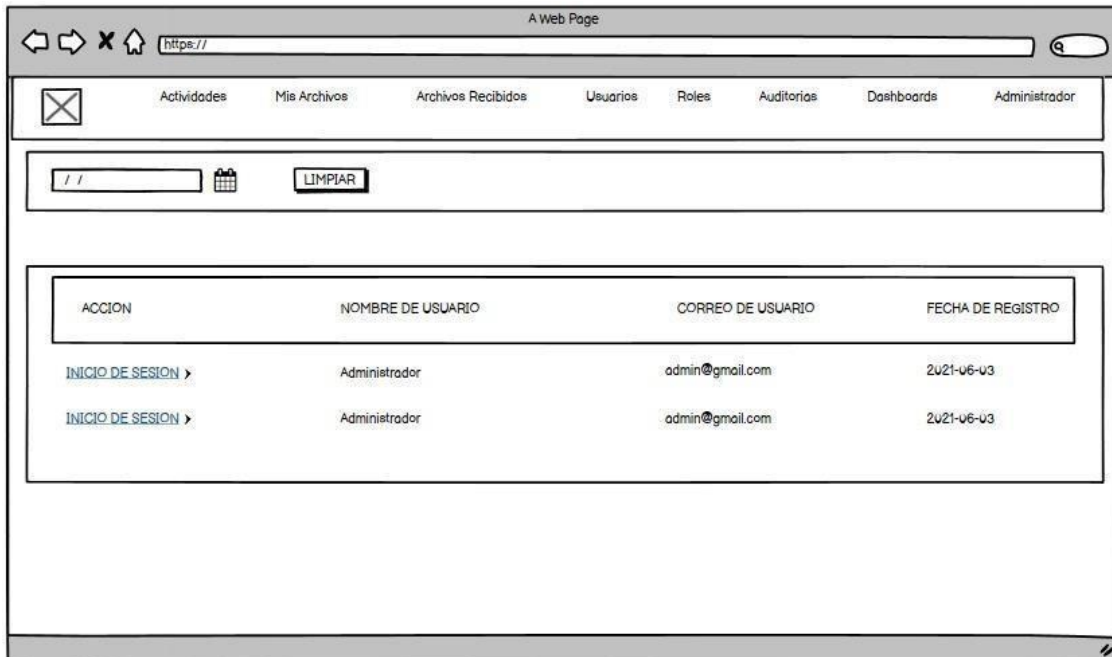
Actual Contraseña

Nueva contraseña

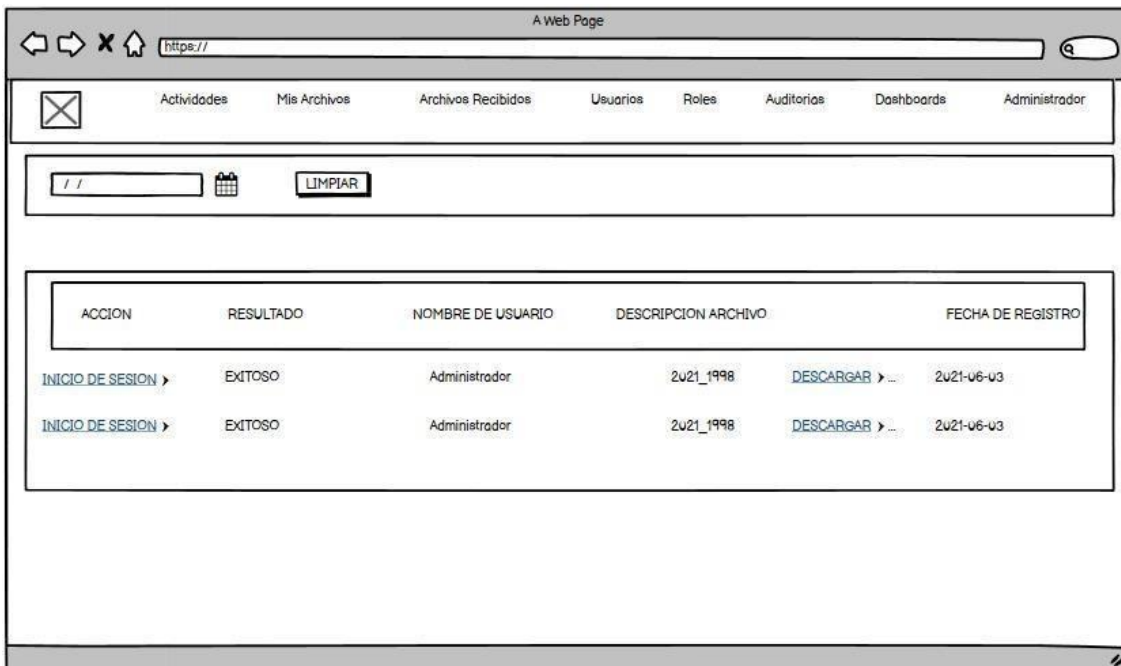
Confirmar Nueva Contraseña

Cancelar Aceptar

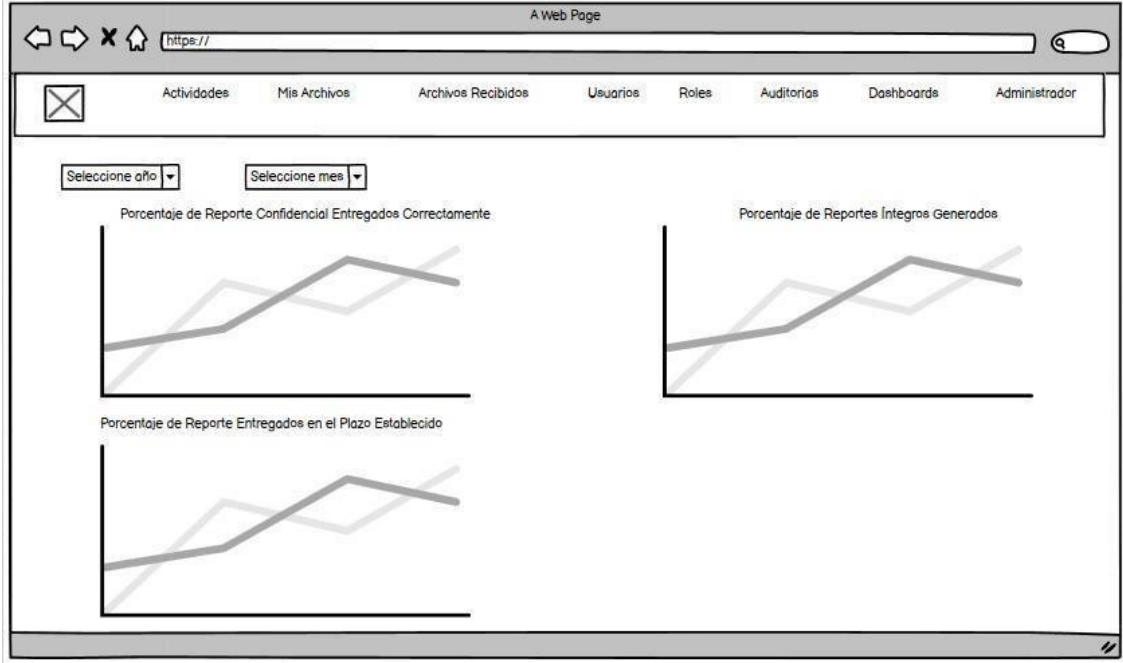
Prototipo Auditoria Usuario



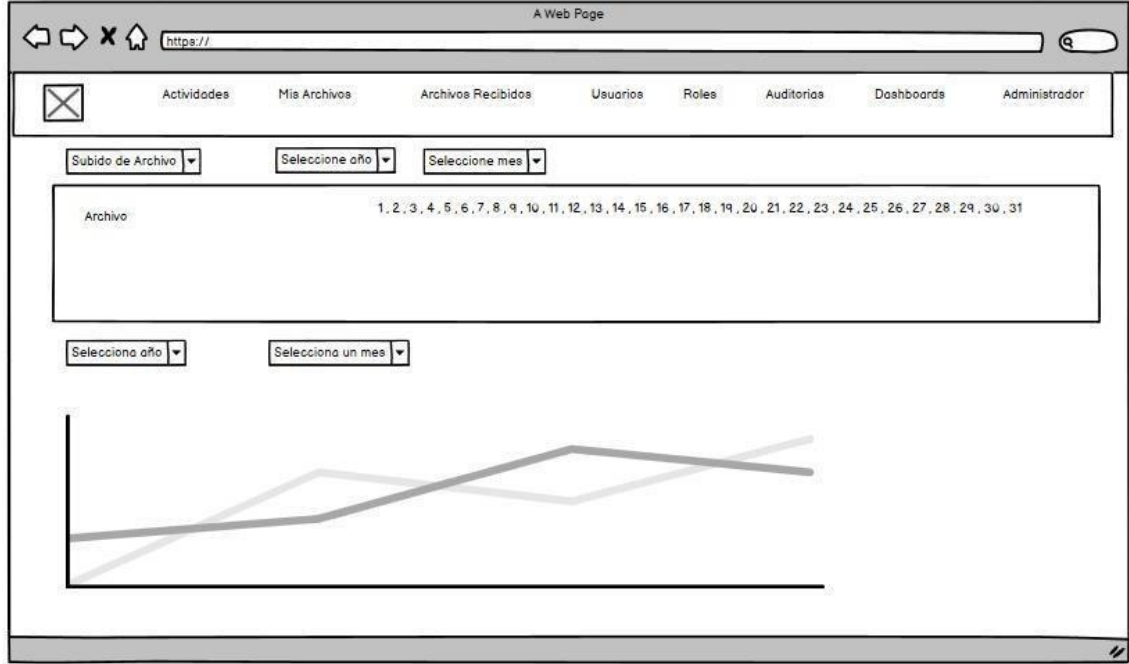
Prototipo Auditoria de Archivos



Prototipo Cuadro de Mando



Prototipo Cuadro de mando 2



Fase 3: Desarrollar el sistema web

- Disponibilidad del cliente

Una de las prioridades en el marco de trabajo de XP es que a lo largo del desarrollo del proyecto se mantenga una excelente comunicación con el usuario, ya que él es una pieza muy importante en el proyecto, puesto que aporta en realizar las historias de usuarios, dar seguimiento a los tiempos que se establecieron y detalla todos los requerimientos que la aplicación web va a tener.

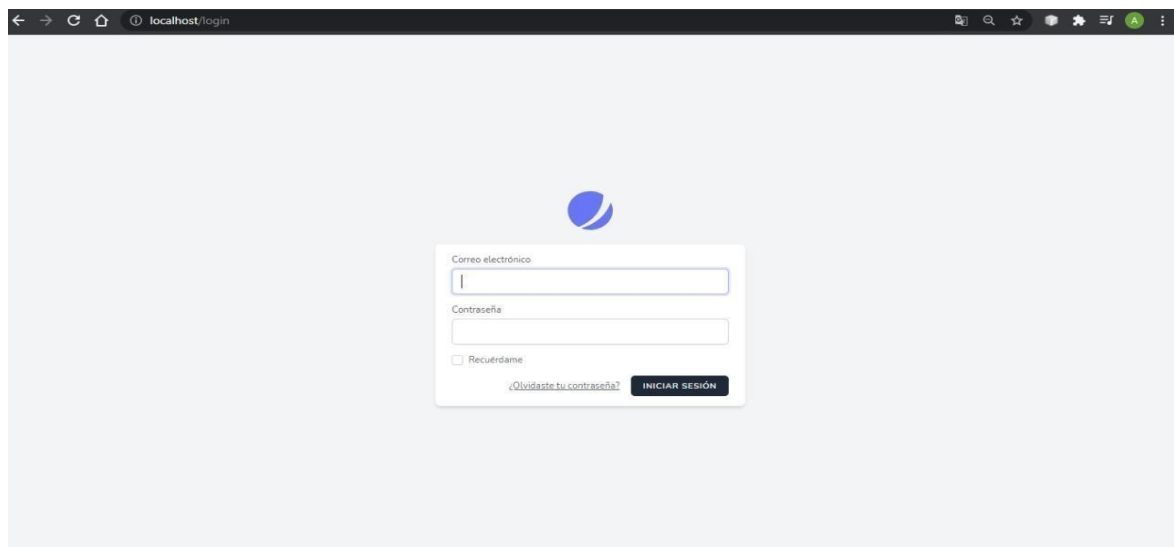
- Integración continúa

La elaboración del proyecto se hizo por módulos, ya que esto era una manera más ordenada de avanzar de a pocos la aplicación web y así poder juntarse ambos programadores para sugerir ideas nuevas o mejoras al proyecto, o que se pueda realizar un cambio.

- Programación en parejas

En cuanto a la programación en parejas, este trabajo de investigación se realizó con las guías de un programador, y por mutuo acuerdo se trabajó y desarrolló la aplicación web en la laptop de los demás integrantes. Ciertas veces fue necesario utilizar el acceso remoto mediante AnyDesk para poder avanzar con todos los requerimientos a tiempo. Finalmente, el trabajo se pudo concluir de la mejor manera y que los usuarios no tengan problemas al usarlo. La programación se desarrolló con PHP, usando el MVC, para que el código este bien estructurado.

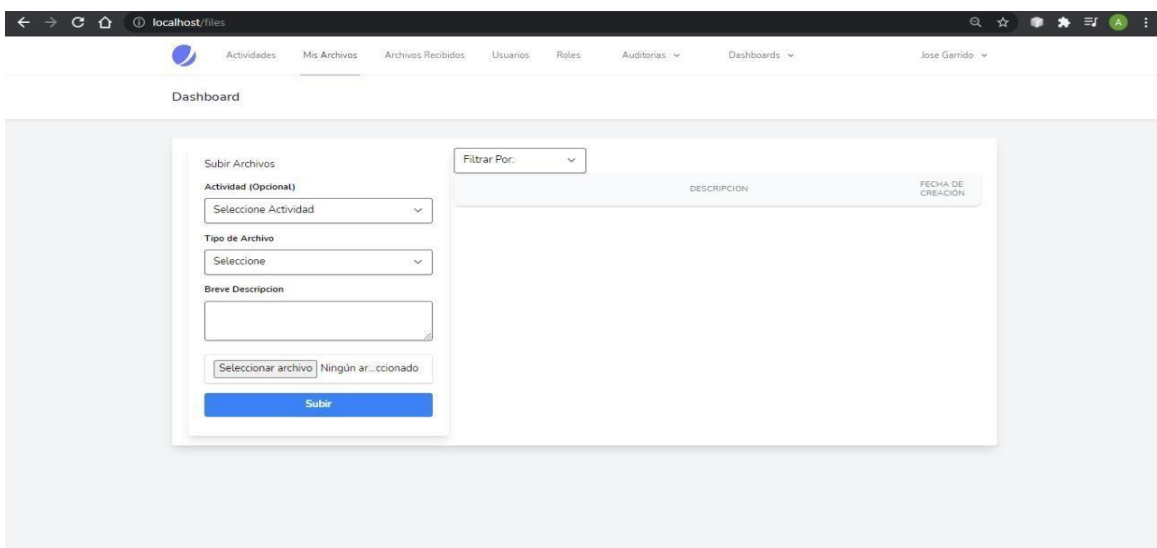
Interfaz de inicio de sesión



Inicio de sesión Controlador

```
Handler.php X
app > Exceptions > Handler.php
1 <?php
2
3 namespace App\Exceptions;
4
5 use Illuminate\Foundation\Exceptions\Handler as ExceptionHandler;
6 use Throwable;
7
8 class Handler extends ExceptionHandler
9 {
10     /**
11      * A list of the exception types that are not reported.
12      *
13      * @var array
14      */
15     protected $dontReport = [
16         //
17     ];
18
19     /**
20      * A list of the inputs that are never flashed for validation exceptions.
21      *
22      * @var array
23      */
24     protected $dontFlash = [
25         'current_password',
26         'password',
27         'password_confirmation',
28     ];
29
30     /**
31      * Register the exception handling callbacks for the application.
32      *
33      * @return void
```

Interfaz de Mis Archivos



Mis Archivos Controlador

```
DashboardController.php X
app > Http > Controllers > DashboardController.php
1  <?php
2
3  namespace App\Http\Controllers;
4
5  use App\Http\Controllers\Controller;
6  use App\Models\File;
7  use App\Models\UserFileAudit;
8  use Illuminate\Http\Request;
9  use Illuminate\Support\Facades\DB;
10
11 class DashboardController extends Controller
12 {
13     public function file_result(){
14         return view('admin.data.file_result');
15     }
16
17     public function table(){
18         return view('admin.data.table');
19     }
20
21     public function data(){
22         $data = DB::table('user_file_audits')
23             ->select(DB::raw("MONTH(created_at) as month,SUM(type ='download') download, SUM(type ='upload') upload
24             ->whereMonth('created_at','5')
25             ->whereYear('created_at','2021')
26             ->groupBy('month')
27             ->get()->toArray();
28         return $data;
29     }
30 }
31
```

Módulo de Archivo Recibidos

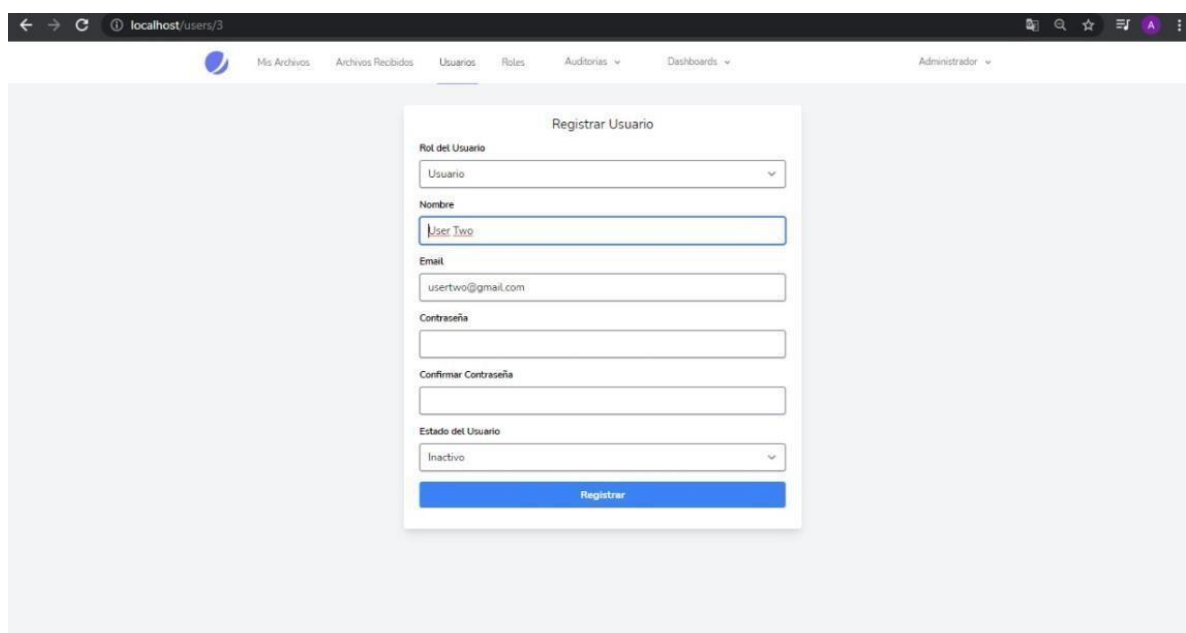
The screenshot shows a web browser at localhost/get-files. The dashboard has a navigation menu with items: Actividades, Mis Archivos, Archivos Recibidos (selected), Usuarios, Roles, Auditorias, Dashboards, and Jose Garrido. Below the navigation is a search bar with the text "Buscar" and a magnifying glass icon. The main content area displays a table with the following data:

NOMBRE DEL PROPIETARIO	CORREO DEL PROPIETARIO	DESCRIPCION	FECHA DE CREACION
Angel Arrascue	angel.arrascue@profesionalesasociados.pe	q	2021-06-04 16:17:18
Angel Arrascue	angel.arrascue@profesionalesasociados.pe	a	2021-06-04 16:17:03
Angel Arrascue	angel.arrascue@profesionalesasociados.pe	virtual_box	2021-06-04 16:13:50
User One	userone@gmail.com	gya_2021	2021-06-04 15:44:31
User One	userone@gmail.com	doc-1	2021-06-04 15:30:43
User One	userone@gmail.com	doc	2021-06-04 15:27:31

Archivo Recibidos Controlador

```
FileController.php X
app > Http > Controllers > FileController.php
1  <?php
2
3  namespace App\Http\Controllers;
4
5  use App\Models\File;
6  use App\Models\User;
7  use Illuminate\Http\Request;
8
9  class FileController extends Controller
10 {
11
12     public function index(){
13         return view('admin.files.index');
14     }
15
16     public function get(){
17         return view('admin.files.get');
18     }
19 }
20
```

Interfaz de Registrar Usuario



The screenshot shows a web browser window with the URL `localhost/users/3`. The page displays a registration form titled "Registrar Usuario". The form includes the following fields:

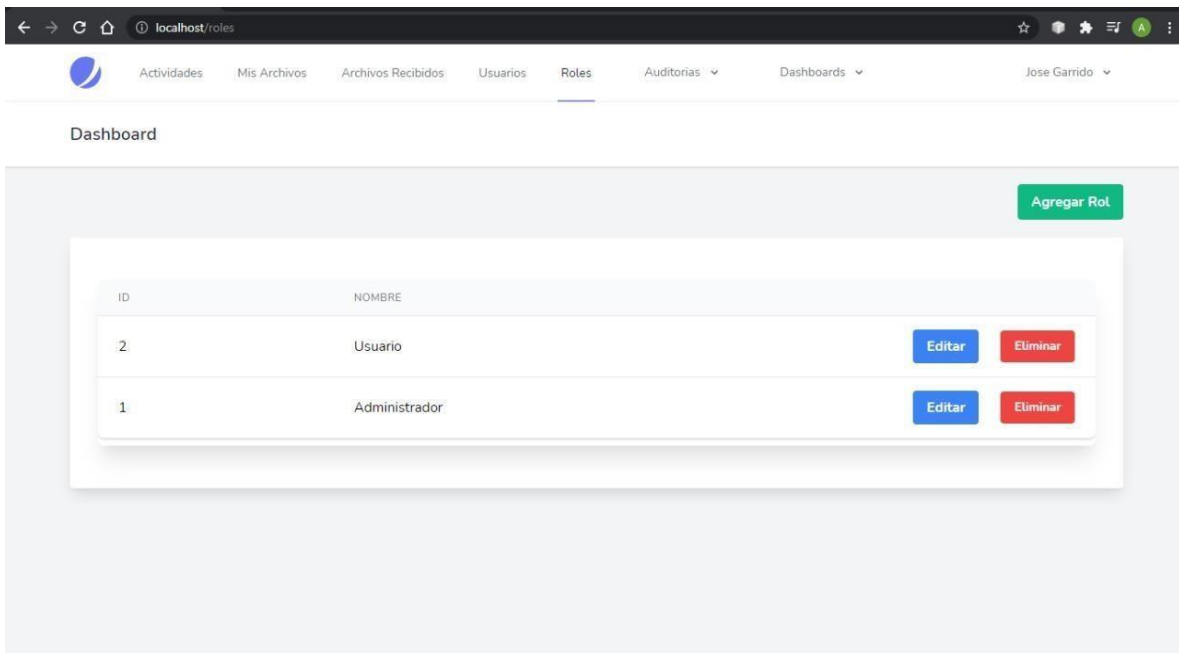
- Rol del Usuario:** A dropdown menu with "Usuario" selected.
- Nombre:** A text input field containing "User Two".
- Email:** A text input field containing "usertwo@gmail.com".
- Contraseña:** A text input field.
- Confirmar Contraseña:** A text input field.
- Estado del Usuario:** A dropdown menu with "Inactivo" selected.

A blue "Registrar" button is located at the bottom of the form.

Registrar Usuario Controlador

```
CreateNewUser.php X
app > Actions > Fortify > CreateNewUser.php
3 namespace App\Actions\Fortify;
4
5 use App\Models\User;
6 use Illuminate\Support\Facades\Hash;
7 use Illuminate\Support\Facades\Validator;
8 use Laravel\Fortify\Contracts\CreatesNewUsers;
9 use Laravel\Jetstream\Jetstream;
10
11 class CreateNewUser implements CreatesNewUsers
12 {
13     use PasswordValidationRules;
14
15     /**
16      * Validate and create a newly registered user.
17      *
18      * @param array $input
19      * @return \App\Models\User
20      */
21     public function create(array $input)
22     {
23         Validator::make($input, [
24             'name' => ['required', 'string', 'max:255'],
25             'email' => ['required', 'string', 'email', 'max:255', 'unique:users'],
26             'password' => $this->passwordRules(),
27             'terms' => Jetstream::hasTermsAndPrivacyPolicyFeature() ? ['required', 'accepted'] : '',
28         ]->validate());
29
30         return User::create([
31             'name' => $input['name'],
32             'email' => $input['email'],
33             'password' => Hash::make($input['password']),
34         ]);
35     }
36 }
```

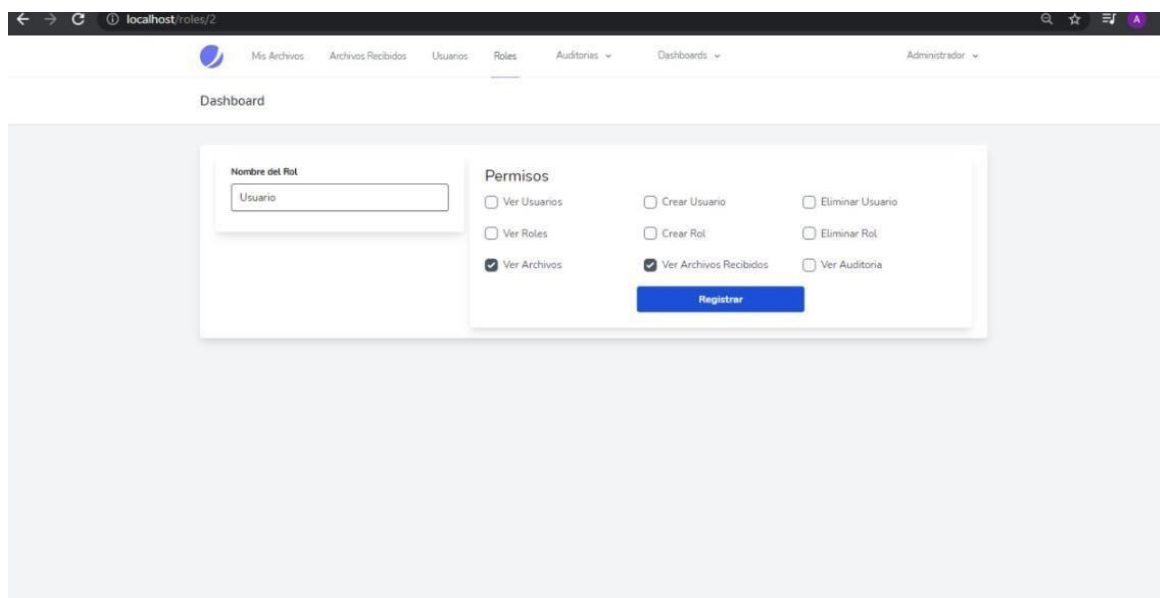
Módulo de Rol



Rol Controlador

```
RoleController.php X
app > Http > Controllers > RoleController.php
1  <?php
2
3  namespace App\Http\Controllers;
4
5  use Illuminate\Http\Request;
6  use Spatie\Permission\Models\Role;
7  use Spatie\Permission\Models\Permission;
8
9  class RoleController extends Controller
10 {
11     public function __construct()
12     {
13         $this->middleware('can:Ver Roles')->only('index');
14         $this->middleware('can:Crear Rol')->only('create','store','edit');
15         $this->middleware('can:Eliminar Rol')->only('destroy');
16         // $this->middleware('can:Editar usuarios')->only('edit','update');
17     }
18
19     public function index(){
20         $roles = Role::latest('id')->paginate('10');
21         return view('admin.roles.index', compact('roles'));
22     }
23 }
```

Interfaz Asignar Roles



Asignar Roles Controlador

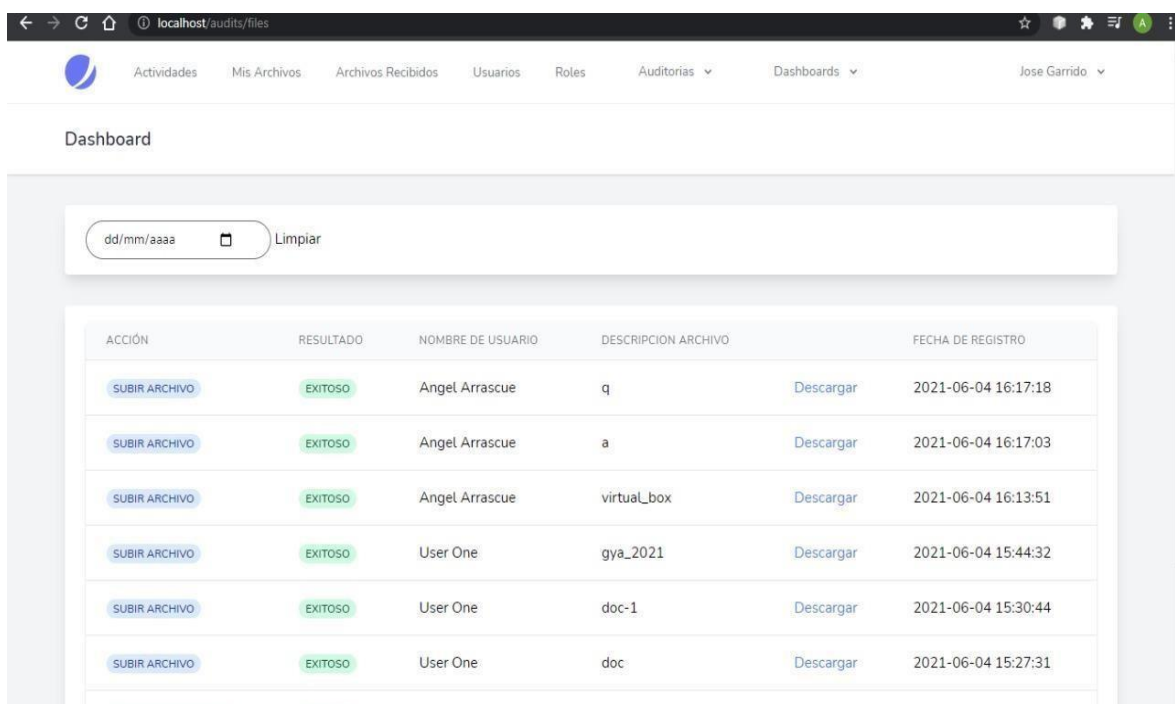
```
public function create(){
    $permissions = Permission::all();
    return view('admin.roles.create', compact('permissions'));
}

public function store(Request $request){
    $request->validate([
        'name' => 'required',
        'permissions' => 'required',
    ], [
        'name.required' => 'El campo Rol es obligatorio.',
        'permissions.required' => 'Los permisos son obligatorios.',
    ]);
    $type = "info";
    $msg = "El Rol se registró con éxito.";
    $role = !isset($request->id) ? new Role() : Role::find($request->id);

    if (!isset($request->id)){
        $role->name= $request->name;
        if(!$role->save()){
            $type = "error";
            $msg = "Error al registrar el error.";
        }else{
            $role->refresh();
            $role->permissions()->attach($request->permissions);
        }
    }else{
        $role->syncPermissions($request->permissions);
        //$role->permissions()->sync($request->permissions);
    }

    return redirect()->route('roles.index')->with($type $msg)-
```

Módulo de Auditoria Usuario



Dashboard

dd/mm/aaaa

ACCIÓN	RESULTADO	NOMBRE DE USUARIO	DESCRIPCION ARCHIVO	FECHA DE REGISTRO
SUBIR ARCHIVO	EXITOSO	Angel Arrascue	q	2021-06-04 16:17:18
SUBIR ARCHIVO	EXITOSO	Angel Arrascue	a	2021-06-04 16:17:03
SUBIR ARCHIVO	EXITOSO	Angel Arrascue	virtual_box	2021-06-04 16:13:51
SUBIR ARCHIVO	EXITOSO	User One	gya_2021	2021-06-04 15:44:32
SUBIR ARCHIVO	EXITOSO	User One	doc-1	2021-06-04 15:30:44
SUBIR ARCHIVO	EXITOSO	User One	doc	2021-06-04 15:27:31

Auditoria Usuario Controlador

```
UserAudit.php x
app > Models > UserAudit.php
1 <?php
2
3 namespace App\Models;
4
5 use Illuminate\Database\Eloquent\Factories\HasFactory;
6 use Illuminate\Database\Eloquent\Model;
7
8 class UserAudit extends Model
9 {
10     use HasFactory;
11
12     const ACTION_UPDATE_PASSWORD = 'update_password';
13     const ACTION_LOGIN = 'login';
14     const ACTION_LOGOUT = 'logout';
15
16     public function user(){
17         return $this->belongsTo('App\Models\User');
18     }
19 }
20
```

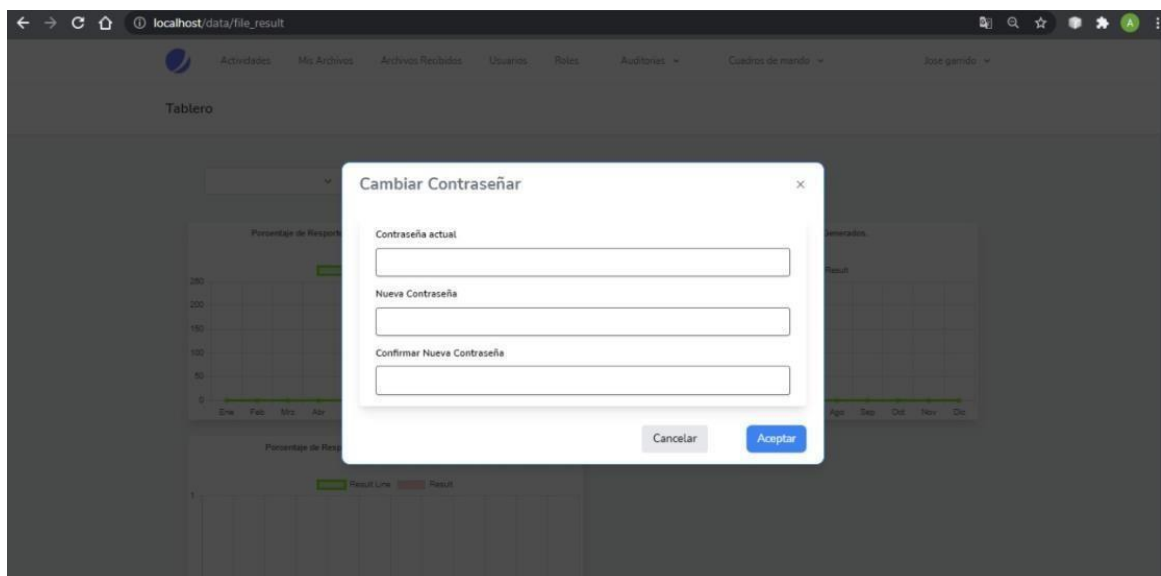
Módulo Auditoria Archivos

The screenshot shows a web application interface for file auditing. At the top, there is a navigation menu with items: Actividades, Mis Archivos, Archivos Recibidos, Usuarios, Roles, Auditorias, Cuadros de mando, and Jose garido. Below the menu, the main content area is titled 'Tablero'. It features a dropdown menu for 'Subida de Archivo' set to '2021'. A table displays file upload data for various users, with columns for days of the month (1-30) and a 'diésis' column. The table shows upload counts for users like 'administrador_asdes', 'administrador_2021_1998', 'userone_doc', 'userone_gya_2021', 'angelarrascue_virtual_box', 'angelarrascue_a', and 'angelarrascue_q'. Below the table, there is a section for 'Seleccoe un mes' and a line chart titled 'Descarga y Subida de archivos por Mes.' The chart has a legend for 'Subida' (blue) and 'Descarga' (green) and shows a significant peak in uploads for the month of October.

Auditoria Archivos Controlador

```
FileResultIndex.php X
app > Http > Livewire > Admin > Data > FileResultIndex.php
6 use Illuminate\Support\Facades\DB;
7 use Livewire\Component;
8
9 class FileResultIndex extends Component
10 {
11     public $search;
12     public $type = 'month', $year, $month;
13     public function render()
14     {
15         $years = DB::table('user_file_audits')
16             ->select(DB::raw('YEAR(created_at) as year'))
17             ->groupBy('year')
18             ->get();
19         return view('livewire.admin.data.file-result-index', compact('years'));
20     }
21
22     public function clear_select(){
23         $this->reset('month','year');
24     }
25
26     public function getMonthsProperty(){
27         return DB::table('user_file_audits')
28             ->select(DB::raw('MONTH(created_at) as month'))
29             ->whereYear('created_at',$this->year)
30             ->groupBy('month')
31             ->get();
32     }
33
34     public function own_months($v){
35         $month = ['Enero','Febrero','Marzo','Abril','Mayo','Junio','Julio','Agosto','Septiembre','Octubre','Novi
36         return $month[$v - 1];
37     }
}
```

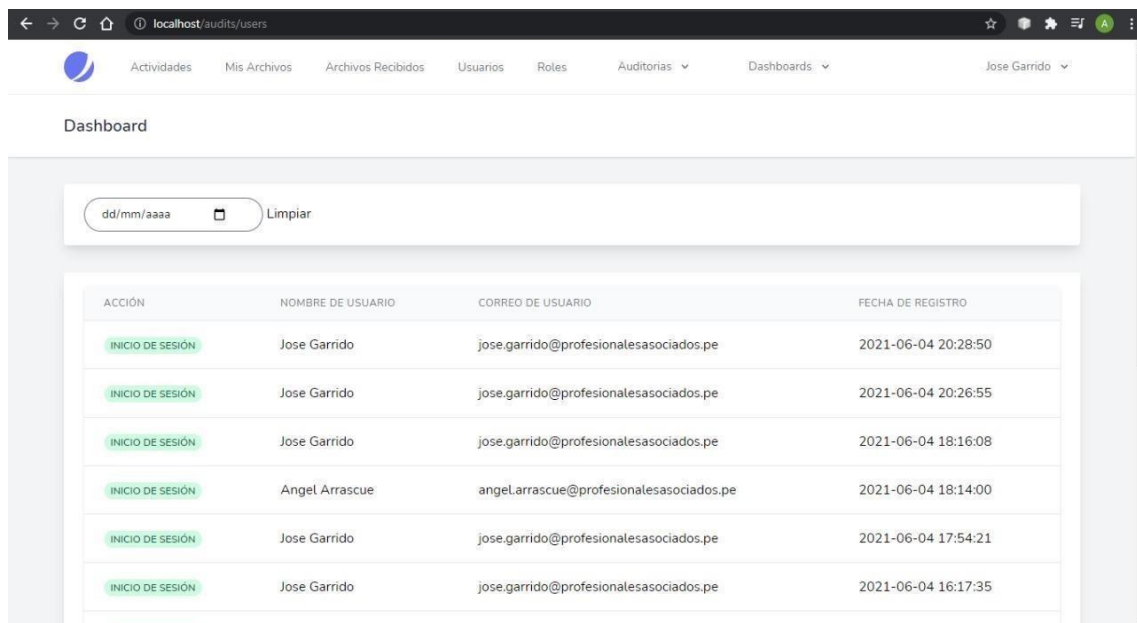
Módulo Resultado de Tabla



Resultado de Tabla Controlador

```
public function password_confirm(){
    Validator::make(
        ['password' => $this->password,],
        [
            'password' => ['required'],
        ],
        [
            'password.required' => 'La contraseña es obligatoria.',
        ]
    )
    ->validate();
    $user = User::where('email', Auth::user()->email)->first();
    if ($user && Hash::check($this->password, $user->password)) {
        $this->emit('close_modal',$this->file_id,$this->file_url);
        $this->reset(['file_id','file_url','password','alert_password']);
    }else{
        $this->alert_password = true;
    }
}
```

Módulo Resultado de Archivos



The screenshot shows a web dashboard with a navigation menu and a table of user activities. The navigation menu includes: Actividades, Mis Archivos, Archivos Recibidos, Usuarios, Roles, Auditorias, Dashboards, and Jose Garrido. The main content area is titled "Dashboard" and features a date filter (dd/mm/aaaa) and a "Limpiar" button. Below the filter is a table with the following data:

ACCIÓN	NOMBRE DE USUARIO	CORREO DE USUARIO	FECHA DE REGISTRO
INICIO DE SESIÓN	Jose Garrido	jose.garrido@profesionalesasociados.pe	2021-06-04 20:28:50
INICIO DE SESIÓN	Jose Garrido	jose.garrido@profesionalesasociados.pe	2021-06-04 20:26:55
INICIO DE SESIÓN	Jose Garrido	jose.garrido@profesionalesasociados.pe	2021-06-04 18:16:08
INICIO DE SESIÓN	Angel Arrascue	angel.arrascue@profesionalesasociados.pe	2021-06-04 18:14:00
INICIO DE SESIÓN	Jose Garrido	jose.garrido@profesionalesasociados.pe	2021-06-04 17:54:21
INICIO DE SESIÓN	Jose Garrido	jose.garrido@profesionalesasociados.pe	2021-06-04 16:17:35

Resultado de Archivos Controlador

```
FilesIndex.php X
app > Http > Livewire > Admin > Audits > FilesIndex.php
1 | k?php
2 |
3 | namespace App\Http\Livewire\Admin\Audits;
4 |
5 | use App\Events\FileDownloadUpload;
6 | use App\Models\UserFileAudit;
7 | use Exception;
8 | use Livewire\Component;
9 |
10 | class FilesIndex extends Component
11 | {
12 |     public $date;
13 |
14 |     public function render()
15 |     {
16 |         $user_file_audits = UserFileAudit::when($this->date, function($query, $data){
17 |             return $query->whereDate('created_at',$data);
18 |         })
19 |             ->latest('id')->paginate(15);
20 |         return view('livewire.admin.audits.files-index', compact('user_file_audits'));
21 |     }
22 |
23 |     public function download($id, $url){
24 |         try {
25 |             $result = response()->download(storage_path('app/public/'. $url));
26 |             FileDownloadUpload::dispatch(UserFileAudit::RESULT_SUCCESS, UserFileAudit::TYPE_DOWNLOAD,$id);
27 |             return $result;
28 |         } catch (Exception $e) {
29 |             FileDownloadUpload::dispatch(UserFileAudit::RESULT_ERROR, UserFileAudit::TYPE_DOWNLOAD,$id);
30 |         }
31 |     }
32 | }
```

Módulo de Usuarios

Actividades Mis Archivos Archivos Recibidos Usuarios Roles Auditorias Cuadros de mando Jose garrido

Tablero

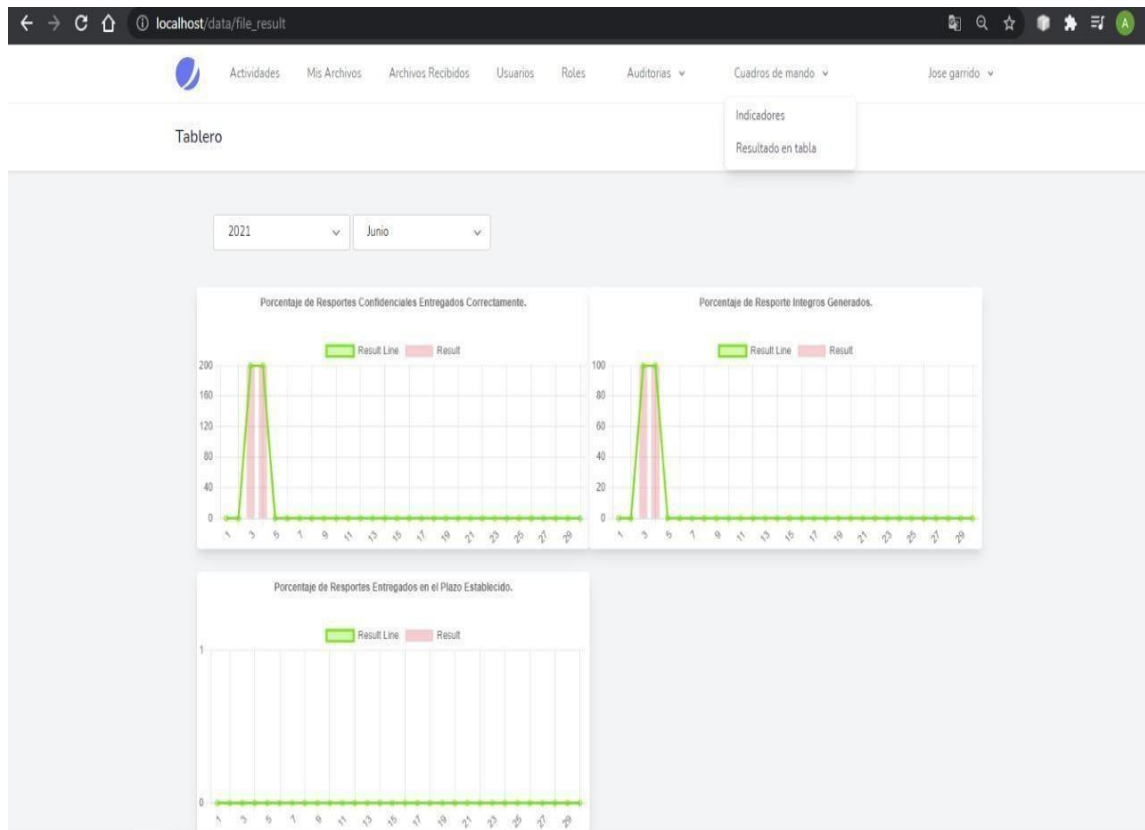
Agregar Usuario

NOMBRE	CORREO ELECTRÓNICO	ESTADO		
Nataly Aldana	nataly.aldana@profesionalesasociados.pe	ACTIVO	Editar	Eliminar
Luz Orosco	luz.orosco@profesionalesasociados.pe	ACTIVO	Editar	Eliminar
Jose garrido	jose.garrido@profesionalesasociados.pe	ACTIVO	Editar	Eliminar
Jhoset Linan	jhoset.linan@profesionalesasociados.pe	ACTIVO	Editar	Eliminar
Ángel Arrascue	angel.arrascue@profesionalesasociados.pe	ACTIVO	Editar	Eliminar
Usuario dos	usertwo@gmail.com	ACTIVO	Editar	Eliminar

Usuarios Controlador

```
UserController.php X
app > Http > Controllers > UserController.php
1  <?php
2
3  namespace App\Http\Controllers;
4
5  use App\Events\UserAuditType;
6  use App\Models\User;
7  use App\Models\UserAudit;
8  use Illuminate\Http\Request;
9  use Illuminate\Support\Facades\Auth;
10 use Illuminate\Support\Facades\Hash;
11 use Illuminate\Support\Facades\Validator;
12 use Spatie\Permission\Models\Role;
13
14 class UserController extends Controller
15 {
16     public function __construct()
17     {
18         $this->middleware('can:Ver Usuarios')->only('index');
19         $this->middleware('can:Crear Usuario')->only('create','store','edit');
20         $this->middleware('can:Eliminar Usuario')->only('destroy');
21         // $this->middleware('can:Editar usuarios')->only('edit','update');
22     }
23
24     public function index(){
25         $users = User::latest('id')->paginate(10);
26         return view('admin.users.index', compact('users'));
27     }
28
29     public function create(){
30         $roles = Role::all();
31         return view('admin.users.create', compact('roles'));
32     }
33 }
```

Interfaz Indicadores



Indicadores Controlador

```
private function getIndOne(){
    $group = ($this->month) ? 'DAY' : 'MONTH';
    $files_success = DB::table('user_file_audits')
        ->select(DB::raw('COUNT(file_id) as files_count, '.$group.'(created_at) as '.$group))
        ->where('type','upload')
        ->where('result','success')
        ->whereYear('created_at',$this->year)
        ->when($this->month, function($query, $data){
            return $query->whereMonth('created_at',$data);
        })
        ->groupBy($group)
        ->get();
    $files_success = json_decode($files_success, true);
    $files = DB::table('files')
        ->select(DB::raw('COUNT(id) as files_count, '.$group.'(created_at) as '.$group))
        ->where('file_type','Confidencial')
        ->whereYear('created_at',$this->year)
        ->when($this->month, function($query, $data){
            return $query->whereMonth('created_at',$data);
        })
        ->groupBy($group)
        ->get();
    $files = json_decode($files, true);
    $count = ($this->month && $this->year) ? $this->getDays() : 12;

    $arr = [];
    for ($i=1; $i <= $count; $i++) {
        $fs = 0;
        $f = 0;
        $in = array_search($i, array_column($files_success, $group));
        if($in !== false){
            $fs = $files_success[$in]['files count'];
        }
    }
}
```

Interfaz Actividades

Subir Archivos

Tipo de Archivo

Breve Descripción

Fecha Limite

Fecha de Cierre

Filtrar Por:

ARCHIVOS ACEPTADOS	DESCRIPCION	FECHA LIMITE	FECHA DE CIERRE	
Archivos	Confidencial	DOCUMENTO_2021-06-04	2021-06-03 16:09:00	2021-06-05 16:09:00

Actividades Controlador

```
protected function getListeners()
{
    return ['download'];
}

public function set_url($id,$url){
    $this->file_url = $url;
    $this->file_id = $id;
    $this->emit('open_modal');
}

public function download($id, $url){
    try {
        $result = response()->download(storage_path('app/public/'. $url));
        FileDownloadUpload::dispatch(UserFileAudit::RESULT_SUCCESS, UserFileAudit::TYPE_DOWNLOAD,$id);
        return $result;
    } catch (Exception $e) {
        FileDownloadUpload::dispatch(UserFileAudit::RESULT_ERROR, UserFileAudit::TYPE_DOWNLOAD,$id);
    }
}

public function password_confirm(){
    Validator::make(
        ['password' => $this->password,],
        [
            'password' => ['required'],
        ],
        [
            'password.required' => 'La contraseña es obligatoria.',
        ]
    )
    ->validate();
}
```