UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SGSI con ISO 27001 aplicado a la empresa SOLTESI S.A.C. del distrito de Jesús María 2021

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTOR:

Poma Ramos, Alexander (orcid.org/0000-0003-1248-5060)

ASESORA:

Mgtr. Menendez Mueras, Rosa (orcid.org/0000-0003-2403-7679)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LIMA – PERÚ

2021

DEDICATORIA

El trabajo de investigación es gracias a Dios, por encima de todos que es quien nos ha inspirado y dado fuerzas para poder desarrollar y obtener un resultado que nos permite lograr uno de los primeros objetivos en nuestra carrera universitaria.

A nuestros padres por el ayuda brindado hasta el final de nuestra carrera, ya que gracias a ellos es que hoy en día hemos logrado llegar a dónde estamos y decirles que ha sido un orgullo y un privilegio ser su hijo, gracias.

AGRADECIMIENTO

Agradecemos a todos los docentes de la escuela de Ingeniería de Sistemas de la Universidad Cesar Vallejo, por habernos brindado sus sabidurías y el conocimiento adecuado para ser un profesional, a Dr. Menéndez Mueras Rosa tutora de nuestro proyecto de investigación quien nos ha orientado con su rectitud y paciencia como docente.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

Este trabajo de investigación se realizó con el objetivo de determinar la influencia del SGSI en la empresa Soltesi S.A.C. con el uso de la ISO 27001.

La investigación es de tipo aplicada y se tomó como diseño de investigación experimental del tipo pre-experimental porque pretende determinar la influencia en la variable dependiente. Como resultado se obtuvo que las incidencias que se efectuaban en la empresa y no se solucionaban al 99% implementando el SGSI con la norma ISO 27001 mejorara significativamente en resolver las incidencias al menor tiempo posible, teniendo como pruebas los resultados por cada indicador aplicando el pre test y post tes.

El resultado del indicador integridad, con el pre-test se obtuvo con un valor media de 32% de incidencias resueltas al mes y que al realizar el post-test se obtuvo un valor media de 75% de incidencias resultas en un mes, siguiendo con el resultado de la confidencialidad, con el pre-test se obtuvo con un valor media de 15% de incidencias resultas al mes y que al realizar el post-test se obtuvo un valor media de 80% de incidencias resultas en un mes, como fin el resultado de disponibilidad, con el pre-test se obtuvo con un valor media de 17% de incidencias resultas al mes y que al realizar el post-test se obtuvo un valor media de 81% de incidencias resultas en un mes.

Palabras clave: SGSI, ISO 27001, Seguridad Información.

ABSTRACT

This research work was carried out with the objective of determining the influence of the ISMS in the company Soltesi S.A.C. with the use of ISO 27001.

The research is of an applied type and was taken as an experimental research design of the pre-experimental type because it aims to determine the influence on the dependent variable. As a result, it was obtained that the incidents that were carried out in the company and were not solved at 99% by implementing the ISMS with the ISO 27001 standard improved significantly in resolving incidents in the shortest possible time, having as evidence the results for each indicator applying the pre test and post test.

The result of the integrity indicator, with the pre-test, was obtained with an average value of 32% of incidents resolved per month and that when performing the post-test an average value of 75% of incidents resolved in one month was obtained, following with the result of confidentiality, with the pre-test an average value of 15% of incidents resulted per month was obtained and that when performing the post-test an average value of 80% of incidents resulted in one month was obtained, as Finally, the result of availability, with the pre-test was obtained with an average value of 17% of incidents resulting per month and that when performing the post-test an average value of 81% of incidents resulting in one month was obtained.

Keywords: ISMS, ISO 27001, Information Security.

I. INTRODUCCIÓN

"Actualmente la información […] viene siendo un universo mucho más grande de lo que uno tiene pensando, ya sea por tema de aprendizaje o por hechos ya ocurridos, […] uno de los puntos importante en la seguridad de la información es minimizar riesgos, mitigando problemas halladas en el sistema, así mismo existe por diversos modos, ya sea por la entrada de datos por donde se transporta la información". (Romero, et al. 2018, p. 13)

Dado a lo mencionado, La empresa Soltesi S.A.C; se encarga de implementar software para la solución de procesos de registro, venta y administración, debido a ello la empresa, no cuenta con un respaldo de resguardar la información que se establece en la empresa. Es ahí donde los datos e información no están segura, la información de la BD, y los usuarios son vulnerables a ser hackeados, es por ello que hoy en día las empresas cuentan con un S.G.S.I. como es la ISO 27001 en cual apoya a las pequeñas y grandes empresas. En lo que es seguridad a la información lo cual genera una confianza de portar un software muy robusto y seguro a los ataques cibernéticos.

Uno de los puntos más importante en la seguridad de la información es el ingreso no permitido a los datos de la empresa, lo primordial es el ingreso ilegitimo de contraseña del servidor, donde no está permitido ingresar a los datos de la empresa, sin ninguna autorización de la persona a carga, además es informal generar copia a los códigos de fuentes generados por el área de desarrollo de software, tomar fotos a las áreas laborales, insertar USB a las computadoras, etc. La interacción e intercambio de datos mediante las redes WAN o LAN, es sumamente uno de los favoritos instrumento para los malware, ya que se inicia mediante él envió de algún correo o abrir algún spam en la computadora, lo cual genera lentitud a la maquina e intentando acceder a los servidores para poder enviarse datos privados ya sea de clientes o de la empresa.

Existe diversos métodos en donde se puede prevenir, algún acto vandálico por

internet por ejemplo el firewall, uno de las principales fuentes de protección de datos, antivirus para poder proteger de malwares descargados por internet y estándares de ISO 27001 lo cual aporta pasos para poder implementar las normas políticas de seguridad que pueda resguardar información privadas de la empresa.

Por ello está redundante investigación, en donde el problema que se está dando en la empresa Soltesi S.A.C. se quiere implementar un SGSI con ISO 27001 que pueda identificar las incidencias de acceso al sistema, perdida de datos y resguardar los datos de código de fuente con la que se generó el software.

El autor de este proyecto de investigación formula el problema general así ¿Cuál es el nivel del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María?, y como problema especifica de la siguiente manera, ¿Cuál es el nivel de integridad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María?, ¿Cuál es el nivel de confidencialidad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María? Y ¿Cuál es el nivel de disponibilidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María?

El proyecto de investigación propone aplicar la ISO 27001 para la empresa SOLTESI S.A.C. de esta manera se tendrá un plan de estudio que se podrá certificar con la Norma ISO 27001, además hace que las empresas sean más productivas, dando a entender que tienen mayor responsabilidad en mantener la información de sus clientes resguardados, además tiene un prestigio a nivel mundial sobre su efectividad en la seguridad de la información.

El proyecto se justifica en forma operativa porque hoy por hoy la empresa Soltesi S.A.C. realiza la creación e implementación de softwares, solucionando los problemas de las empresas, así como los registros, administración y ventas de las funciones que realizan las empresas.

De esta manera el autor propone como objetivo general, determinar la influencia

de la seguridad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María, y como objetivos específicos: Determinar la influencia de la confidencialidad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María, determinar la influencia de la integridad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María y determinar la influencia de la disponibilidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María.

De esta manera el autor propone como hipótesis, el SGSI mejora significativamente con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María, y como hipótesis especificas: El SGSI mejora significativamente la integridad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María, El SGSI mejora significativamente la confidencialidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María y el SGSI mejora significativamente la disponibilidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María.

II. MARCO TEÓRICO

A continuación, para este trabajo de investigación se investigo en diversos gestores y repositorios de distintas universidad, instituto y revistas los cuales fueron recogidos para los antecedentes.

Se realizo a detalle diversos campos, repositorios etc., que se asemejan a la variable dependiente e independiente, por ello se tomaron como antecedentes:

Figueroa (2019), así mismo tiene como objetivo de desarrollar un plan de S. I. basado en la ISO 27002 para el fortalecer de la gestión de la información en el departamento del área TIC de la Uniandes extensión Babahoyo, donde se realizó el tipo de investigación aplicada, de campo y bibliográfico, diseño de investigación no experimental, se tomó en cuenta a la población al grupo de gestión de la información en el departamento de TIC de la Uniandes extensión Babahoyo con un total de 25 personas; Se llego a la conclusión de que la implementación del plan de seguridad informática, permitirá mejorar la gestión de información en el departamento TIC, de igual manera se recomendó implementar exámenes periódicas, a la seguridad informática planteada para aumentar los controles necesarios y así alcanzar una certificación de seguridad informática.

Moreira (2019), desarrollar un plan de seguridad informática en redes, para la cooperativa de ahorro y crédito san Antonio, el mismo que luego de ser aplicada producirá un mejoramiento de la gestión operativa que realiza la empresa, tipo de investigación aplicada, diseño de investigación no experimental, se tomó en cuenta a la población 1526 personas de la cooperativa de ahorro y crédito San Antonio, como muestra está formado por 226 personas; Se concluyo que la indiferencia por parte de la gerencia y los entes directivos, no se realiza el apoyo económico a la gestión de información para implantar medidas de seguridad, lo cual provoca que la entidad tengo una mayor exposición a los riesgos, como recomendación se debe realizar un proceso de concientización periódico, además se deben firmar actas de conocimiento del plan de seguridad con acuerdos de confidencialidad a todos los funcionarios de la cooperativa.

Meneses (et. al) (2017) con el objetivo de diseñar un S.G.S.I. , basado en el estándar de la ISO 27001, con el tipo de investigación no experimental y con el diseño de investigación descriptiva, se tomó en cuenta a la población del área administrativo de la cámara de comercio; así mismo se llegó a la conclusión de la falta mantenimiento informático que realizan en cada espacio de procesos en la Cámara de Comercio Aguachica, donde la implementación de las normas que regularan, estandarizaran y garanticen los tres puntos más importante de la S. I., confidencialidad disponibilidad e integridad de los datos, de igual manera se recomendó a la Gerencia de la Cámara de Comercio de sistema, lograr unir todo los procesos de manejo de los recursos de TI.

Casadiegos, Quintero y Toro (2014) en su tesis, S.G.S.I. para el área de la E.S.E. del Hospital Local de Rio de Oro Cesar, Realizado en la universidad de Francisco de Paula Santander Ocaña, teniendo como objetivo, plantear un SGSI, de igual manera como resultado se realizó el modelado de negocio donde se detalló los procesos que se debe llevar para realizar en el área de contabilidad de la E.S.E. logrando visualizar la cadena de valor, modelando los procesos a través del Busness Motivation Model, logrando así crear la estructura orgánica y identificando la tecnología de información. Tipo de investigación aplicada, Diseño de, de igual manera la muestra que se tomó para realizar esta investigación son el gerente, contado, auxiliar y la encargada de la facturación.

Guevara (2018), se dio a reconocer los cambios en el DTIC ante una propuesta de controles de seguridad de la información, tipo de investigación exploratorio y como diseño de investigación se realizó el cuasi experimental, de igual manera la población por el personal de la dirección de tecnología y la comunicación de la escuela superior Politécnica, de igual manera la muestra, como conclusión se dio a analizar las leyes que son vigente el Ecuador, porque son creadas con el objetivo de ser cumplidas y que garanticen el buen funcionamiento y manejo de las instituciones públicas y privadas, ya que son ellos poseen la información de los personales de la ciudadanía, de igual manera se recomendó estandarizarse en la norma ISO 27001, ya que es la uncia certificable que no genere cambios. Los resultados que se llegaron a tener aplicando la propuesta ayudaría en perfeccionar la calidad de la Seguridad de la Información tomando como referencia a la

disponibilidad, integridad y confidencialidad de los datos de la norma ISO 27001, porque se pretenderá incluir los principios de la seguridad informática para el mejoramiento de la Dirección de Tecnología y Comunicación.

Para Rojas y Moreno (2016) con el objetivo principal de decretar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las pymes de Perú, tipo de investigación enfoque cuantitativo, diseño de investigación Cuantitativo No-Experimental, en la población según las estadísticas del INEI, en el Perú hay un total de 1.713.272 empresa, donde el 99.6% son consideradas pequeñas, micro o mediadas empresas. Los resultados fueron que la empresa Zavala Cargo S.A.C. tener una falta de contingencia ante posibles ataques de seguridad de la información, es tener información regalada, para ello se debe realizar planes de ataques contra los ciberataques, que permite tomar una decisión confiable para resguardar la información tanto de los clientes y del personal. Así mismo se recomendó a la empresa Zavala Cargo S.A.C. elabore las políticas de seguridad y ciberseguridad en la empresa con el fin de resguardar la información de los clientes y personal de trabajo.

Por lo tanto, Vilca (2017) cuyo objetivo determinar el mejoramiento al implementar un SGSI para perfeccionar la seguridad en los campos de recursos humanos en la empresa Geosurevey S.A. logrando obtener resultados la implementación del sistema los trabajadores de cada área de soporte se demoraban entre 12 a 24 horas en solucionar los problemas, donde el 75.8% de los trabajadores brindo como resultado, ahora luego de la implementación los trabajadores se demoraban entre 1 y 2 horas como máximo para resolver el problema que se le planteaba, donde el 69.7% de los trabajares brindaron como resultado, es por ello que la norma ISO 27002 ayudo a incrementar la productividad de los trabajadores tanto en sitios web de ocio como en las demás actividades. Tipo de investigación aplicado y diseño de investigación que presenta es el pre experimental, con respeto a la población se considera a los integrantes de la organización administrativa y operativo de la empresa, para la muestra se consideraría a todos de la población, porque la cantidad de la población es muy pequeña. Como conclusión se obtuvo la optimización de los procesos de formación y capacitación

sobre la importancia de la seguridad de la información, a los personales del campo directivo de la empresa.

Según Mercedes (2017) de manera de que el objetivo principal es determinar las características del diseño del SGSI, bajo la Normativa de Protocolos de Internet ISO/IEC 27001 2014. Se obtuvo como resultado que la seguridad de la información en la institución no se viene gestionado, por ello se requiere la implementación del SGSI que implicara aumento de esfuerzo y compromiso de los empleadores de la empresa MPH. Tipo de investigación aplicada, ya que se diseñará un SGSI dentro de la Municipalidad Provincial de Huamanga, diseño de investigación no experimental, porque no se va manipular la variable. La población esta constituida por los empleadores de la Municipalidad Provincial de Huamanga y la muestra es un muestreo probabilístico, la cual esta constituido por los empleadores de la Subgerencia de Sistema y Tecnología. Como conclusión se indico la importancia de diseñar el SGSI para la Municipalidad Provincial de Huamanga, mejora la seguridad informática en la dirección, identificando el alcance del SGSI, se recomendó que al utilizar los procedimientos en esta investigación es preciso para diseñar los SGSI para diversidad municipalidades.

Para Celis (2018) con el objetivo de presentar un plan de seguridad de la información para la Central Hidroeléctrica de Carhuaquero, para mitigar riesgo. El tipo de investigación realizado en este proyecto es la investigación es descriptiva, como diseño de investigación es experimental, para la población esta conformada por 40 usuarios de la central Hidroeléctrica, así mismo la muestra se calcula aplicando la formula logrando obtener 36 usuarios, Como conclusión se realizará el análisis y gestión de riesgos conformado por la UPH, además se recomendó brindar charlas y capacitaciones o talleres sobre temas de seguridad informática a los usuarios.

Así mismo Niño (2018) el objetivo general de la investigación modelar un SGSI, que permita resguardar la disponibilidad, confidencialidad e integridad de la información, en los procesos de la gerencia del instituto nacional de estadística informática ODEI de Lambayeque. Tipo de investigación trasversal, diseño de investigación descriptiva porque permite determinar los problemas presentados, en cuanto a la población se tomara en cuenta al área cuadro personal del Instituto

Nacional de Estadística, la muestra censal porque se llega a escoger al conjunto de las áreas del instituto, como conclusión la implementación de un SGSI, para disminuir los peligros informáticos, así mismo se recomendó un grado alto en cuanto a la eficiencia, fiabilidad, rapidez y trazabilidad que requiere las actividades de ODEI Lambayeque.

A continuación, se realizó las definiciones de las variables planteadas para el proyecto de investigación:

Para la investigación Piattini, Peso sostienen que:

> La crisis de la ingeniería del software y los desastres en donde se reportan fallos de software que pueden llegar a causar en las organizaciones problemas a futuro se les conoce como CHAOS, ya que hace referencias a los retrasos de entrega de informes. En el último informe, se señaló que solo el 29% de los proyectos informáticos se llegó a estimar, además con los recursos planificados y con una calidad aceptable, mientras que en un 19% fracasan totalmente. El resto del 52% se termina, pero consumiendo muchos más recursos con menos funcionalidad de las previas. Hay que destacar que el uso de metodologías agiles mejoran esta situación ya que, según el Standish Group, los proyectos que aplican metodologías tradicionales. Aunque ya (Jorgensen y Molokken Ostvod, 2006) expresaban dudas sobre algunas cifras de informe Chaos, en general podemos decir que dan una imagen de lo que sucede en la industria del software. (2018, p. 106)

Según lo declarado por Piattini y Peso es que existe proyectos de creación de software que, si no logran cumplir con el planificado, no se lograra llegar al objetivo planteado, debido a que los proyectos informáticos son aplicados con metodologías tradicionales mas no con las nuevas metodologías agiles.

Para esta investigación Pérez deduce que:

> Toda la entidad, empresas, organismo, etc., con el desempeño de su actividad, generan y almacenan información que puede ser más o menos valiosa. Pongamos el caso de una empresa. En su actividad diaria genera información de forma de clientes, proveedores, datos de

> contactos, pedidos, albaranes, facturas, protección, planos. (2015, p. 215)

Para esta investigación Pérez comenta que:

> Tener en cuenta que los fundamentos de la seguridad de la información son procesos, ya que la seguridad no es comercial, mas si gestionar, es ahí donde se genera las ventajas para la seguridad de la información en gestionar, y evitar la interrupción en el área de trabajo o trabajos administrativos, ahorrando costes que se generan por falta de seguridad de información, Llegando a descubrir si existe fraudes en la propia empresa. (2015, p. 235)

Lo que quiere decir el autor, es poder optar por medidas de prevención que puede beneficiar mucho a sector empresarial, en cuanto a la seguridad informática de los datos, en donde nos permite resguardar cada información que nosotros tenemos para que así no ser extorsionados o chantajeado por terceras personas.

Confidencialidad

Según Piattini (2018) “Es el momento en que el sistema sea segura y que los datos solo sean accesibles cuando se tiene autorizado”. (p. 207)

Integridad

Según Piattini (2018) “Es el momento en que el sistema o componente del producto, previene el acceso y la modificación no autorizada de los programas y datos”. (p. 207)

Según Baca (2016) “La seguridad de la información es una diciplina de bases políticas con normas internas y externas para las pequeñas y grandes empresas, donde se tiene como función proteger la integridad, disponibilidad, confidencialidad de los datos”. (p. 11)

En lo mencionado anteriormente, la seguridad informática tiene el funcion de proteger la libertad de los datos ya sea interno y externo, eso debido a los riesgos de perdida de información que ocurre a diario en las empresas.

Confidencialidad

Según Baca (2016), “Se refiere a la información debe de encontrarse protegida contra los ingresos no autorizado, donde se previene la derivación u alteración de la información”. (p. 35)

Integridad

Según Baca (2016), “Se refiere a que la información recibida sea precisa, completa y válida de acuerdo con los valores y expectativas del negocio”. (p. 35)

Disponibilidad

Según Baca (2016) “Se refiere a la información necesaria para llevar a cabo cualquier etapa de un proceso administrativo, de modo que la información esté a la mano cuando el proceso la necesite en cualquier momento”. (p. 36).

Según Gómez (2017) “como principales temas, de la seguridad informática se podría destacar a los siguientes”. (p. 40)

- Gestionar y disminuir los riesgos, previniendo los posibles errores y amenazas a la seguridad.
- Garantizar el adecuado uso de recursos y del software del sistema.
- Prever la perdida de información y realizar una recuperación del sistema en caso de alguna incidencia por seguridad.
- Para cumplir los objetivos de la organización se debe plantear los cuatros planos de actuación.

Según Cuervo (2017) “ISO 27001 es una norma internacional publicada por la Organización Internacional de Normalización (ISO), considerada para ser publicada en 2013 y rebautizada como ISO/IEC 27001:2013”. (p. 43)

Según Calder (2017) “la ISO 27001 se puede realizar la implementación en cualquier tipo de organización, ya sea pequeña, grande, publicada o privada, eso da lo mismo para las organizaciones. La ISO 27001 está redactada por los mejores metodólogos para que se realice una buena implementación de Gestión de la Seguridad en una organización. Actualmente la certificación de la norma ISO 27001 es un significado de que la norma ISO 27001 esta implementado en la empresa,

logrando visualizar que la empresa está en proceso de poder gestionar la integridad, disponibilidad e integridad de los datos” (p.6).

Según el autor Calder (2017) “La ISO 27001:2013 es una norma que se puede implementar en distintas empresas sea privada o pública lo cual tiende a decir que ser una empresa certificada con la norma ISO 27001 te da la ventaja de que tu empresa a que la seguridad de información es sumamente excelente”. (p. 11)

III. METODOLOGÍA

3.1. Tipo y Diseño de Investigación

De acuerdo a los análisis que se dieron a la investigación, se ha logrado determinar que la investigación es del tipo aplicada, porque se asemeja al uso de conocimientos teóricos y prácticos llegando así resolver y determinar problemas.

Según Baena (2017) “La investigación es de tipo aplicada, ya que fija un punto de estudio de una cuestión en acción, también puede aportar hechos nuevos a lo ya investigado […] por lo tanto este modo se puede confiar con pruebas ya usadas”. (p. 18)

El objetivo de la investigación fue aplicado, porque se va estudiar un problema destinado a la acción. La investigación aplicada puede proporcionar nuevos hechos […] La investigación aplicada tiene como objetivo estudiar un problema destinado a la acción para que pueda confiar en los hechos revelados. (Baena,2017, p. 18)

Para este estudio se considero un diseño de investigación experimental de tipo pre-experimental, ya que tiene objetivo determinar el efecto sobre la variable dependiente Seguridad, mediante la realización de pruebas previas y posteriores.

La investigación experimental es representación del manejo de la variable experimental que no se comprobó, ya sea en momentos restringidos controladas, con un objetivo de detallar la causa que produce el problema. (Baena,2017, p. 18).

Figura 1. Formula de incidencias

En dónde:

G: es el gripo de estudio, en esta investigación es la Empresa Soltesi S.A.C.

X: Es el tratamiento a realizar en la investigación se utilizará SGSI.

O1: (Pretest) Es la medición previa de los sujetos o casos del grupo de estudio determinado, en esta investigación se realizar la ISO 27001.

O2: (Postest) Es la medición posterior de los sujetos o casos del grupo de estudio determinado en esta investigación se realizará la ISO 27001

3.2. Variables y Operacionalización

Definición Conceptual

Variable Independiente (VI): SGSI

Cuervo (2017) “El SGSI está conformado por las cuatro fases lo cual se debe implementar en forma seguida para así poder disminuir riesgos sobre los 3 pilares de la seguridad de la información”. (p. 104).

Esta variable se va medir con 1 dimensiones el de seguridad, Se utilizo la ficha de registro como instrumento y un balotario de 15 preguntas.

Variable Dependiente (VD): ISO 27001

Cuervo (2017) “La ISO 27001 es una norma publica donde se detalla como dirigir la seguridad de la información […] la implementación de un S.G.S.I. se realiza en cualquier campo labora”. (p. 104)

Definición Operacional

Variable Dependiente (VD): Seguridad de información

Esta variable medirá 1 dimensión, seguridad de la información y los 3 indicadores, confidencialidad, disponibilidad e integridad, en donde se utilizó la Ficha de registro como instrumento conformado por 15 preguntas, que será dirigido para los trabajos de la empresa SOLTESI para medir la seguridad de la información.

El primero indica para la investigación el porcentaje de Incidencia de confiabilidad, así como se muestra la formula establecida.

$$PIC = \frac{N°IC}{TI}$$

Figura 2. Indicador Confidencialidad

Fuente: Elaboración Jeimy J.

El segundo indica que se empleara para este estudio es el Porcentaje de Incidencia de integridad, tal y como se muestra en la formula establecida

$$PII = \frac{N°II}{TI}$$

Figura 3. Indicador Integridad

Fuente: Elaboración Jeimy J.

El tercer indica que se empleara para este estudio es el Porcentaje de Incidencia de Disponibilidad, tal y como se muestra en la formula establecida

$$PID = \frac{N°ID}{TI}$$

Figura 4. Indicador Disponibilidad

Fuente: Elaboración Jeimy J.

3.3 Población, Muestra y Muestreo

Población

Hernández et. al. (2018), “La población es un conjunto de objetos con que se trabaja previamente para determinar en número y características de que tipo de información se requiere generalmente trabajar”. (p. 105)

Con respecto a lo comentario anteriormente, para esta investigación se determinó que la población a evaluar el S.G.S.I. seria de 22 fichas de registros de incidencias, en la empresa S.A.C. del distrito de Jesús María.

Muestra

Baena (2017), “La muestra es una parte que representa al mundo de estudio de la población, la muestra se selecciona por distintas técnicas tanto muestreo probabilístico y no probabilístico”. (p. 12)

Para esta investigación, se aplicó la muestra a 22 fichas de registros de incidencias, dado la similitud con la población, para esta investigación se registró según la ocurrencia observada en la ficha de registro durante 1 mes en el área de TI de la empresa Soltesi S.A.C. del distrito de Jesús María.

Muestreo

Baena (2017), “El muestreo es un procedimiento en donde los miembros de la población persona o cosas, se selecciona como representativo para realizar la prueba de la investigación, […] entendible y con una selección muy rápida y eficaz de enumerar la población”. (p. 35)

Ya que la población es diminuta con un muestreo de 22 trabajadores, se realizó solo 22 fichas de registros de incidencias para el muestreo.

3.4. Técnicas e instrumentos de recolección de datos

Hernández, Ramos et. (2018), “La observación se puede utilizar en diferentes tiempos de investigación, como una etapa inicial, que constituye una vía para la exploración del fenómeno que se va a realizar el estudio”. (p. 97)

Técnica de Recolección de Datos

Para la investigación se utilizó la técnica de ficha de observación, la cual nos permitirá registrar las incidencias en la seguridad de los datos en los sectores de la empresa Soltesi S.A.C. del distrito de Jesús María.

Instrumento de Recolección de Datos

Sampieri (2016), “La ficha de registro es una de las opciones para el diseño o método de obtener datos, es el mas usado en los temas de

investigación experimenta, transversal etc., así mismo en ficha de registro". (p. 29)

Para la investigación se diseñó como instrumento para la recolección de datos es la ficha de registro, lo cual nos permitirá recolocar registrar información específicamente para estimar las incidencias de perdida de información en la empresa Soltesi S.A.C. Jesús María.

Validez de Contenido

Hernández, Fernández y Bautista (2017), "comento que la validez es el instrumento de medición que examina diversos tipos de evidencia seleccionada, a mayor evidencia de validez encontrada y criterios se acerca mas a brindar las variables para medir, que evalúa todo tipo de evidencia recolectada, a mayor evidencia de validez de participio, de validez de criterios se acerca más a brindar las variables que se pretende medir". (p. 204)

Para esta investigación se utilizó la validez de contenido mediante los juicios de experto, donde se aceptó el cuestionario planteado por 3 ingenieros y un asesor.

Tabla 1 *Matriz de validación de instrumento*

Validez de juicio de Experto	Grado Académico	Opción de Aplicabilidad
Jauregui Briceño, Carlos Eduardo	Magister	Aplicable
Méndez Muera, Rosas	Magister	Aplicable
Montoya Negrillo, Danny José	Magister	Aplicable
Chávez Pinillos, Frey Elmer	Doctor	Aplicable

Fuente: elaboración propia

En la tabla 6, se muestra los frutos de evaluación de validez del instrumento, para el especialista Jauregui Briceño, Carlos Eduardo ingeniero de sistema lo cual califico al instrumento de ficha de registro como válido, para la especialista Menéndez Muera, Rosa ingeniera de sistema lo cual calificó al

instrumento de ficha de registro como válido, para el especialista Montoya Negrillo, Danny José lo cual califico al instrumento de ficha de registro como valido y para el Doctor Chávez Pinillos, Fredy Elmer califico al instrumento como válido.

Validez de Criterio

Es el criterio que logra medir la relación entre la externa variable, dando a saber que el indicador o índice se esta midiendo con el instrumento considerado.

Validez de Constructo

Es el grado de prueba donde se llega a medir los significados que se les brinda, es así que para este presente estudio se asignara una validez asignada por el juicio de experto.

Confiabilidad

De acuerdo a lo mencionado, la estadística inferencial estudia las técnicas y los procedimientos

Para la medición de confiabilidad del instrumento, se utilizó en el análisis de la confiabilidad, en cual, mediante el cálculo de coeficiente de Alpha de Cronbach, para poder identificar la fiabilidad, donde el coeficiente de Alpha de Cronbach tiende a tomar los valores ente 0 y 1, siendo 0 la fiabilidad nula y 1 la confiabilidad total de datos, para obtener un valor alto en el intervalo de 0.8 y 1.

3.5. Procedimientos

El procedimiento de recolectar datos para el desarrollo de la investigación fue planeado entre los 15 a 30 días del mes de junio con fin de recaudar información necesaria.

Para la recopilación de datos se planteó los lunes a viernes, el tiempo que la empresa Soltesi S.A.C labora, además que el análisis se desarrollará antes y después la aplicación del Sistema de Gestión de la Seguridad de la Información, para cumplir con lo preparado para la recolecta de datos.

Luego de haber recolocado los datos del pretest y postest a través de la ficha de registro, se ingresarán los datos al programa de SPSS, para ver si cumple con lo planteado en la hipótesis, seguidamente mostrar resultados de forma gráfica y en tablas.

3.6. Métodos de Análisis de datos.

Hernández, Fernández, Baptista (2017), “Donde el método de análisis de datos consiste en evaluar los datos requeridos de la población, este proceso realizado en el programa SPSS, donde se realizo el trabajo de generar resultados de acuerdo a los datos analizados, de acuerdo a los objetivos de las hipótesis en la investigación. Por otro lado, el método de análisis se desglosa en dos tipos análisis descriptivo e inferencial”. (p. 38)

De acuerdo al estudio planteado se desarrollará un análisis cuantitativo, donde los resultados obtenidos en las fichas de registro se representarán mediante gráficos que derivan del SPSS.

Análisis Descriptivo

Hernández, Fernández y Baptista (2017), deduce los resultados de los análisis descriptivos, tiende a ser disciplinaria ya que tiene como función ordenar, resumir y analizar el conjunto de los datos mediante técnicas y métodos. (p. 32)

De acuerdo a lo dicho anteriormente la estadística que se describió tiende a ser técnicas y procedimientos que beneficia en mostrar los datos en conjunto donde se mide la mediana moda y media de los datos hallados.

Análisis Inferencial

Hernández, Fernández y Baptista (2017), “El análisis inferencial nos concede extraer resultados sobre la población a partir de los datos obtenidos e la muestra”. (p. 45)

De acuerdo a lo mencionado, la estadística inferencial estudia las técnicas y los procedimientos en esta investigación se utiliza el método T-Student quien tiene como objetivo mostrar la comparación de dos muestras de igual población, ya que la población es menor.

3.7. Aspectos Éticos

Para esta investigación el autor se siente comprometido con los resultados obtenidos de la veracidad y la confiabilidad de los datos que se obtuvieron, con la muestra al final de los resultados. Lo cual considero que las normas aplicables para la redacción del marco teórico se citan adecuadamente a los aportes de los investigadores citados.

De acuerdo a lo dicho el proyecto se realiza dentro de los alineamientos comunicada por la oficina de la investigación y la Escuela Profesional de Ingeniera de Sistema de la Universidad Cesar Vallejo Sede Atea (Resolución de consejo Universitario N°0389 2017 UCV).

Proporcionados por la oficina de investigación y la Escuela profesional de Ingeniería de Sistema de la Universidad Cesar Vallejo Sede Ate (Resolución de Consejo Universitario N° 0389 2017 UCV). Se desarrolla la investigación que cumple con los requerimientos del diseño cuantitativo de enfoque científico.

El presente estudio tiene especial cuidado en el uso de los conceptos teóricos y bibliográficos de otros autores (Decreto legislativo N°822 Ley sobre el derecho de autor). Se redacta de manera clara cada uno de estos aportes siguiendo la normativa del ISO 690 – 2, referenciado a sus autores y modo de obtención del material.

La investigación valida la selección de la mitología a implementar para la variable independiente. Sistema de Gestión de la Seguridad de la Información. En base a la evaluación de expertos. Los expertos responderán a un documento de validación de la metodología, permitiendo optar por la

metodología mas apropiada para la investigación.

Finalmente, el estudio presenta la información acerca de la empres SOLTESI S.A.C. la información asociada fue tratado bajo los lineamientos. La ley 29733 Ley de Tratamiento de Datos Personales, a fin de conservar la integridad de la misma y la transparencia en los fines para los cuales son dispuestos (ISO / IEC 29100)

IV RESULTADOS

Análisis descriptivo

Para esta investigación donde se llevó a cabo un S.G.S.I. en la empresa Soltesi S.A.C. en el distrito de Jesús María, así mismo se aplicó un Pre-Test en la cual ayudo a mostrar las principales condiciones de los indicadores, siguiendo a ello se puso en marcha la normativa ISO 27001 para el mejoramiento en la integridad, disponibilidad e confidencialidad de los datos.

Tabla 2 *Estadísticas de muestras pretest y postest de la dimensión Seguridad*

Estadísticas de muestras emparejadas

		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	PreTest_Seguridad	21,5547	22	5,29890	1,12973
	Postest_Seguridad	79,3427	22	5,86475	1,25037

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

En este caso de la dimensión seguridad, dado que el pre-test se llegó a obtener un valor media de 21.55% incidencias atendidas en la empresa Soltesi S.A.C. por mes, así mismo en el post-test la media fue de 79.34% de incidencias atendidas en la empresa Soltesi S.A.C. por mes, donde se visualiza que existe una diferencia abismal en las cantidades de incidencias atendidas durante un mes, eso antes de implementar el SGSI con la Normativa ISO 27001.

INDICADOR: INTEGRIDAD

De acuerdo a los resultados estadísticos conseguidos como descriptivo en la integridad de datos se describe en la tabla siguiente.

Medidas descriptivas de la integridad de datos donde muestra un antes y un después de la implementación de la auditoria en el sistema.

Tabla 3 *Estadísticas de muestras pretest y postest indicador integridad*

Estadísticas de muestras emparejadas

		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Pre Test Integirdad	32,2805	22	10,88603	2,32091
	Post Test Integridad	75,1518	22	11,75769	2,50675

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

En la tabla, se muestra las incidencias de integridad de datos, dado en el Pre-Test donde se muestra con un valor de media 32,28 por incidencias en 1 mes, por lo tanto, en el post Post-Test la media fue de 75,15 por incidencias en 1 mes, donde se ve una gran escala de diferencia del antes y después que sea implementado el SGSI con la Norma ISO 27001.

INDICADOR: CONFIDENCILIDAD

De acuerdo a los resultados estadísticos conseguidos como descriptivo en la integridad de datos se describe en la tabla siguiente.

Medidas descriptivas de la integridad de datos donde se muestra un antes y un después de la implementación de la auditoria en el sistema.

Tabla 4 *Estadísticas de muestras pretest y postest indicador confidencialidad*

Estadísticas de muestras emparejadas

		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Pre Test Confidencialidad	15,2177	22	7,06705	1,50670
	Post Test Confidencialidad	80,9773	22	10,42357	2,22231

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

En la tabla, se muestra las incidencias de integridad de datos, dado en el Pre-Test donde se muestra con un valor de media 15,21 por incidencias en 1 mes, por lo tanto, en el post Post-Test la media fue de 80,97 por incidencias en 1 mes, donde se ve una gran escala de diferencia del antes y después que sea implementado el SGSI con la Norma ISO 27001.

INDICADOR: DISPONIBILIDAD

De acuerdo a los resultados estadísticos conseguidos como descriptivo en la integridad de datos se describe en la tabla siguiente.

Medidas descriptivas de la integridad de datos donde se muestra un antes y un después de la implementación de la auditoria en el sistema.

Tabla 5 *Estadísticas de muestras pretest y postest indicador disponibilidad*

Estadísticas de muestras emparejadas

		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Pre Test Disponibilidad	17,1659	22	8,24837	1,75856
	Post Test Disponibilidad	81,8991	22	12,98795	2,76904

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

En la tabla, se muestra las incidencias de integridad de datos, dado en el Pre-Test donde se muestra con un valor de media 17,16 por incidencias en 1 mes, por lo tanto, en el post Post-Test la media fue de 81,89 por incidencias en 1 mes, donde se ve una gran escala de diferencia del antes y después que sea implementado el SGSI con la Norma ISO 27001.

Análisis Inferencial

Prueba de Normalidad:

La prueba de normalidad que se seleccionó fue shapiro Wilk, ya que mi muestra es de 22 ficha de registros, ya que es menor a 50 elementos. Se realizo mediante los

3 indicadores, cada uno con sus respectivos ficha de registro con un ítem de 22 registros cada uno, así mismo se realizó el análisis de la prueba de normalidad para hallar la prueba de hipótesis para la investigación.

Luego de recolectar información con la ficha de registro, se ingresó los datos estadísticos al programa IBM SPSS con las siguientes condiciones.

- Distribución paramétrica o normal (>0.05)
- Distribución No paramétrica o no normal (<0.05)

Se dio a conocer los resultados siguientes:

INDICADOR: INTEGRIDAD

Acuerdo a los datos para el indicador de integridad entre el (Pre-Test y Post-Test) tiende a contar con una distribución normal.

Para esta prueba de normalidad para el indicador integridad se muestra en la siguiente imagen el antes y después de implementar un SGSI ISO 27001.

Tabla 6 *Tabla de prueba de normalidad del indicador Integridad*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pre Test Integirdad	,104	22	,200*	,960	22	,497
Post Test Integridad	,177	22	,072	,923	22	,086

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia del programa SPSS

Según la tabla mostrada, donde valor de significancia en el indicado de integridad antes de implementar un SGSI (Pre-Test), fue de 0.497 siendo así mayor a lo esperado del nivel de la significancia de 0.05, dando así una distribución normal o paramétrica, siguiendo a lo estudiado después de implementar el SGSI, el valor de la significancia fue de 0.086, siendo así mayor a lo esperado del nivel de la significancia de 0.05, dando así una distribución normal o paramétrica.

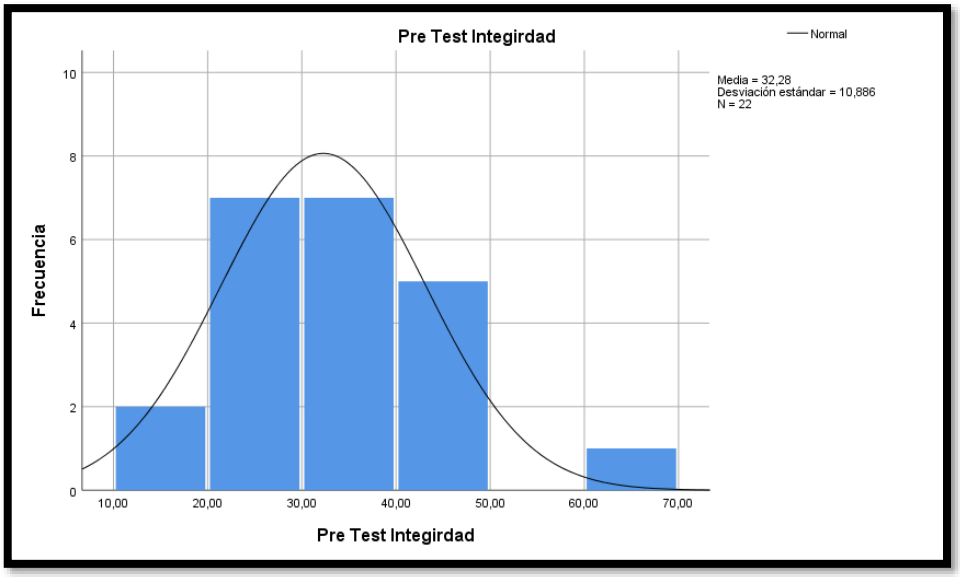


Figura 5 Integridad (Pre-test)

Fuente: Elaboración propia

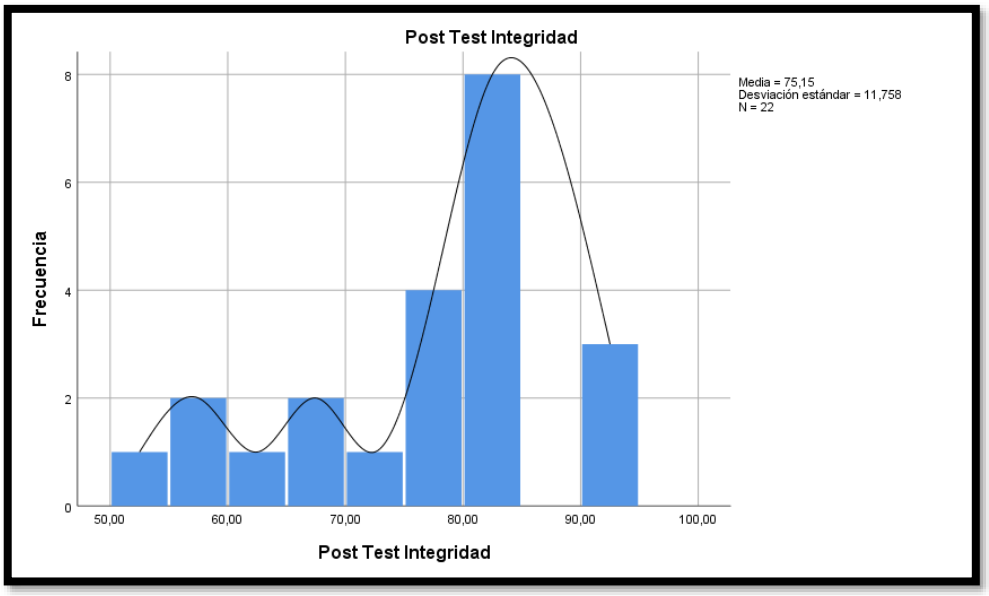


Figura 6 Integridad (Pos-test)

Fuente: Elaboración propia

INDICADOR: CONFIDENCILIDAD

Acuerdo a los datos para el indicador confidencialidad entre el (Pre-Test y Post-Test) tiende a contar con una distribución normal.

Para esta prueba de normalidad del indicador confidencialidad se muestra en la siguiente imagen el antes y después de implementar un SGSI ISO 27001.

Tabla 7 *Tabla de prueba de normalidad del indicador confidencialidad*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pre Test Confidencialidad	,152	22	,200*	,946	22	,261
Post Test Confidencialidad	,135	22	,200*	,929	22	,116

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

Según la tabla, el valor de significancia en el indicado de integridad antes de implementar un SGSI (Pre-Test), fue de 0.261 siendo así mayor a lo esperado del nivel de la significancia de 0.05, dando así una distribución normal o paramétrica, siguiendo a lo estudiado después de implementar el SGSI, el valor de la significancia fue de 0.116, siendo así mayor a lo esperado del nivel de la significancia de 0.05, dando así una distribución normal o paramétrica.

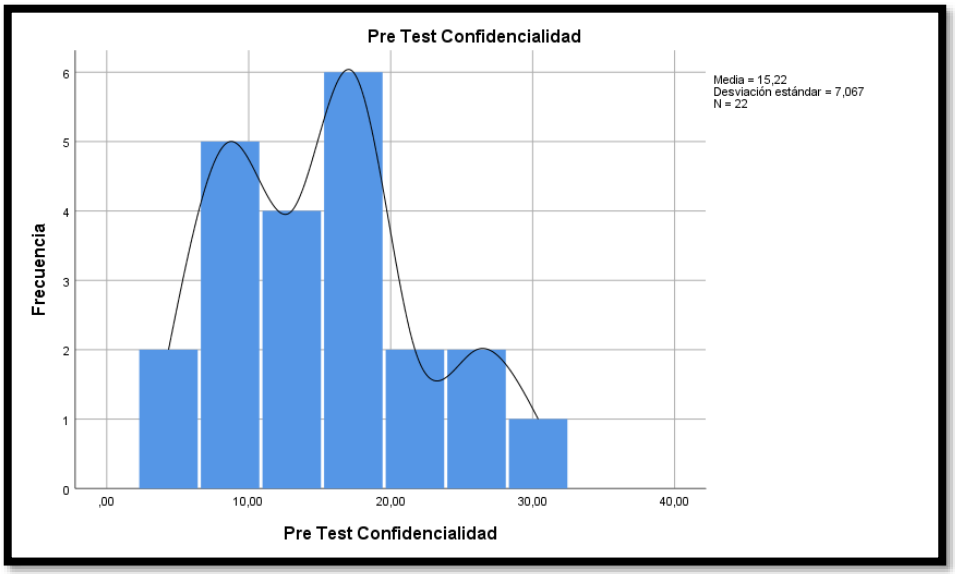


Figura 7 Confidencialidad (Pre-test)

Fuente: Elaboración propia SPSS

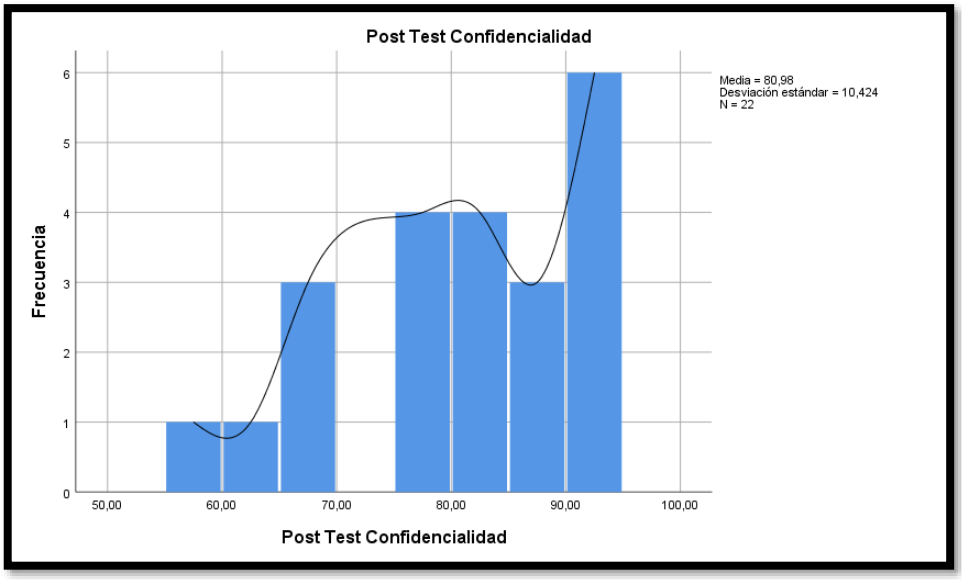


Figura 8 Confidencialidad (Pos-test)

Fuente: Elaboración propia SPSS

INDICADOR: DISPONIBILIDAD

Acuerdo a los datos para el indicador disponibilidad entre el (Pre-Test y Post-Test) tiende a contar con la distribución normal.

Para esta prueba de normalidad del indicador disponibilidad se muestra en la siguiente imagen el antes y después de implementar un SGSI ISO 27001.

Tabla 8 *Tabla de prueba de normalidad del indicador disponibilidad*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pre Test Disponibilidad	,149	22	,200*	,906	22	,040
Post Test Disponibilidad	,206	22	,016	,882	22	,013

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

Según la tabla, el valor de significancia en el indicado de integridad antes de implementar un SGSI (Pre-Test), fue de 0.040 siendo así mayor a lo esperado del nivel de la significancia de 0.05, dando así una distribución normal o paramétrica,

siguiendo a lo estudiado después de implementar el SGSI, el valor de la significancia fue de 0.013, siendo así mayor a lo esperado del nivel de la significancia de 0.05, dando así una distribución normal o paramétrica.

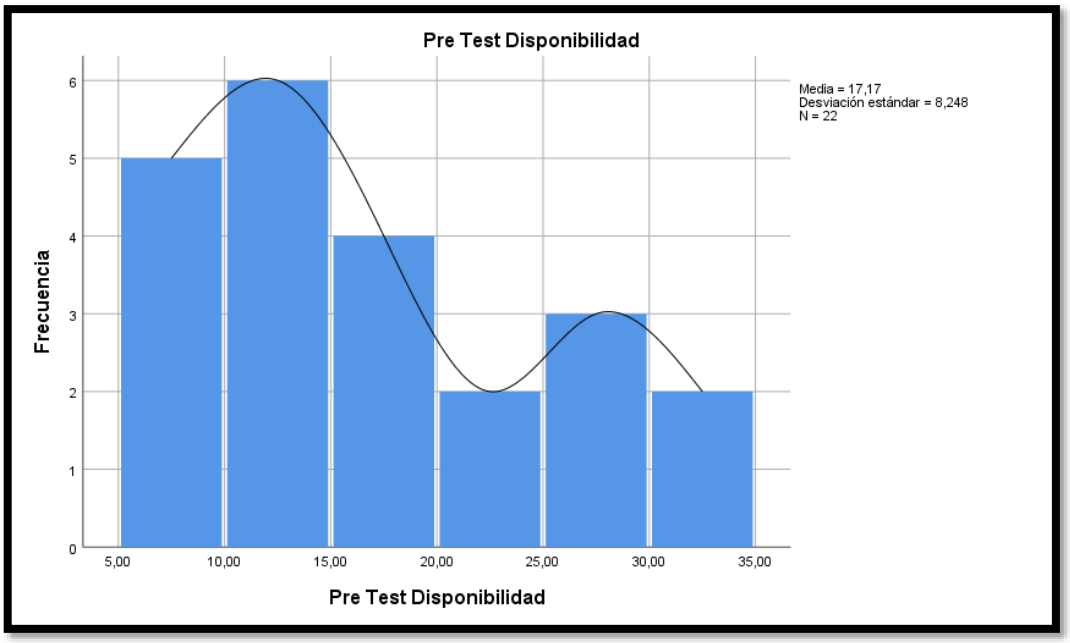


Figura 9 Disponibilidad (Pre-test)

Fuente: Elaboración propia SPSS

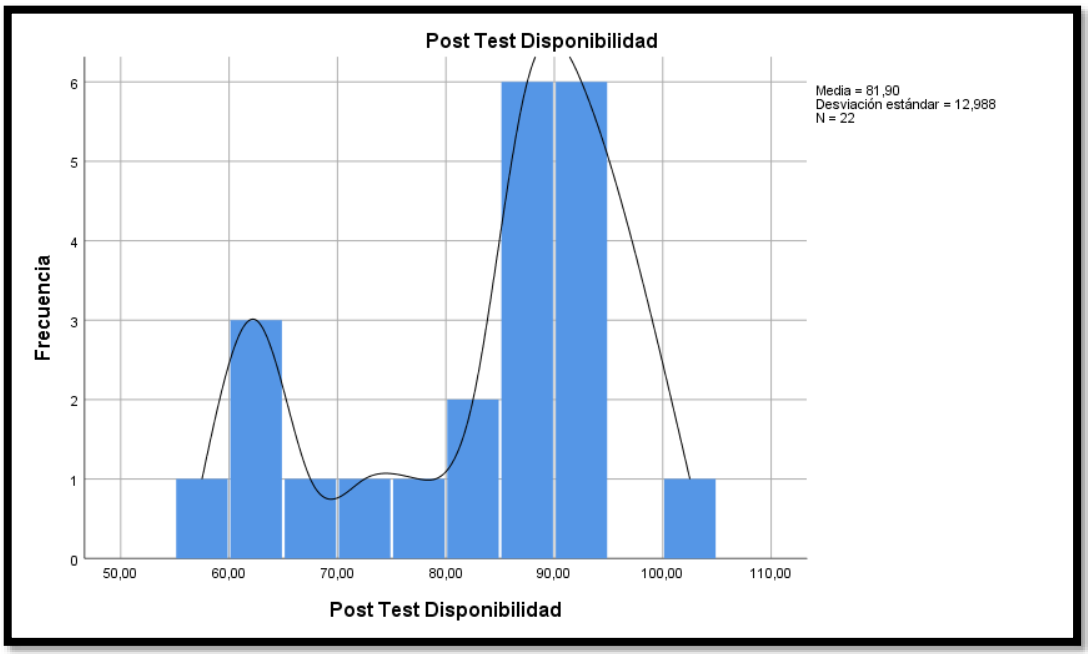


Figura 10 Disponibilidad (Pos-test)

Fuente: Elaboración propia SPSS

Prueba de Hipótesis General

Para esta prueba de hipótesis, se brindó la prueba de T-Student, ya que al realizar un Pre-Test y un Post-tes se obtuvo la distribución es “Normal” y su valor de significancia siendo menor a 0.005, por ello se rechaza la hipótesis Nula y se acepta la hipótesis alterna.

En la tabla siguiente se observa la prueba realizada mediante el T-Student para la dimensión seguridad para la seguridad de la información, el antes y después de ser implementar el SGSI.

HG: El SGSI mejora significativamente con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021.

H0: El SGSI no mejora significativamente con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021.

Tabla 9 *Prueba de Hipótesis para la dimensión seguridad*

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	PreTest_Seguridad - Postest_Seguridad	-57,78803	7,93107	1,69091	-61,30447	-54,27159	-34,176	21	,000

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

- Si la significancia es <0.005, acepta la Hipótesis Alterna.
- Si la significancia es >0.005, rechaza la hipótesis alterna.

Valida dación de Hipótesis.

Luego de haber aplicado la prueba de T-Student, se puede apreciar que la significancia es 0.000, donde está por debajo a 0.005. Por lo tanto, para esta investigación se acepta la Hipótesis Alterna.

Prueba de Hipótesis 1

H1: El SGSI mejora significativamente la Integridad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021.

H0: El SGSI no mejora significativamente la Integridad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021.

Prueba de Hipótesis del indicador Integridad

Para la prueba de hipótesis, se brindó la prueba de T-Student, ya que al realizar un Pre-Test y un Post-tes se obtuvo la distribución es “Normal” y su valor de significancia siendo menor a 0.005, por ello se rechaza la hipótesis Nula y se acepta la hipótesis alterna.

En la tabla siguiente se observa que la prueba realizada mediante el T-Student para la dimensión seguridad para la seguridad de la información, el antes y después de ser implementar el SGSI.

Tabla 10 *Prueba de Hipótesis para el indicador integridad*

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	Pre Test Integirdad - Post Test Integridad	21,23773	21,18089	4,51578	11,84665	30,62881	4,703	21	,000

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

- Si la significancia es <0.005, se acepta la Hipótesis Alterna.
- Si la significancia es >0.005, se rechaza la hipótesis alterna.

Valida dación de Hipótesis.

Luego de haber aplicado la prueba de T-Student, se puede apreciar que la significancia es 0.000, donde está por debajo a 0.005. Por lo tanto, para esta investigación se acepta la Hipótesis Alterna.

Prueba de Hipótesis 2

H2: El SGSI mejora significativamente la confidencialidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021.

H0: El SGSI no mejora significativamente la confidencialidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021.

Prueba de Hipótesis del indicador Confidencialidad

Para esta prueba de hipótesis, se brindó la prueba de T-Student, ya que al realizar un Pre-Test y un Post-tes se obtuvo la distribución es “Normal” y su valor de significancia siendo menor a 0.005, por ello se rechaza la hipótesis Nula y se acepta la hipótesis alterna.

En la tabla siguiente se observa que la prueba realizada mediante el T-Student para la dimensión seguridad para la seguridad de la información, el antes y después de ser implementar el SGSI.

Tabla 11 *Prueba de hipótesis para el indicador confidencialidad*

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	Pre Test Confidencialidad - Post Test Confidencialidad	-65,75955	14,32582	3,05428	-72,11126	-59,40783	-21,530	21	,000

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

Si la significancia es <0.005, se acepta la Hipótesis Alterna.
Si la significancia es >0.005, se rechaza la hipótesis alterna.

Valida dación de Hipótesis.

Luego de haber aplicado la prueba de T-Student, se puede apreciar que el valor de la Significancia es de 0.287, donde es mayor a 0.005. Por lo tanto, para esta investigación se acepta la Hipótesis Alterna.

Prueba de Hipótesis 3

H3: El SGSI mejora significativamente la disponibilidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021.

H0: El SGSI no mejora significativamente la disponibilidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021.

Prueba de Hipótesis del indicador Disponibilidad

Para esta prueba de hipótesis, se brindó la prueba de T-Student, ya que al realizar un Pre-Test y un Post-tes se obtuvo la distribución es “Normal” y su valor de significancia siendo menor a 0.005, por ello se rechaza la hipótesis Nula y se acepta la hipótesis alterna.

En la tabla siguiente se observa que la prueba realizada mediante el T-Student para la dimensión seguridad para la seguridad de la información, el antes y después de ser implementar el SGSI.

Tabla 12 *Prueba de hipótesis para el indicador disponibilidad*

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	Pre Test Disponibilidad - Post Test Disponibilidad	-64,73318	14,01104	2,98716	-70,94533	-58,52104	-21,670	21	,000

Fuente: Tabla de resultados del total de incidencias resueltas SPSS

- Si la significancia es <0.005, acepta la Hipótesis Alterna.
- Si la significancia es >0.005, rechaza la hipótesis alterna.

Valida dación de Hipótesis.

Luego de haber aplicado la prueba de T-Student, se puede apreciar que el valor de la Significancia es de 1.26, donde es menor a 0.005. Por lo tanto, para esta investigación se acepta la Hipótesis Alterna.

V DISCUSIÓN

Posterior a desarrollo del proyecto de investigación y a los resultados obtenidos de los análisis estadísticos. Se efectuó la comparación, seguidamente la discusión que en el contraste se origina.

A partir de los hallazgos encontrados, se comprobó que la hipótesis propuesta, se afirma que el SGSI mejora significativamente con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021, donde se obtuvo como resultado que antes de ser implementado el SGSI el 21,55% de incidencias son atenidas durante 1 mes, y luego de implementar un SGSI se obtuvo como resultado que el 79,34% de incidencias son atendidas durante 1 mes y teniendo un nivel de significancia siendo menor a 0.005. Ante estos resultados podemos deducir que la el SGSI con ISO 27001 viene mitigando riesgos de vulnerabilidades ante posibles ataques.

De igual manera la hipótesis del indicador integridad, se afirmó que el SGSI mejora significativamente la integridad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021, donde se obtuvo como resultado que antes de ser implementado el SGSI el 32.28% de incidencias son atenidas durante 1 mes, y luego de implementar un SGSI se obtuvo como resultado que el 75.15% de incidencias son atendidas durante 1 mes y teniendo un nivel de significancia siendo menor a 0.005. Ante estos resultados podemos deducir que la el SGSI con ISO 27001 viene mitigando riesgos de vulnerabilidades ante posibles ataques.

Así mismo en la hipótesis del indicador confidencialidad, se afirmó que el SGSI mejora significativamente la confidencialidad con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María 2021, donde se obtuvo como resultado que antes de ser implementado el SGSI el 15,21% de incidencias son atenidas durante 1 mes, y luego de implementar un SGSI se obtuvo como resultado que el 80.97% de incidencias son atendidas durante 1 mes y teniendo un nivel de significancia siendo menor a 0.005. Ante estos resultados podemos deducir que la el SGSI con ISO 27001 viene mitigando riesgos de vulnerabilidades ante posibles ataques.

Como ultimo la hipótesis del indicador disponibilidad, se afirmó que el SGSI mejora significativamente la disponibilidad con ISO 27001 en la empresa Soltesi S.A.C. del

distrito de Jesús María 2021, donde se obtuvo como resultado que antes de ser implementado el SGSI el 17.16% de incidencias son atenidas durante 1 mes, y luego de implementar un SGSI se obtuvo como resultado que el 81.89% de incidencias son atendidas durante 1 mes y teniendo un nivel de significancia siendo menor a 0.005. Ante estos resultados podemos deducir que la el SGSI con ISO 27001 viene mitigando riesgos de vulnerabilidades ante posibles ataques.

De momento que la seguridad de la información mejoro la calidad de seguridad, por ello Guevara (2018) realizo una investigación a las normas de seguridad indico que si ayuda en la calidad de resguardar la seguridad basándose en los parámetros de la Norma ISO 27001, teniendo en cuenta los pilares como la confiabilidad, disponibilidad e integridad como punto de partida, de acuerdo a lo estudiado sostuvo que obtuvo como resultado que mejoro un 64,11% la calidad de seguridad de la información regularizando todo los procesos de desgaste que se viene mostrando en los incidentes de error que se encuentre en la empresa.

Como resultados comparativos de Guevara (2018) se determinó que la empresa en el estado actual que se encontraba su población del 9.1% no tenían regencia alguna sobre las normas de laborales en cuanto a los protocolos de seguridad de información, ya posteriormente aplicada el SGSI se obtuvo que el 90% de la población conocían sobre los riesgos de mitigación de errores en la empresa, logrando así que la empresa tiende a disminuir el margen de error que se generaba ya sea por perdida de información o por no tener conocimiento de políticas de seguridad.

Así mismo Mercedes (2017) comprobó los reportes entregados utilizando el sistema web de la gestión de seguridad de la información mejora un 25.61%, así mismo sin el sistema web fue de 72.33% y con el uso del sistema web la media fue de 97.94%, eso quiere decir que la administración de la seguridad de la información si mejora la confidencialidad e disponibilidad de los datos generados por la página web.

VI CONCLUSIONES

1. Para esta investigación se tendió en cuenta que la implementación de un SGSI, basado en la Norma ISO 27001 genera un cambio abismal en la seguridad de la información, donde antes de ser implementada el SGSI tiene un 21,55% de incidencias resueltas durante 1 mes y después de ser implementada el SGSI se obtuvo que un 79,34% de incidencias son resultas, logrando así disminuir los riesgos de perdida de información en la empresa.

2. Respecto al indicador integridad de la Norma ISO 27001 en la empresa Soltesi S.A.C. Jesús María 2021, sin haber implementado el SGSI, tiene una media de 32.28% de incidencias son resueltas por mes, de otra manera después de implementar un SGSI basado en la Normal ISO 27001, se tiene como media que el 75.15% de incidencias son resultas por mes. Por lo tanto, el SGSI si tiene efecto positivo en las incidencias resultas por cada mes.

3. En cuanto al indicador confidencialidad de la Norma ISO 27001 en la empresa Soltesi S.A.C. Jesús María 2021, sin haber implementado el SGSI, tiene una media de 15.21% de incidencias resueltas por mes, de otra manera después de implementar un SGSI basado en la Normal ISO 27001, se tiene como media que el 80.97% de incidencias son resueltas por mes. Por lo tanto, el SGSI si tiene efecto positivo en las incidencias resultas por cada mes.

4. Así mismo el indicador disponibilidad de la Norma ISO 27001 en la empresa Soltesi S.A.C. Jesús María 2021, sin haber implementado el SGSI, tiene una media de 17.16% de incidencias son resueltas por mes, de otra manera después de implementar un SGSI basado en la Normal ISO 27001, se tiene como media que el 81.89% de incidencias son resueltas por mes. Por lo tanto, el SGSI si tiene efecto positivo en las incidencias resultas por cada mes.

VII RECOMENDACIONES

1. Se sugiere que se implemente un área de sistema que se encargue de la seguridad de todas las áreas de la empresa, ya que cada área necesita de mantenimiento por semana en caso de que ocurra alguna incidencia o problema que afecte el rendimiento de la empresa o del trabajador.

2. Otro factor importante es realizar actualizaciones semanales de cada área, tanto como en la Base de Datos, como también en los servidores e computadoras de trabajo, ya que los ataques cibernéticos viene siendo más fuerte, como ejemplo el phishing, Malware, Inyecciones SQL, etc., que son los principales herramientas usadas por el ciber ataque utilizando cada año y en cada evento informático de ejemplo el Bono 2020 que brindo el estado en pandemia del COVID.

3. Como bien dicen que la seguridad es primero, se recomienda brindar tanto una seguridad a los trabajares dentro de la empresa, eso que quiere decir, en instalar cámaras de vigilancia, para poder vigilar tanto a la empresa como a los trabajares, si en caso de que suceda algo y la seguridad de vigilancia viene siendo observada se da aviso para poder acercarse al personal que se encuentre en peligro o este efectuando algún hecho prejuicioso.

4. Hoy en día la tecnología viene siendo muy avanzada es por ello que la información ya no es segura en las computadores o almacenamiento físicos, es por ello que se recomienda utilizar las nubes como servidores para la empresa o como almacenamiento, así mismo se realiza menor campo posible en ya no usar servidores físicos, sino servidores dirigidos por otras empresas que brindan servicio de nube(internet).

REFERENCIAS

ABREGO, Demian, SÁNCHEZ, Yesenia, MEDINA, José; 2017, Influencia de los sistemas de información en los resultados organizacionales, SciELO Analytics, Vol. 62, N° 2; p. 32.

ALCÁNTARA, Julio. 2015. Guía de Implementación de la Seguridad basado en ISO/IEC 27001, para apoyar la seguridad en los Sistemas de Información de la Comisaría norte P.N.P. en la ciudad de Chiclayo. PERÚ: Universidad Católica Santo Toribio de Mogrovejo, 2015. 157pp

ARÉVALO, José, BAYONA, Ramón, RICO, Dewar, 2015, Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información, Udistrital, Vol. 19 N°. 46, pp. 123-134

BACA, Gabriel. Introducción de la seguridad informática. 1.a ed. patria: 35pp. México: Universidad Autónoma, 2016.

ISBN: 9786077444718

BAHID, Eugenia. Scrum y extreme programing para programadores, pp. 162, 2012. Buenos Aires, Argentina.

CALDER, Alan, Nuevos pasos para el éxito Una visión de conjunto para la aplicación de la ISO 27001:2013. Reino Unido: IT Governance Publishing, 2014.

ISBN: 978-1-84928-929-0

CUERVO, Sara. Implementación ISO 27001, Madrid: Empresa Ficticia S.A. , 2017. 115 pp.

GÓMEZ, Álvarez. Enciclopedia de la seguridad informática. 3ra ed. Ra-Ma: España, 2017. 120pp.

ISBN: 9788499643946

GÓMEZ, Álvaro y Suárez, Carlos. 2011. Sistemas de Información. Herramientas prácticas para la gestión (3ª. ed.) MEXICO: Alfa y Omega Grupo Editor, 2011. 360pp. ISBN: 978-607-7854-45-6

Metodología de Investigación científica, por HERNÁNDEZ Arturo [et al.] 1ra Edición, Área de innovación y desarrollo 2018-

ISBN 978-84-948257-0-5

MARBAISE, Magali, El modelo de canvas. Ed c2017. Española: España 2017. 136pp.

ISBN: 978-2-8-0628-058-9

PÉREZ, Julio, Protección de datos y seguridad de la información, 4ta ed. 2015, Madrid, España, pp. 192.

ISBN: 978-84-9964-560-5

PIATTINI, Mario, CALERO, Coral y MORAGA, Ángeles. Calidad de producto y proceso de software. 5.a ed. Ra-Ma: España, 2015. 666pp.

ISBN: 9788478979615

RIAÑO, Martha, HOYOS, Eduardo, VALERO, Ivone, 2016, Evolución de un sistema de gestión de seguridad y salud en el trabajo e impacto en la accidentalidad laboral: Estudio de caso en empresas del sector petroquímico en Colombia, SciELO Analytics, Vol. 18, N° 55, p. 72.

SAMPIERI, Carlos. Metodología de la investigación, 6ta Edición, Punta Santa Fe, México: Industria Editorial Mexicana, Reg. Núm. 736, 2014 ,169 pp.

ISBN: 978-1-4562-2396-0

SCRUMSTUDY, Cuerpo y conocimiento de Scrum (Guía SBOK). 3era ED, Indian School Road, Arizona, 2017, 353pp.

ISBN: 978-0-9899252-0-4

TEJADA, Ester, Gestión de incidentes de seguridad informática.1ra Edición, Malaga: IC Editorial 2014, pp 234.
ISBN: 978-84-16351-70-1

VALENCIA, Francisco, OROZCO, Mauricio, Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000, Revista lbérica de Sistemas y Tecnologías de Información, Vol. 2014, N.º 22, pp. 78.

ANEXOS

Anexo 2: Matriz de operacionalización

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Ítems / Formula	Instrumento	Escala de Medición
Seguridad de la Información	Según Baca (2016) La seguridad Informática es la disciplina que, con base a políticas, 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 seguro, ante cualquier tipo de amenazas, logrando minimizar los riesgos tanto físicos como lógicos. (p. 11)	Esta variable se medirá 1 dimensión seguridad de la información y sus 3 indicadores confidencialidad, disponibilidad y integridad, en donde se utilizará la ficha de registro de registro como instrumento que está conformado por 22 registros de incidencias que fueron dirigidos para los trabajos de la empresa Soltesi S.A.C. para medir la seguridad de la información.	Seguridad	Confidencialidad	Según: Jeimy J. $PIC = \frac{N°IC}{TI}$ **PIC=** Porcentaje de incidencia de confidencialidad **N°IC=** Numero de incidencia de confidencialidad **TI=** Total de incidencia	Ficha de registro	Razón
				Integridad	Según: Jeimy J. $PII = \frac{N°II}{TI}$ **PII=** Porcentaje de incidencia de integridad **N°II=** Numero de incidencia de integridad **TI=** Total de incidencia		
				Disponibilidad	Según: Jeimy J. $PID = \frac{N°ID}{TI}$ **PID=** Porcentaje de incidencia de disponibilidad **N°ID=** Numero de incidencia de disponibilidad **TI=** Total de incidencia		

Anexo 3: Matriz de consistencia

<table>
<tr><th>PROBLEMA</th><th>OBJETIVO</th><th>HIPÓTESIS</th><th>VARIABLES</th><th>DIMENSIONES</th><th>INDICADOR</th><th>METODOLOGÍA</th></tr>
<tr><td>GENERAL</td><td>GENERAL</td><td>GENERAL</td><td>INDEPENDIENTES</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="6">Tipo de Investigación:

Aplicada

Diseño de Investigación:

Experimental

Población:

22 personas

Muestra:

22 registros</td></tr>
<tr><td>Cuál es el nivel del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td>Determinar la influencia del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td>El SGSI mejora significativamente con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td>Sistema de Gestión de la Seguridad de la Información (SGSI)</td></tr>
<tr><td>ESPECIFICO</td><td>ESPECIFICO</td><td>ESPECIFICO</td><td>DEPENDIENTES</td><td></td><td></td></tr>
<tr><td>Cuál es el nivel de integridad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td>Determinar la influencia de la integridad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td>El SGSI mejora significativamente la integridad de la seguridad de información en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td rowspan="2">ISO 27001</td><td rowspan="2">Seguridad</td><td>integridad</td></tr>
<tr><td>Cuál es el nivel de confidencialidad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td>Determinar la influencia de la confidencialidad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td>El SGSI mejora significativamente la confidencialidad de la seguridad de información en la empresa Soltesi S.A.C. del distrito de Jesús María</td><td>Confidencialidad</td></tr>
</table>

Cuál es el nivel de disponibilidad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María	Determinar la influencia de la disponibilidad del SGSI con ISO 27001 en la empresa Soltesi S.A.C. del distrito de Jesús María.	El SGSI mejora significativamente la disponibilidad de la seguridad de información en la empresa Soltesi S.A.C. del distrito de Jesús María.			Disponibilidad	**Muestreo:** No probabilístico

Anexo 4: Ficha de Registro

FICHA DE REGISTRO			
OBJETIVO:	Determinar la influencia de la integridad del SGSI de la seguridad en la información en la empresa Soltesi S.A.C. del distrito de Jesús María		
INDICADOR:	Porcentaje de Incidencias resueltas en primer nivel		
INVESTIGADOR:	Poma Ramos Alexander	Tipo de prueba	Pre Test
EMPRESA:	Soltesi S.A.C.		
PROCESO OBSERVADO:	Gestión de Incidencia Integridad		
FORMULA:	$PII = \frac{N°II}{TI}$	**PII=** Porcentaje de incidencia de integridad **N°II=** Numero de incidencia de integridad **TI=** Total de incidencia	

Ítem	Fecha	N° II	TI	PII
1	07/10/19	2	10	20.00
2	08/10/19	5	15	33.33
3	09/10/19	5	19	26.32
4	10/10/19	3	22	13.64
5	11/10/19	4	12	33.33
6	12/10/19	4	14	28.57
7	14/10/19	6	18	33.33
8	15/10/19	6	20	30.00
9	16/10/19	8	19	42.11
10	17/10/19	4	17	23.53
11	18/10/19	2	15	13.33
12	16/10/19	4	16	25.00
13	21/10/19	5	14	35.71
14	22/10/19	5	12	41.67
15	23/10/19	6	13	46.15
16	24/10/19	2	8	25.00
17	25/10/19	4	10	40.00
18	26/10/19	8	13	61.54
19	28/10/19	4	10	40.00
20	29/10/19	5	14	35.71
21	30/10/19	4	14	28.57
22	31/10/19	6	18	33.33

FICHA DE REGISTRO				
OBJETIVO:	Determinar la influencia de la integridad del SGSI de la seguridad en la información en la empresa Soltesi S.A.C. del distrito de Jesús María			
INDICADOR:	Porcentaje de Incidencias resueltas en primer nivel			
INVESTIGADOR:	Poma Ramos Alexander	Tipo de prueba	Post Test	
EMPRESA:	Soltesi S.A.C.			
PROCESO OBSERVADO:	Gestión de Incidencia Integridad			
FORMULA:	$PII = \frac{N°II}{TI}$	**PII=** Porcentaje de incidencia de integridad **N°II=** Numero de incidencia de integridad **TI=** Total de incidencia		

Ítem	Fecha	N° II	TI	PII
1	04/11/19	9	10	90.00
2	05/11/19	5	6	83.33
3	06/11/19	6	8	75.00
4	07/11/19	10	11	90.91
5	08/11/19	5	9	55.56
6	09/11/19	3	4	75.00
7	11/11/19	4	5	80.00
8	12/11/19	4	6	66.67
9	13/11/19	5	9	55.56
10	14/11/19	10	11	90.91
11	15/11/19	8	10	80.00
12	16/11/19	10	12	83.33
13	18/11/19	6	10	60.00
14	19/11/19	4	5	80.00
15	20/11/19	9	11	81.82
16	21/11/19	5	6	83.33
17	22/11/19	2	3	66.67
18	23/11/19	7	10	70.00
19	25/11/19	10	12	83.33
20	26/11/19	10	13	76.92
21	27/11/19	4	8	50.00
22	28/11/19	3	4	75.00

FICHA DE REGISTRO				
OBJETIVO:	Determinar la influencia de la confidencialidad del SGSI de la seguridad en la información en la empresa Soltesi S.A.C. del distrito de Jesús María			
INDICADOR:	Porcentaje de Incidencias resueltas en primer nivel			
INVESTIGADOR:	Poma Ramos Alexander	Tipo de prueba	Pre Test	
EMPRESA:	Soltesi S.A.C.			
PROCESO OBSERVADO:	Gestión de Incidencia de la Confidencialidad			
FORMULA:	$PIC = \frac{N°IC}{TI}$	**PIC=** Porcentaje de incidencia de confidencialidad **N°IC=** Numero de incidencia de confidencialidad **TI=** Total de incidencia		

Ítem	Fecha	N° IC	TI	PIC
1	07/10/19	2	23	8.70
2	08/10/19	3	18	13.04
3	09/10/19	5	26	21.74
4	10/10/19	2	18	8.70
5	11/10/19	1	15	4.35
6	12/10/19	4	22	17.39
7	14/10/19	2	10	8.70
8	15/10/19	6	16	26.09
9	16/10/19	4	19	17.39
10	17/10/19	3	21	13.04
11	18/10/19	4	16	17.39
12	16/10/19	2	10	8.70
13	21/10/19	1	13	4.35
14	22/10/19	5	16	21.74
15	23/10/19	4	19	17.39
16	24/10/19	2	14	8.70
17	25/10/19	3	13	13.04
18	26/10/19	7	26	30.43
19	28/10/19	4	20	17.39
20	29/10/19	6	16	26.09
21	30/10/19	3	14	13.04
22	31/10/19	4	23	17.39

FICHA DE REGISTRO				
OBJETIVO:	Determinar la influencia de la confidencialidad del SGSI de la seguridad en la información en la empresa Soltesi S.A.C. del distrito de Jesús María			
INDICADOR:	Porcentaje de Incidencias resueltas en primer nivel			
INVESTIGADOR:	Poma Ramos Alexander	Tipo de prueba	Post Test	
EMPRESA:	Soltesi S.A.C.			
PROCESO OBSERVADO:	Gestión de Incidencia de la Confidencialidad			
FORMULA:	$PIC = \frac{N°IC}{TI}$	**PIC=** Porcentaje de incidencia de confidencialidad **N°IC=** Numero de incidencia de confidencialidad **TI=** Total de incidencia		

Ítem	Fecha	N° IC	TI	PIC
1	04/11/19	10	13	76.92
2	05/11/19	15	16	93.75
3	06/11/19	13	15	86.67
4	07/11/19	11	16	68.75
5	08/11/19	9	13	69.23
6	09/11/19	11	14	78.57
7	11/11/19	12	16	75.00
8	12/11/19	8	13	61.54
9	13/11/19	10	12	83.33
10	14/11/19	15	16	93.75
11	15/11/19	12	15	80.00
12	16/11/19	14	18	77.78
13	18/11/19	9	10	90.00
14	19/11/19	11	16	68.75
15	20/11/19	14	16	87.50
16	21/11/19	12	13	92.31
17	22/11/19	13	15	86.67
18	23/11/19	10	17	58.82
19	25/11/19	11	13	84.62
20	26/11/19	16	19	84.21
21	27/11/19	14	15	93.33
22	28/11/19	18	20	90.00

FICHA DE REGISTRO				
OBJETIVO:	Determinar la influencia de la disponibilidad del SGSI de la seguridad en la información en la empresa Soltesi S.A.C. del distrito de Jesús María			
INDICADOR:	Porcentaje de Incidencias resueltas en primer nivel			
INVESTIGADOR:	Poma Ramos Alexander	Tipo de prueba	Pre Test	
EMPRESA:	Soltesi S.A.C.			
PROCESO OBSERVADO:	Gestión de Incidencia de la Disponibilidad			
FORMULA:	$PID = \frac{N°ID}{TI}$	**PIC=** Porcentaje de incidencia de disponibilidad **N°ID=** Numero de incidencia de disponibilidad **TI=** Total de incidencia		

Ítem	Fecha	N° ID	TI	PID
1	07/10/19	2	23	8.70
2	08/10/19	3	16	18.75
3	09/10/19	4	15	26.67
4	10/10/19	6	18	33.33
5	11/10/19	5	20	25.00
6	12/10/19	1	13	7.69
7	14/10/19	2	18	11.11
8	15/10/19	3	22	13.64
9	16/10/19	5	21	23.81
10	17/10/19	6	18	33.33
11	18/10/19	3	23	13.04
12	16/10/19	2	25	8.00
13	21/10/19	5	24	20.83
14	22/10/19	3	28	10.71
15	23/10/19	2	24	8.33
16	24/10/19	4	22	18.18
17	25/10/19	6	21	28.57
18	26/10/19	3	20	15.00
19	28/10/19	3	21	14.29
20	29/10/19	2	18	11.11
21	30/10/19	2	24	8.33
22	31/10/19	5	26	19.23

FICHA DE REGISTRO			
OBJETIVO:	Determinar la influencia de la disponibilidad del SGSI de la seguridad en la información en la empresa Soltesi S.A.C. del distrito de Jesús María		
INDICADOR:	Porcentaje de Incidencias resueltas en primer nivel		
INVESTIGADOR:	Poma Ramos Alexander	Tipo de prueba	Post Test
EMPRESA:	Soltesi S.A.C.		
PROCESO OBSERVADO:	Gestión de Incidencia de la Disponibilidad		
FORMULA:	$PID = \frac{N°ID}{TI}$	**PIC=** Porcentaje de incidencia de disponibilidad **N°ID=** Numero de incidencia de disponibilidad **TI=** Total de incidencia	

Ítem	Fecha	N° ID	TI	PID
1	04/11/19	10	12	83.33
2	05/11/19	11	16	68.75
3	06/11/19	9	15	60.00
4	07/11/19	12	13	92.31
5	08/11/19	13	14	92.86
6	09/11/19	11	12	91.67
7	11/11/19	9	15	60.00
8	12/11/19	12	13	92.31
9	13/11/19	13	15	86.67
10	14/11/19	11	14	78.57
11	15/11/19	10	16	62.50
12	16/11/19	10	14	71.43
13	18/11/19	12	12	100.00
14	19/11/19	13	15	86.67
15	20/11/19	14	17	82.35
16	21/11/19	12	14	85.71
17	22/11/19	16	18	88.89
18	23/11/19	18	19	94.74
19	25/11/19	13	14	92.86
20	26/11/19	16	18	88.89
21	27/11/19	10	18	55.56
22	28/11/19	12	14	85.71

Anexo 5: Formato de validación de instrumentos firmados

UCV UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL ISNTRUMENTO QUE MIDE:

N°	DIMENSIONES / ítems		Pertinencia		Relevancia		Claridad		Sugerencias
1	DIMENSIONES: Integridad		Si	No	Si	No	Si	No	
	Según Cano: **PII=** Porcentaje de incidencia de integridad **N°II=** Numero de incidencia de integridad **TI=** Total de incidencia	$PII = \frac{N°II}{TI}$	X		X		X		
2	DIMENSIONES: Confidencialidad		Si	No	Si	No	Si	No	
	Según Cano: **PIC=** Porcentaje de incidencia de confidencialidad **N°IC=** Numero de incidencia de confidencialidad **TI=** Total de incidencia	$PIC = \frac{N°IC}{TI}$	X		X		X		
3	DIMENSIONES: Disponibilidad		Si	No	Si	No	Si	No	
	Según Cano: **PID=** Porcentaje de incidencia de disponibilidad **N°ID=** Numero de incidencia de disponibilidad **TI=** Total de incidencia	$PID = \frac{N°ID}{TI}$	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: Montoya Negrillo, Dany Jose DNI: 10857517

Especialidad del validador: Mg. en Sistemas

25 de 11 del 2019

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** 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 Informante

UCV UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL ISNTRUMENTO QUE MIDE:

N°	DIMENSIONES / ítems		Pertinencia		Relevancia		Claridad		Sugerencias
1	DIMENSIONES: Integridad		Si	No	Si	No	Si	No	
	Según Cano: **PII=** Porcentaje de incidencia de integridad **N°II=** Numero de incidencia de integridad **TI=** Total de incidencia	$PII = \frac{N°II}{TI}$	X		X		X		
2	DIMENSIONES: Confidencialidad		Si	No	Si	No	Si	No	
	Según Cano: **PIC=** Porcentaje de incidencia de confidencialidad **N°IC=** Numero de incidencia de confidencialidad **TI=** Total de incidencia	$PIC = \frac{N°IC}{TI}$	X		X		X		
3	DIMENSIONES: Disponibilidad		Si	No	Si	No	Si	No	
	Según Cano: **PID=** Porcentaje de incidencia de disponibilidad **N°ID=** Numero de incidencia de disponibilidad **TI=** Total de incidencia	$PID = \frac{N°ID}{TI}$	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: Zaruqui Briceño, Carlos DNI: 18172264

Especialidad del validador: Esp. Sistemas

21 de 11 del 2019

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados

Firma del Experto Informante

Anexo 6: Carta de compromiso

UNIVERSIDAD CÉSAR VALLEJO

CARTA DE COMPROMISO

Yo Alexander Poma Ramos identificado con DNI 73951658 y con código 6500089126 de la Escuela Profesional de Ingeniería de Sistema por ***mutuo acuerdo, en libertad y por iniciativa propia,*** *he decidido* realizar el **PROYECTO DE INVESTIGACION** que tiene por título:

SGSI PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA SOLTESI S.A.C. DE JESÚS MARÍA

Soy conciente y tengo conocimiento:

1.- Que, el artículo 45° de la Ley Universitaria N° 30220, estipula que "la obtención de los grados y títulos se realiza de acuerdo a las exigencias académicas que cada universidad establezca en sus respectivas normas internas"; asimismo lo establecido en los numerales 45.1; 45.2; 45.4 y 45.5 con relación a los requisitos mínimos para la obtención del Grado de Bachiller y Título Profesional.

2.- Que, la Resolución Rectoral N° 0089-2019/UCV, dispone que los estudiantes que ingresaron a la Universidad Cesar Vallejo desde el semestre académico 2014-II, deberán presentar un "TRABAJO DE INVESTIGACIÓN" para optar el Grado Académico de Bachiller. Además, para optar el Título Profesional, deberán presentar una "TESIS".

3. Que, en mutuo acuerdo asumimos las consecuencias legales de lo que significa hacer el trabajo de investigación, el proyecto de investigación y la tesis.

En señal de conformidad con lo establecido damos fe de nuestro compromiso.

Poma Ramos Alexander	73951658	
Apellidos y Nombres	DNI	Firma

Ate, 25 de Setiembre del 2019

Anexo 7: Carta de autorización de la empresa

Soltesi
SOLUCIONES TECNOLÓGICAS SISTÉMICAS S.A.C

Jesús María, 05 de Noviembre de 2019

AUTORIZACIÓN DEL PERMISO

Empresa	: Soluciones Tecnológicas Sistémicas S.A.C.
Tipo	: Permiso Practicante
Sección	: Desarrollo de Software
Jefe	: Héctor Jara Paucar

Presente:

Por medio de la presente carta N° 066-2019/EP-ING.SIS.UCV-ATE, la empresa Soluciones Tecnológicas Sistémicas S.A.C:

Por medio de este conducto la empresa, acepta su solicitud, para facilitarle el permiso al área de desarrollo de software, por intermedio de nuestro jefe de manera para que logre recabarla la información necesaria para su investigación a alumno de la Universidad Cesar Vallejo.

Por lo anteriormente expuesto se autoriza, el ingreso al estudiante Alexander Poma Ramos identificado con DNI 73951658 de la Universidad Cesar Vallejo.

Gracias por su comprensión

Héctor Jara Paucar
Soluciones Tecnológicas Sistémicas S.A.C.

Anexo 8: Cronograma de los proyectos

Cronograma proyecto Tesis

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
SGSI con ISO 27001 aplicado a la empresa SOLTESI S.A.C. del distrito de Jesús María 2021	**412.8 días**	**lun 15/07/19**	lun 5/07/21	
1. Selección de titulo de la investigacíon	6 días	lun 15/07/19	mié 24/07/19	
2. Desarrollo del Capitulo I	**29 días**	**mié 24/07/19**	**jue 12/09/19**	**2**
2.1 Introducción	6 días	mié 24/07/19	vie 2/08/19	
2.2 Realidad problematica	4 días	lun 5/08/19	vie 9/08/19	4
2.3 Trabajos previos	7 días	lun 12/08/19	jue 22/08/19	5
2.4 Formulacion de los problema	4 días	jue 22/08/19	jue 29/08/19	6
2.5 Formulacion de los objetivos	4 días	jue 29/08/19	jue 5/09/19	7
2.6 Formulacion de las hipotesis	4 días	jue 5/09/19	jue 12/09/19	8
3. Desarrollo de Capitulo III. Metología	**48 días**	**vie 13/09/19**	jue 5/12/19	**9;3**
3.1 Tipó y diseño de investigación	3 días	vie 13/09/19	mié 18/09/19	
3.2. Variables y Operacionalización	3 días	mié 18/09/19	mar 24/09/19	11
3.3 Población, Muestra y Muestreo	4 días	mar 24/09/19	mar 1/10/19	12
3.4. Técnicas e instrumentos de recolección de datos	5 días	mar 1/10/19	mié 9/10/19	13
3.5. Procedimientos	5 días	mié 9/10/19	jue 17/10/19	14
3.6. Métodos de Análisis de datos	5 días	vie 18/10/19	lun 28/10/19	15
3.7. Aspectos Éticos	3 días	lun 28/10/19	jue 31/10/19	16
3.8 Recursos y Presupuesto	10 días	vie 1/11/19	mar 19/11/19	17
3.9 Financiamiento	10 días	mar 19/11/19	jue 5/12/19	18
4. Resultados	15 días	vie 2/04/21	mié 28/04/21	
5. Discución	5 días	mié 28/04/21	jue 6/05/21	20
6. Concluciones	5 días	vie 7/05/21	lun 17/05/21	21

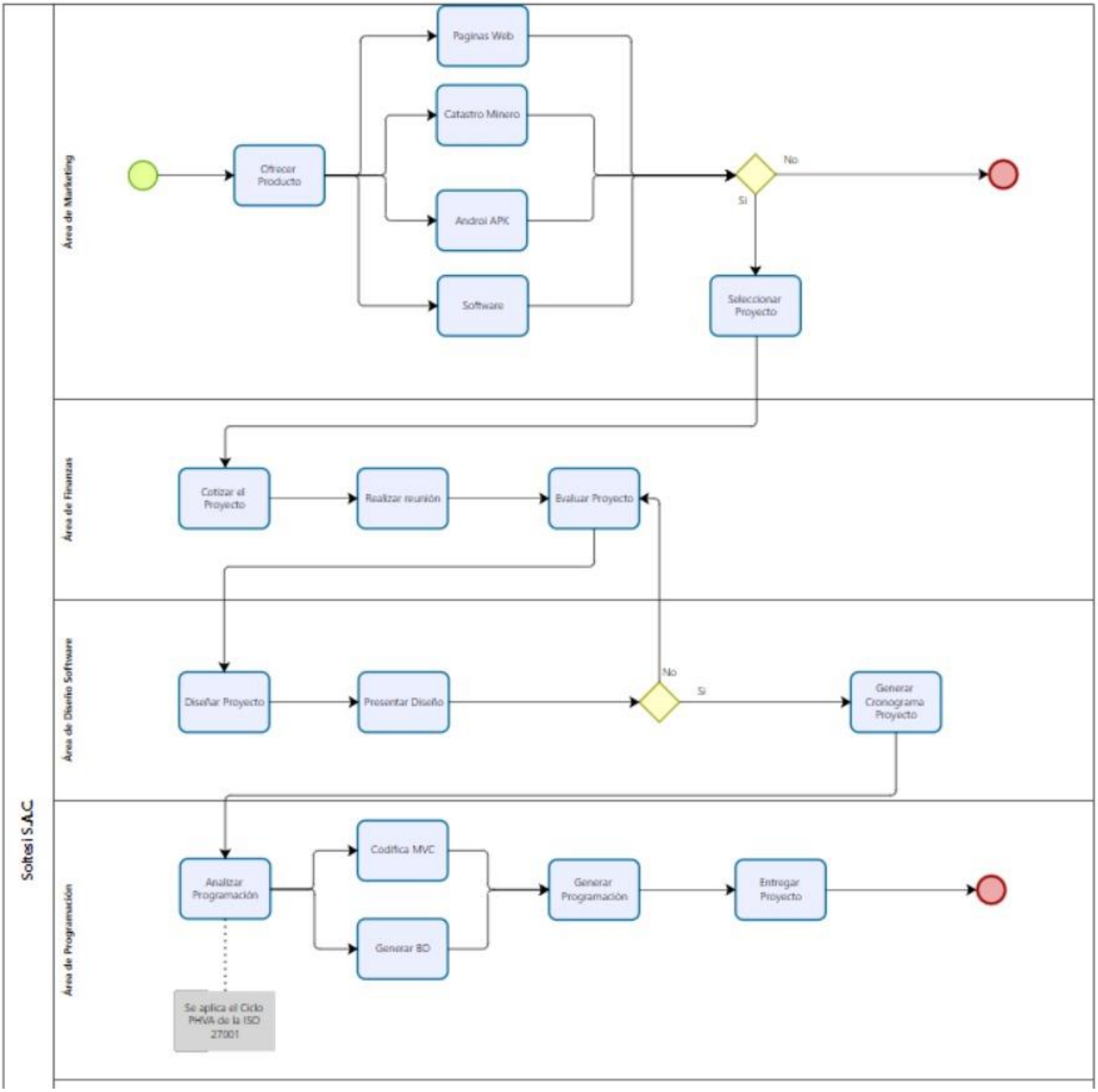
3.11 Cronograma Proyecto

Nombre de tarea	Duración	Comienzo	Fin
PROCESO DE AUDITORÍA DE SEGURIDAD INFORMATICA ISO 27001 PARA LA EMPRESA "SOLTESI S.A.C.	**114.8 días**	**mar 10/11/20**	**vie 28/05/21**
1. Capitulo 1	**12 días**	**mar 10/11/20**	**lun 30/11/20**
1.1 Descripción de la empresa Soltesi S.A.C.	5 días		
1.2 Equipamiento	**12 días**	**mar 10/11/20**	**lun 30/11/20**
1.2.1 Características de los servidores	10 días	mar 10/11/20	jue 26/11/20
1.2.2 Características de las PC	2 días	jue 26/11/20	lun 30/11/20
2. Capitulo 2	**15 días**	**jue 7/01/21**	**mar 2/02/21**
2.1 Norma ISO 27001	15 días	mar 10/11/20	vie 4/12/20
2.2 Piratas informáticos	**2 días**	**mar 10/11/20**	**jue 12/11/20**
2.3 Vulnerabilidad	1 día	jue 12/11/20	vie 13/11/20
2.4 Seguridad informática	2 días	vie 13/11/20	mié 18/11/20
2.5 Integridad de la información	1 día	mié 18/11/20	jue 19/11/20
2.6 Soporte de almacenamiento	1 día	jue 19/11/20	vie 20/11/20
2.7 Acceso a la información	1 día	vie 20/11/20	lun 23/11/20
2.8 Restauración de datos	1 día	mar 24/11/20	mié 25/11/20
2.9 Servidor	1 día	mié 25/11/20	jue 26/11/20
2.10 Virus informático	2 días	jue 26/11/20	lun 30/11/20
2.11 Copias de seguridad	1 día	mar 1/12/20	mié 2/12/20
3. Capitulo 3	**51.6 días**	**mar 2/02/21**	**lun 3/05/21**
3.1 Consideraciones	**6 días**	**vie 13/11/20**	**mié 25/11/20**
3.2 Medidas, controles, procedimientos, normas y estándares de seguridad.	3 días	mié 11/11/20	sáb 14/11/20
3.3. Contraseñas	**2 días**	**mar 10/11/20**	**jue 12/11/20**
3.4 Privilegios del Personal	**2 días**	**mar 10/11/20**	**jue 12/11/20**
3.5 Cifrado de información	**1 día**	**jue 12/11/20**	**vie 13/11/20**
4. Capitulo 4	**10 días**	**lun 3/05/21**	**mié 19/05/21**
4.1 Soporte y Actualizaciones Soltesi S.A.C.	**10 días**	**mar 10/11/20**	**jue 26/11/20**
4.2 Registro y actualización de entrada y salida de información	2 días	mar 10/11/20	jue 12/11/20
4.3 Copias de seguridad y recuperación de datos	2 días	jue 12/11/20	lun 16/11/20
4.4 Lugar de almacenamiento de copias de seguridad en la empresa Soltesi S.A.C	2 días	mar 17/11/20	jue 19/11/20

Nombre de tarea	Duración	Comienzo	Fin
4. Capitulo 4	**10 días**	**lun 3/05/21**	**mié 19/05/21**
4.1 Soporte y Actualizaciones Soltesi S.A.C.	**10 días**	**mar 10/11/20**	**jue 26/11/20**
4.2 Registro y actualización de entrada y salida de información	2 días	mar 10/11/20	jue 12/11/20
4.3 Copias de seguridad y recuperación de datos	2 días	jue 12/11/20	lun 16/11/20
4.4 Lugar de almacenamiento de copias de seguridad en la empresa Soltesi S.A.C	2 días	mar 17/11/20	jue 19/11/20
4.7 Cuentas de usuario	**3 días**	**mar 10/11/20**	**vie 13/11/20**
5. Capitulo 5	**6 días**	**mié 19/05/21**	**vie 28/05/21**
5.1 Uso de recursos informáticos	**1 día**	**mié 19/05/21**	**jue 20/05/21**
5.3 Manipulación de datos personales	**3 días**	**mié 19/05/21**	**lun 24/05/21**
5.4 Accesos de personal a soportes de datos e información	**3 días**	**jue 20/05/21**	**mar 25/05/21**
5.5 Confidencialidad con todo el personal	**2 días**	**mié 26/05/21**	**vie 28/05/21**
6. Capitulo 6	**25 días**	**mar 10/11/20**	**mié 23/12/20**
6.2 Almacenamiento de la información	**3 días**	**mar 10/11/20**	**vie 13/11/20**
6.3 Accesos de personal a cuarto de servidores	**2 días**	**vie 13/11/20**	**mié 18/11/20**
6.4 Estructura física del ambiente informático	**14 días**	**mié 18/11/20**	**vie 11/12/20**
6.5 Factores ambientales del entorno informático	2 días	vie 18/12/20	mié 23/12/20
6.6 Medidas de protección del ambiente informático	**1 día**	**mar 10/11/20**	**mié 11/11/20**
6.7 Protección a riesgos identificados	**1 día**	**mié 11/11/20**	**jue 12/11/20**
7. Capitulo 7	**16 días**	**mar 10/11/20**	**lun 7/12/20**
7.1 Personal autorizado a conceder, alterar o anular accesos sobre datos y recursos	1 día	mar 10/11/20	mié 11/11/20
7.2 Número máximo de intentos de conexión	1 día	mié 11/11/20	jue 12/11/20
7.3 Descarga de información	1 día	jue 12/11/20	vie 13/11/20
7.4 Conexiones entre empresas y redes públicas o privadas	2 días	vie 13/11/20	mié 18/11/20
7.5 Responsabilidad del personal ante contraseñas y equipos	2 días	mié 18/11/20	vie 20/11/20
7.6 Seguridad ante el trabajo remoto	3 días	vie 20/11/20	jue 26/11/20
7.7 Seguridad ante el trabajo remoto en la empresa Soltesi S.A.C.	2 días	jue 26/11/20	lun 30/11/20
7.8 Técnicas de identificación y autenticación	1 día	mar 1/12/20	mié 2/12/20

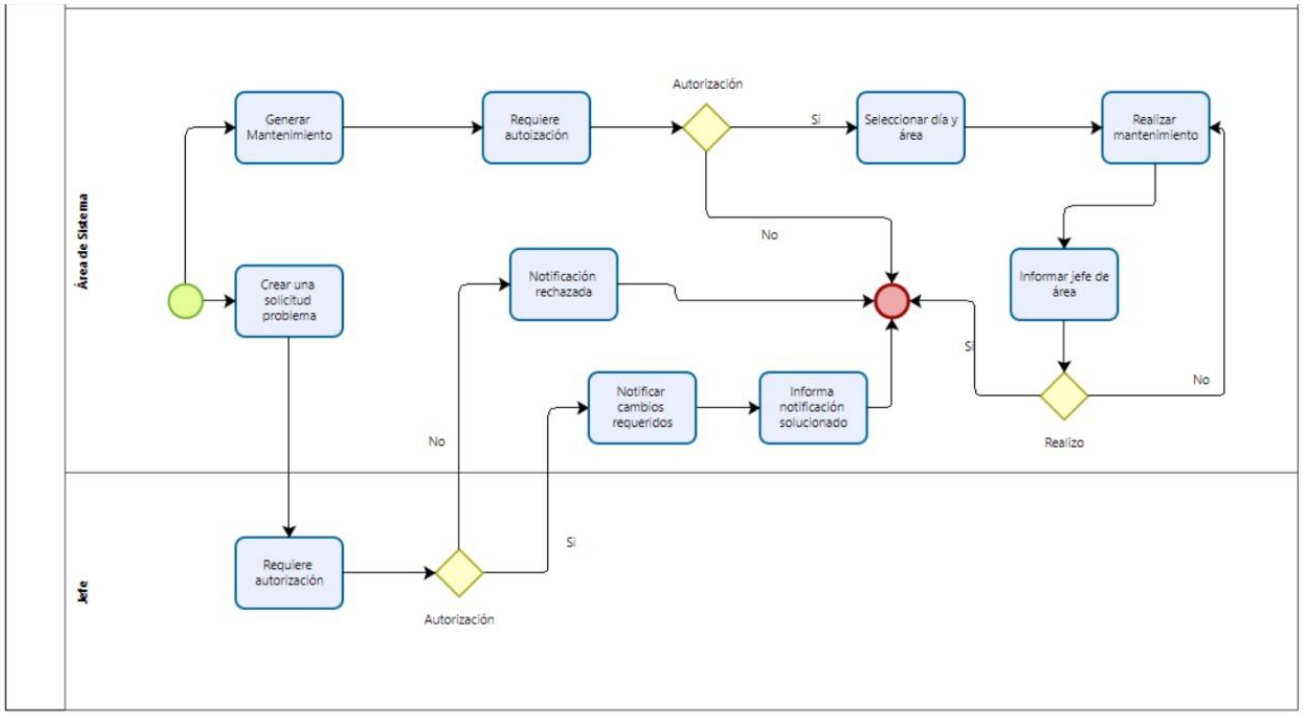
Anexo 9: Estructura de la empresa Soltesi S.A.C. Antes y después

Antes



Fuente Empres Soltesi S.A.C.

Después



Fuente elaboración propia

Anexo 10: Pre test Porcentaje de incidencias

Acta de la validación de Matriz de medición de incidencias

Este documento tiene como objetivo validar la matriz de incidencias lo cual va a permitir determinar el impacto de las incidencias en seguridad de la información en la empresa Soltesi S.A.C. del distrito de Jesús María.

MATRIZ DE INCIDENCIA			IMPACTO		
			BAJA	MEDIA	ALTA
			1	2	3
URGENCIA	ALTA	3	3	6	9
	MEDIA	2	2	4	6
	BAJA	1	1	2	3

TITULO	“SGSI para la seguridad de la información en la empresa Soltesi S.A.C. del distrito de Jesús María”	
OBJETIVOS	O.E.1: Determinar la influencia de la confidencialidad del SGSI en la seguridad de la información en la empresa Soltesi S.A.C. del distrito de Jesús María. O.E.2: Determinar la influencia de la integridad del SGSI de la seguridad en la información en la empresa Soltesi S.A.C. del distrito de Jesús Marí. O.E.3: Determinar la influencia de la disponibilidad del SGSI de la seguridad en la información en la empresa Soltesi S.A.C. del distrito de Jesús María.	
GESTIÓN DE INCIDENCIA	**PORCENTAJE DE INCIDENCIA**	**FORMULA**
Confidencialidad	$PIC = \frac{N°IC}{TI}$	**PIC=** Porcentaje de incidencia de confidencialidad **N°IC=** Numero de incidencia de confidencialidad **TI=** Total de incidencia

Integridad	$PII = \frac{N°II}{TI}$	**PIC=** Porcentaje de incidencia de integridad **N°II=** Numero de incidencia de integridad **TI=** Total de incidencia
Disponibilidad	$PID = \frac{N°ID}{TI}$	**PIC=** Porcentaje de incidencia de disponibilidad **N°ID=** Numero de incidencia de disponibilidad **TI=** Total de incidencia

Desarrollo del marco de trabajo SCRUM (Metodología Agiles)

RESUMEN

El mercado actual es altamente competitivo y cambiante la metodología ágil. En ese contexto el desarrollo del software busca básicamente rapidez, calidad y reducción de costos en la ejecución de sus proyectos; para asumir estos retos es necesario tener agilidad y flexibilidad. Estas características se constituyen en el fundamento mismo de las metodologías agiles de desarrollo.

En el ámbito de las metodologías de desarrollo de software existe un gran número de alternativas y los responsables de cada proyecto tienen la difícil tarea de seleccionar la alternativa que mejor se ajuste a sus necesidades y recursos.

El presente estudio se enfocó en el análisis del método ágil SCRUM para la implementación de una metodología aplicada al desarrollo de software realizada por la empresa Soltesi S.A.C.

La ejecución y culminación del proyecto permitió establecer una metodología basada en Scrum, complementada con otros métodos. El resultado es un producto de software funcional, en cuyo desarrollo se pudo demostrar la validez de Scrum aplicado a proyectos de software de mediano tamaño, en entornos cambiantes, con grupos de trabajo pequeños que involucran permanentemente al dueño del producto.

INTORUDCCIÓN

Hoy en día los avances tecnológicos vienen dominando al mundo mercantil, ya que cualquier actividad o cualquier registro anteriormente se realizaba a mano y con el pasar de los años la tecnología mediante el software viene ayudando mucho en poder realizar las actividades rápidamente, tanto así que facilita al usuario en poder realizar sus actividades en un menor tiempo.

Así mismo las páginas web que vienen siendo publicidad, son muy valiosa en donde cualquier persona natural viene a ingresar para poder informarse sobre que realiza la empresa o persona dueño de la página, tanto así que atrae clientes de distintas partes del mundo, otro punto importante de la tecnología viene a ser los softwares que flexibilizan el trabajo a las empresas donde se agilizan los procesos de trabajo, de modo que va genera mayores ingresos a la empresa con menores costos en menor tiempo posible.

La implementación y utilización del sistema desarrollado ha permitido optimizar el proceso, disminuir considerablemente los recursos utilizados y brindar un mejor servicio a sus clientes.

Para el desarrollo de la aplicación descrita, se planteó el estudio y utilización del Método Ágil Scrum, aplicado al desarrollo de software, lo cual constituye un aporte significativo en el estudio y utilización de metodologías ágiles de desarrollo como alternativa a las metodologías tradicionales.

La ejecución del proyecto permitió además evidenciar las fortalezas y debilidades de la utilización de Scrum en proyectos de desarrollo de software.

METODOLOGÍA

Es necesario aclarar que SCRUM, más que una metodología de desarrollo de software, es un método de gestión de proyectos, el cual puede adaptarse a cualquier tipo de proyecto y no únicamente a los de desarrollo de software. Aplicada al desarrollo de software, está basado en el modelo de las metodologías ágiles, incrementales, basadas en iteraciones y revisiones continuas. El objetivo principal es elevar al máximo la productividad del equipo de desarrollo. Reduce al máximo las actividades no orientadas a producir software funcional y produce resultados en periodos cortos de tiempo.

Como método, enfatiza valores y prácticas de gestión, sin pronunciarse sobre requerimientos, prácticas de desarrollo, implementación y demás cuestiones técnicas. Más bien delega completamente al equipo la responsabilidad de decidir la mejor manera de trabajar para ser lo más productivos posibles. Es esta característica hizo que, durante la ejecución del proyecto se complementara la filosofía del método Scrum con herramientas, métodos y procedimientos utilizados en otras metodologías, tanto ágiles como tradicionales.

1.1 Desarrollo iterativo e incremental

Scrum está basado en el modelo iterativo e incremental de las metodologías ágiles de desarrollo.

Para el proyecto, en un Sprint 0 se planificó, cuatro iteraciones de Sprints, cada una con una duración de cuatros semanas. Cada Sprint (1 - 2) buscaba incrementar funcionalidades agrupadas en módulos de la aplicación. La planificación inicial permitió definir el Backlog del producto, el cual se constituyó en la base lo los Backlogs de cada Sprint.

La finalización de cada Sprint dio como resultado una versión estable del producto, con el incremento de las funcionalidades planificadas, las mismas que eran presentadas al Product Owner. Para ello, es recomendable que cada requisito

planificado se complete en una única iteración incluyendo pruebas y documentaciones.

La Figura 1 detalla los objetivos planteados en cada Sprint desarrollado durante la ejecución del proyecto I.P.S.S.

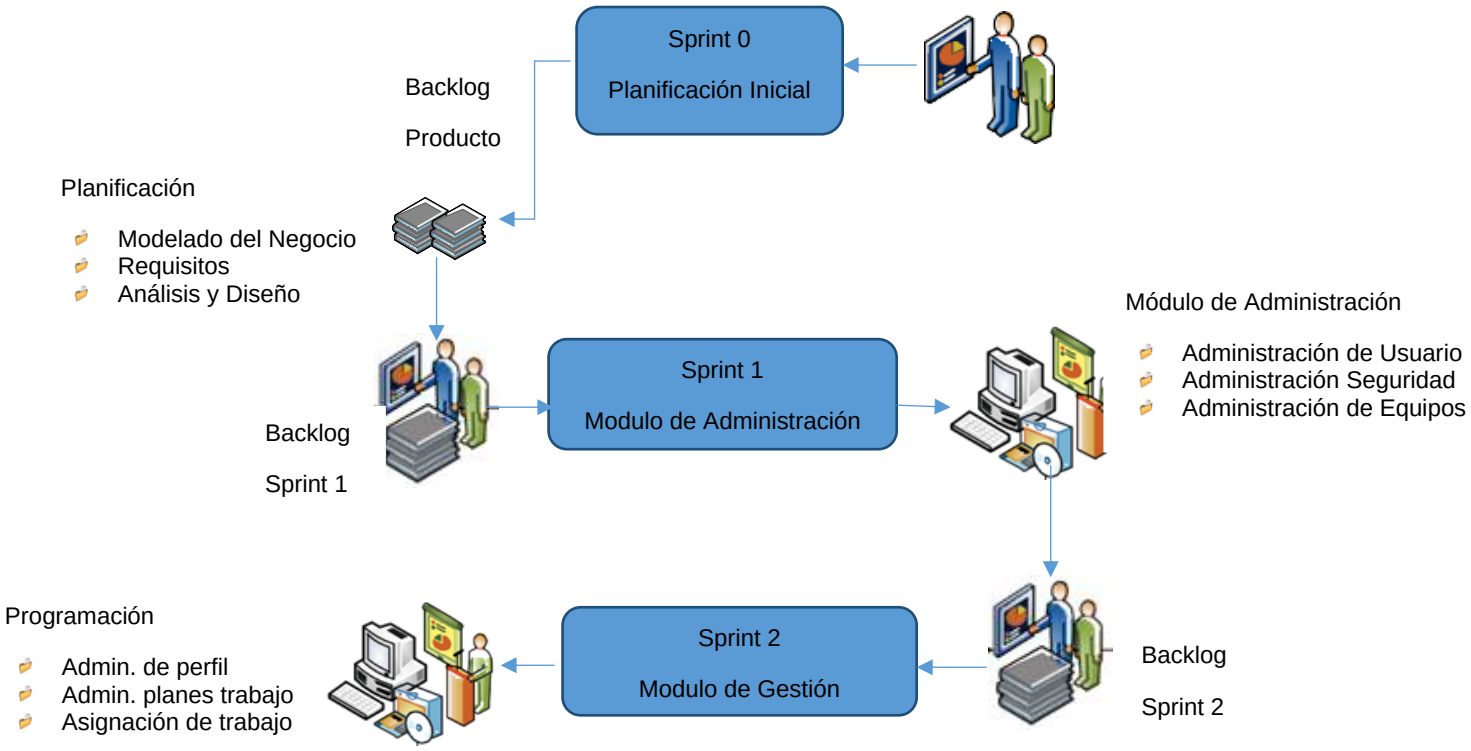


Figura 11 Sprints del proyecto de I.P.S.S

1.2 Fases

Cada iteración o Sprint del proyecto puede entenderse como un pequeño proyecto individual; en cada iteración se repite un proceso de trabajo similar (iterativo) para proporcionar un resultado completo sobre el producto final, así el Product Owner obtiene los beneficios del proyecto de forma incremental.
La ejecución de cada Sprint del proyecto puede dividirse en 5 fases, similares al ciclo de vida del modelo en cascada, como se muestra en la Figura 2.

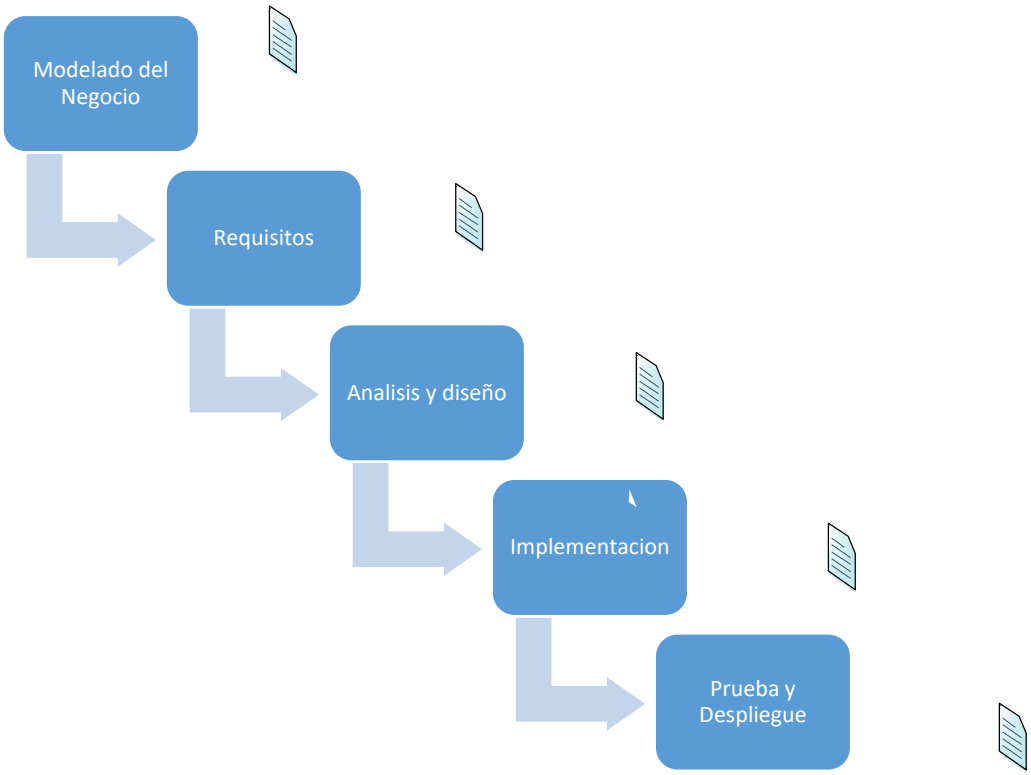


Figura 12 Fases de un Sprint del proyecto de I.P.S.S.

1.2.1 Modelado del negocio

El modelado del negocio tiene como objetivo el comprender y describir de forma simplificada la realidad del negocio.

Esta fase se la llevo a cabo principalmente durante el Sprint 0, el cual tenía como objetivo analizar el negocio, los requerimientos, plantear una arquitectura base y planificar en forma macro el trabajo a realizar en los Sprints 1 y 2.

Durante el desarrollo de los Sprints planificados, se realizaron afinamientos específicos a los objetivos de cada Sprint.

1.2.2 Requisitos

Esta fase tiene como propósito especificar las funcionalidades que serán implementadas durante el Sprint.

En el Sprint 0 se especificaron las funcionalidades de toda la aplicación, mientras que en cada Sprint se analizó de forma detallas los requerimientos específicos, según los objetivos planteados.

1.2.3 Análisis y diseño

El análisis intenta descubrir qué es lo que realmente se necesita, para llegar a una comprensión adecuada de los requerimientos ¿Qué hacer? El diseño representa las características que permitirán la implementación de los requerimientos en forma efectiva ¿Cómo hacerlo?

Respecto del diseño, en el Sprint 0 se planteó una arquitectura candidata, la misma que fue ratificada o modificada, según el análisis de los requerimientos a implementar en cada Sprint.

1.2.4 Implementación

En esta etapa, el equipo de desarrollo implementa las funcionalidades necesarias, de acuerdo a las especificaciones analizadas y según el diseño planteado.

Esta etapa fue pasada por alto en el Sprint 0, pues el objetivo de este Sprint, fue el de analizar y planificar el proyecto como tal. En los Sprints 1 y 2 el resultado de esta etapa fue el incremento de funcionalidades en una versión estable utilizable para el sistema.

1.2.5 Pruebas / Despliegue

La etapa de pruebas tiene como objetivo garantizar el correcto funcionamiento de las funcionalidades implementadas.

Durante la ejecución del proyecto, la etapa de pruebas se la llevo a cabo tanto por los responsables de la implementación como de los usuarios del producto que formaban parte del Team del proyecto.

Para que el usuario pueda realizar las pruebas, fue necesario realizar un despliegue o implantación de la aplicación en un entorno de testing, esto se llevó a cabo con cada incremento de la aplicación.

2. DISEÑO E IMPLEMENTACIÓN

Como resultado del análisis y planificación realizados en el Sprint0, se planificó el desarrollo de la aplicación en 2 Sprints, cada sprint con el objetivo de implementa un módulo independiente.

- Sprint 1: Módulo de Administración
- Sprint 2: Módulo Gestión

Las funcionalidades a implementar en cada Sprint fueron descritas utilizando historias de usuario priorizadas según la importancia que estas tenían para el Product Owner. Posteriormente se analizaron las historias de usuario utilizando casos de uso y sus respectivas especificaciones.

En base al análisis realizado en el Sprint0 se planteó un modelo Cliente – Servidor basado en un desarrollo de N capas (Figura 3), arquitectura predominante para la construcción de software.

2.1 Aplicación de Escritorio

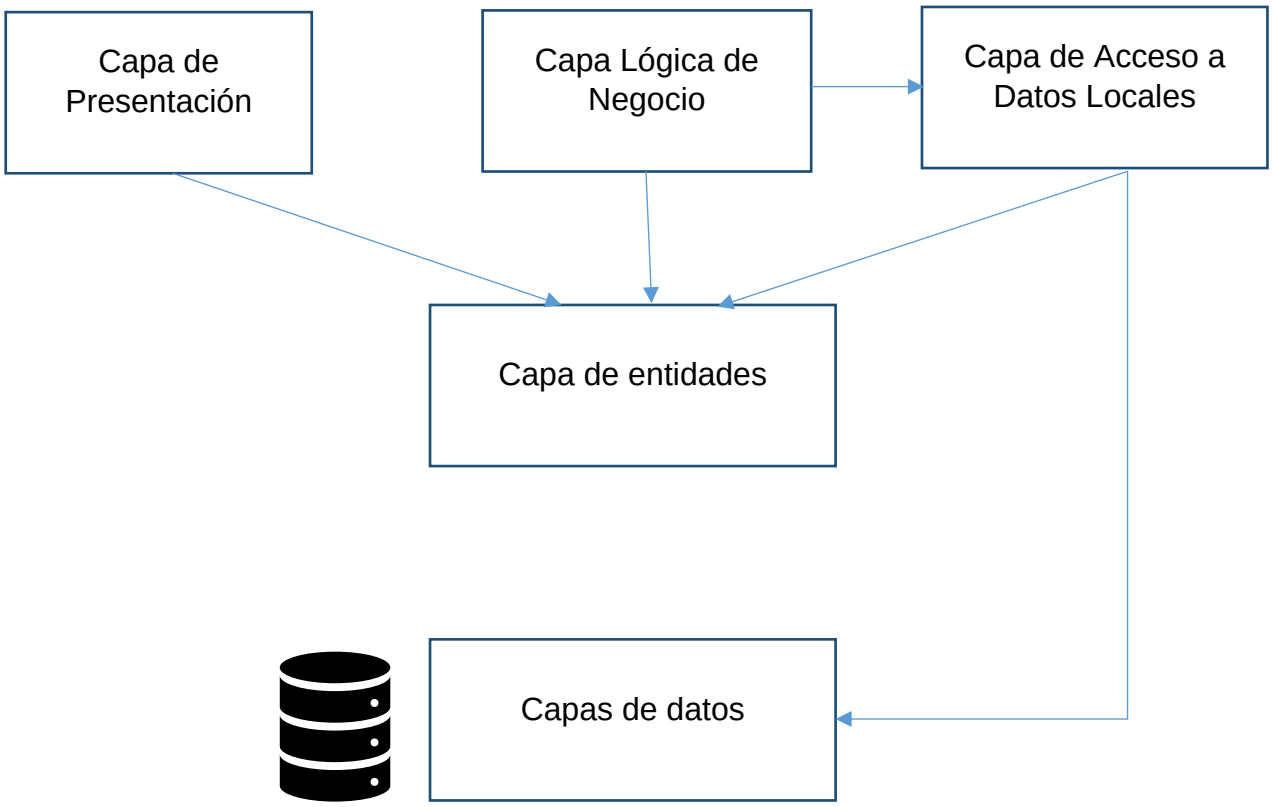


Figura 13 Diagrama lógico del sistema I.P.S.S

3 ROLES Y RESPONSABILIDADES

3.1 ROLES

Los roles son asignados para uno o varias personas, para esto es muy importante la responsabilidad y las habilidades de cada personal que labore en la empresa para la ejecución de sus tareas asignadas.

Así mismo se realizó un análisis exhaustivo de los trabajadores de la empresa, para pertenecer a los roles propuestos por scrum, los roles asignados son 4.

Tabla 13 Roles

Scrum	Seguridad de la información
Stackholder	AIDESEP, Ministerio de Agricultura y Mina, Municipalidad de Ate
Product Owner	Representante del cliente
Scrum Master	Jefe de la empresa (Héctor Milton Jara Paucar)
Development team	Área de Programación (Efraín Espinoza y Jorge Flores)

3.2 Responsabilidades

Product Owner

- Realiza la toma de decisiones para la realización del producto.
- Es la persona responsable de registrar en el Product Backlog todas las épicas e historias de usuarios que definen el sistema durante la ejecución del proyecto.
- Decidir qué historias y en que prioridad se van a desarrollar que ayuden al incremento del producto final.
- Llevar la comunicación a todos los miembros del equipo scrum de lo que se está realizando al igual que a los clientes.
- Las responsabilidades que están asociadas a su rol semejante (ver Tabla 1) seguridad de la información también hacen parte de sus responsabilidades.
- Por ser un funcionario público también le aplican todas las normas en las cuales se definen sus responsabilidades

Scrum Master

- Responsable de que todos los miembros del Equipo Scrum entiendan y adopten los valores, principios y prácticas de la metodología Scrum.
- Liberar al equipo Scrum de los impedimentos que se le puedan presentar y disminuir su productividad y de toda interferencia externa.
- Supervisar el Product Backlog, aclarar las dudas con el Product Owner y

brindar sugerencias que permitan subsanar las inconsistencias que encuentre.

- Supervisar los Gráficos de producto (Burn Up) y de avance (Burn Down).
- Por ser un funcionario público también le aplican todas las normas en las cuales se definen sus responsabilidades disciplinarias, penales, fiscales, patrimoniales y política.

Development Team

- Debe comprender y tener conocimiento del Product Backlog, si se observan inconsistencias o dudas estas deben ser solucionadas o aclaradas con el Product Owner o el Scrum Master
- Auto organizarse para que pueda ejecutar de la mejor manera los requerimientos ingresados en el Product Backlog.
- Por ser un funcionario público también le aplican todas las normas en las cuales se definen sus responsabilidades disciplinarias, penales, fiscales, patrimoniales y política.
- Seleccionar los requerimientos a desarrollar en la iteración para crear el Sprint Backlog. Estos se seleccionan en base a su prioridad.
- Las responsabilidades que están asociadas a su rol semejante (ver Tabla 1) Seguridad de la información también hacen parte de sus responsabilidades.

4. ENTREGABLES DEL PROYECTO

A continuación, se indican y describen cada uno de los artefactos que se generaron durante la ejecución de proyecto y que constituyen los entregables del mismo. Como se había mencionado previamente, SCRUM no es una metodología de Desarrollo de software, de forma que no existe una especificación de artefactos a utilizar, aunque se utilizó modelos y procesos utilizados en otras metodologías como RUP y XP.

Es preciso destacar que de acuerdo a la filosofía de RUP y de casi todos los procesos iterativos e incrementales, todos los artefactos son objeto de modificaciones a lo largo del proceso de desarrollo, y sólo al término del proceso podríamos tener una versión definitiva y completa de cada uno de ellos. Sin embargo, cada iteración estaba orientada a conseguir un cierto grado de completitud y estabilidad de los artefactos.

4.1 Especificación del historial

De acuerdo a los modelos se realizó la identificación del historial para cada Sprint, se realizó una descripción detallad, utilizando una plantilla de documento donde se incluyen: nombre de la historia, numero, prioridad del historial, riesgo de desarrollo, , como se muestra en la Figura 4.

4.1.1 Sprint 0

Tabla 14 Historia ingresar al sistema como usuario

HU001 – Ingresar Sistema		
Numero	1	
Prioridad: Media		Riesgo en desarrollo: Baja
Como	Usuario	
Quiero	Verificar que el sistema me ingrese correctamente al sistema.	
Para	Visualizar el menú del sistema	
Condiciones	• El usuario debe digitar el usuario y contraseña • El sistema te debe mostrar la ventana de ingreso correctamente	
Observación: Solo el administrador puede verificar el detalle del ingreso del personal		

Tabla 15 Validar usuario

HU002 – Validar Usuario	
Numero	2
Prioridad: Alta	Riesgo en desarrollo: Media
Como	Usuario
Quiero	Ingresar al sistema correctamente
Para	Verificar que el usuario ingresado es el correcto
Condiciones	• El sistema debe mostrar la confirmación del sistema de ingreso del usuario • El sistema debe validad sus datos de usuario al momento de ingresar en la parte inferior derecha de la ventana
Observación: Solo el usuario puede verificar su validación de datos de ingreso.	

Tabla 16 Visualizar sistema como usuario

HU003 – Visualizar el Sistema	
Numero	3
Prioridad: Media	Riesgo en desarrollo: Baja
Como	Usuario
Quiero	Visualizar el sistema, que se muestre los campos de trabajo
Para	Realizar los trabajos respectivos
Condiciones	• El usuario debe visualizar el menú completo del sistema • El sistema debe visualizar los botones asignados por el administrador al usuario
Observación: Solo el usuario puede visualizar su ventana de sistema.	

4.1.2 Sprint 1

Tabla 17 Ingresar sistema como administrador

HU001 – Ingresar sistema	
Numero	4
Prioridad: Media	Riesgo en desarrollo: Baja
Como	Administrador
Quiero	Ingresar al sistema correctamente
Para	Visualizar que el sistema ingrese correctamente
Condiciones	• El administrador debe ingresar el usuario y contraseña como administrador • El sistema muestra la ventana del modo administrador
Observación: Solo el administrador visualiza la administración de perfiles a los usuarios.	

Tabla 18 Administrar usuario como administrador

HU002– Administrar Usuario	
Numero	5
Prioridad: Alta	Riesgo en desarrollo: Alta
Como	Administrador
Quiero	Administrar los campos que solo se puede visualizar como usuario
Para	Realizar una administración correctamente a los usuarios nuevos
Condiciones	• El sistema muestra solo los campos a habilitar para cada usuario • El administrador Selecciona los campos a habilitar para cada usuario
Observación: Solo el administrador puede administrar los perfiles de cada usuario registrado en el sistema.	

Tabla 19 Administrar seguridad como administrador

HU003 – Administrar Seguridad Usuario		
Numero	6	
Prioridad: Alta		Riesgo en desarrollo: Alta
Como	Administrador	
Quiero	Administrar los accesos que solo puede acceder el usuario con los permisos generados por el administrador	
Para	Gestionar la seguridad de la empresa y el sistema	
Condiciones	• El sistema muestra los campos de privilegios de seguridad para habilitar accesos al usuario • El administrador selecciona e habilita los campos donde el usuario pueda acceder libremente • El administrador debe recibir alguna notificación de accesos denegados al usuario	
Observación: Solo el administrador puede generar accesos a los usuarios para ingresar a diversas plataformas del sistema.		

4.1.3 Sprint 2

Tabla 20 Análisis del sistema

HU001 – Análisis del Sistema		
Numero	7	
Prioridad: Alta		Riesgo en desarrollo: Media
Como	Administrador	
Quiero	Realizar el análisis completo del sistema	
Para	Realizar el diseño el programa	
Condiciones	• El sistema se debe analizar antes de diseñarse por mockups • Se debe realizar análisis las políticas de seguridad para cada proyecto	
Observación: El administrador y usuarios pueden analizar el sistema si es que falta algún componente para finalizar el proyecto.		

Tabla 21 Diseño del sistema

HU002 – Diseñar el Sistema	
Numero	8
Prioridad: Media	Riesgo en desarrollo: Baja
Como	Administrador
Quiero	Diseñar el sisma completo, de acuerdo al requerimiento del cliente
Para	Realizar la programación diseñada correcta del proyecto
Condiciones	• El usuario debe realizar el diseño del proyecto • El usuario debe realizar el rango de horas para realizar la actividad • El usuario debe realizar el rango de días para realizar la actividad • El administrador debe verificar las actividades realizadas por el usuario
Observación: Solo el usuario esta encarado de diseñar el sistema planteado con el jefe de área.	

Tabla 22 Programación de software

HU003 – Programar software	
Numero	9
Prioridad: Alta	Riesgo en desarrollo: Alta
Como	Administrador
Quiero	Realizar la programación del diseño del sistema
Para	Entregar el proyecto planteado por el cliente
Condiciones	• El usuario debe programar los mockups diseñados • El usuario debe implementar políticas de seguridad a la programación • El usuario programa utilizando el MVC
Observación: El usuario este encargado de observar el diseño de software y ponerse a programar el software planteado el jefe de área.	

Tabla 23 Testear de Software

HU004 – Testear Software		
Numero	10	
Prioridad: Alta		Riesgo en desarrollo: Baja
Como	Administrador	
Quiero	Probar que el sistema funcione correctamente	
Para	Presentar el proyecto terminado a los clientes	
Condiciones	• El usuario debe testear el proyecto finalizado • El usuario debe crear el manual de usuario del sistema • El usuario debe presentar las tablas de la base de datos • El usuario debe presentar las tablas de los casos de usos • El usuario debe presenta informe de fallos al sistema • El administrador debe presentar el sistema terminado	
Observación: El usuario y jefe de área este encargado de testear el proyecto finalizado antes de ser entregados al cliente.		

4.2 Modelo de datos

La información del sistema es soportada por una base de datos relacional, por tanto, este modelo describe la representación lógica de los datos. Para expresar este modelo se utiliza un diagrama que permita la representación de tablas, claves, etc. En cada Sprint se especificó el modelo correspondiente al módulo a implementar.

La Figura 4 muestra el modelo de datos del sistema para la implementación de políticas de seguridad para software, debido a la confidencialidad la empresa está prohibido mostrar la información de la empresa.

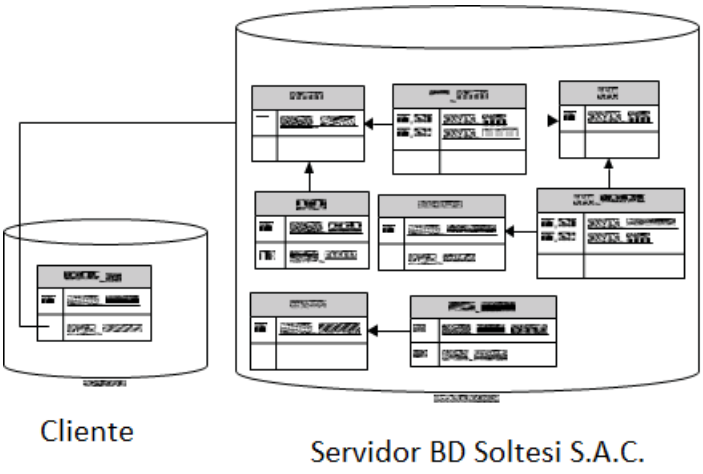


Figura 14 Modelo de datos Sistema I.P.S.S.

4.3 Modelo de Diseño

En cada Sprint se especificó mediante diagramas que permitan visualizar la interacción entre los diferentes componentes del sistema. La Figura 8 muestra como ejemplo, el diagrama de componentes para el módulo de administración, basada en la arquitectura de la aplicación de escritorio descrita previamente en la Figura 5 Diagrama Lógico Sistema I.P.S.S.

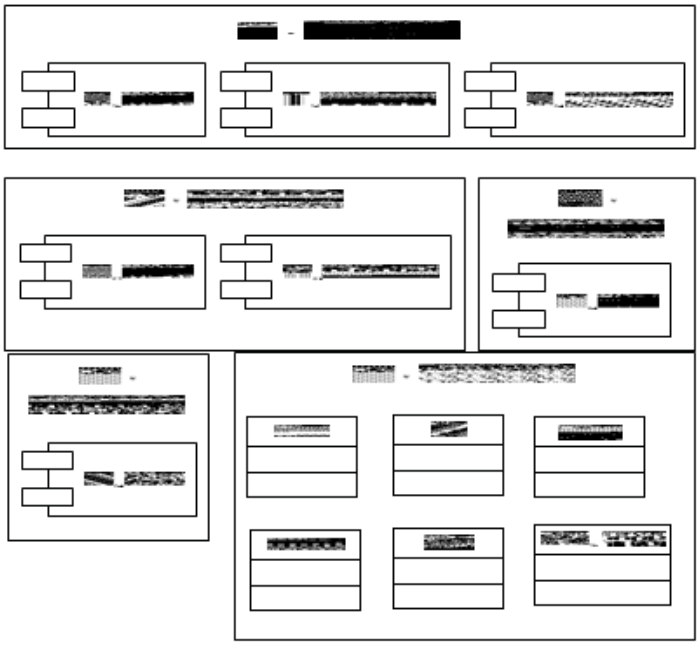


Figura 15 Diseño Componentes Modulo de Administración

4.4 Sprint Backlog

El Sprint Backlog o pila del Sprint, es la lista de tareas determinadas por el equipo para realizar durante el Sprint. A cada Tarea se le asigna un responsable miembro del Team y se estima el tiempo que le llevara completar la tarea.

Para administrar las tareas de cada Sprint y llevar un control de avance de la misma, se utilizó la herramienta “SprintToMeter”; la Figura 5 muestra una captura de pantalla de la herramienta.

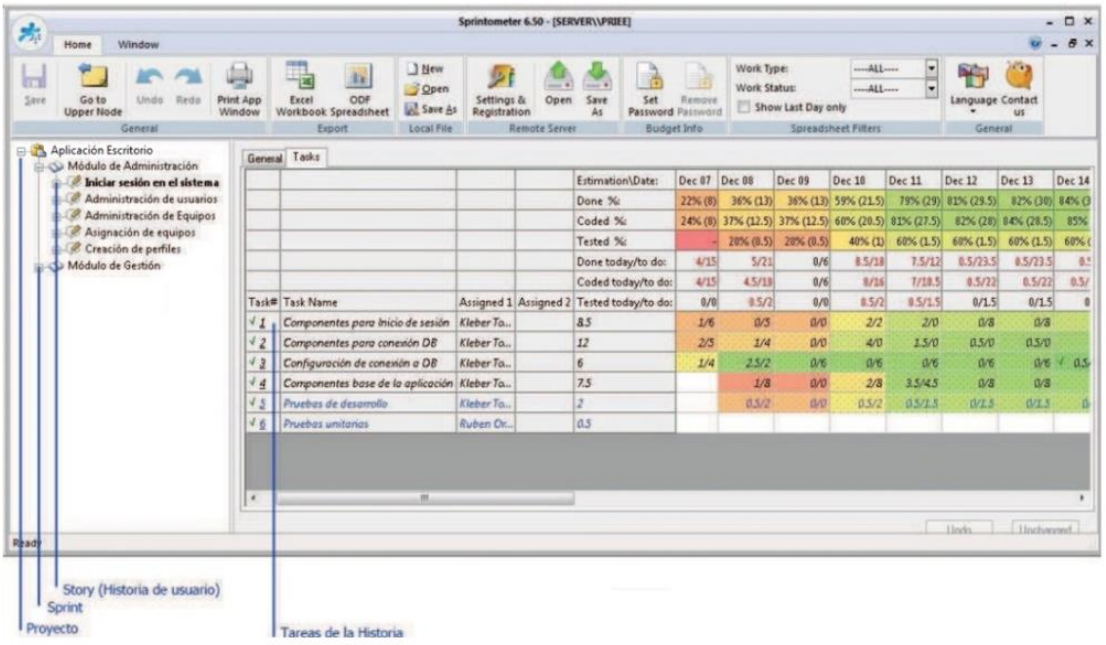


Figura 16 Printscreen - SprintToMeter

4.5 Checklist de Pruebas

Para llevar un control del correcto funcionamiento de los componentes y las funcionalidades implementadas, se registró en archivos de Excel los casos de prueba, valores de entrada, resultados esperados y resultados obtenidos.

La Figura 6 muestra un ejemplo parcial del checklist de pruebas utilizado en el Sprint1- Módulo de Administración.

Tabla 24 Pruebas de software Modulo de Administración

ID	PT001
Sprint	Módulo de Administración
Tipo de pruebas	Pruebas unitarias
Métodos utilizados	Caja Blanca / Caminos
Descripción	Se refiere a las pruebas que se realizaron sucesivamente como el acceso a la base de datos, el registro los usuarios, administración de usuario.
Objetivo	• Administrar la seguridad el sistema, así mismo velar por la seguridad de los datos tanto del cliente como de los usuarios. • Verificar el uso adecuado de los campos administrador por el administrador de cada usuario. • Moderar los accesos a ciertas carpetas compartidas. • Realizar mantenimiento correctivo a las PC
Responsable	Héctor Mirlon Jara Paucar y área de sistema

Método	Casos	Camino	Especifica DB	Genera LOG	Nombre SP	Parámetros	Tiene resultados	Resultado esperado	Resultado
cbrConexion	Ejecución SP (no existe SP)	1=>2=>3=>4=>5=>6=>7=>8=>15=>17	si	no	sp_com_consulta_usuarios	N/A	N/A	El sistema alerta del problema, no existe el SP. Se genera log de errores	ok
cbrConexion	Ejecución SP (no existe SP)	1=>2=>3=>4=>5=>6=>7=>8=>15=>17	no	no	sp_com_consulta_usuarios	N/A	N/A	Seteo de BD, logea error, no logea ejecución, alerta error	ok
cbrConexion	Ejecución SP (no existe SP)	1=>2=>3=>4=>5=>6=>7=>8=>15=>17	si	si	sp_com_consulta_usuarios	N/A	N/A	Genera log de ejecución, alerta del error, genera log de error	ok

Figura 17 Parcial Checklist de pruebas - Sprint 1

Tabla 25 Pruebas de software Modulo de Gestión

ID	PT002
Sprint	Módulo de Gestión
Tipo de pruebas	Pruebas unitarias
Métodos utilizados	Caja Blanca / Caminos
Descripción	Realizar la administración correcta a los perfiles y planes de trabajo de los usuarios, donde se debe visualizar el correcto uso de los componentes para realizar el proyecto al tiempo estimado.
Objetivo	• Administrar los perfiles de cada usuario, para realizar los trabajos respectivos. • Verificar que los usuarios realicen los trabajos respectivos, de acuerdo a su área establecida.
Responsable	Efraín Espinosa, Jorge Flores

4.6 Producto

Luego de realizar el registro correctivo del usuario, el administrador se encargará de administrar su perfil de trabajo, como también los accesos a ciertos puntos de trabajo para la empresa. El producto, a partir de la primera fase de Construcción del Sprint1 es desarrollado incremental e iterativamente, obteniéndose seguridad al momento de generar el proyecto solicitado por el usuario.

4.7 Manuales

Sobre la versión final del producto, se generó el respectivo manual de usuario e instalación que le permitirá al cliente la fácil instalación y utilización del proyecto contratado.

5. CONCLUSIONES

- Siendo SCRUM un método de gestión de proyectos en general, este está siendo utilizada con bastante éxito en el área del desarrollo de software. Los resultados obtenidos en la ejecución del presente proyecto, permiten evidenciar su validez, especialmente en proyectos pequeños y medianos, con entornos cambiantes, grupos de trabajo pequeños que involucran permanentemente al dueño del producto.

- Como metodología de desarrollo, SCRUM deja algunos vacíos, especialmente en lo referente a los artefactos o entregables a utilizar. Estos vacíos metodológicos fueron exitosamente complementados utilizando modelos de otras metodologías, especialmente R.U.P. y X.P.

- La comunicación constante entre todos los implicados del proyecto se constituyó en un pilar fundamental de la conclusión exitosa del mismo. Scrum indica que se deben realizar reuniones diarias con los miembros del equipo; si bien esto no fue posible realizar, se procuró mantener como mínimo una reunión semanal. Estas reuniones permitían evaluar continuamente los avances de las tareas planteadas para cada sprint, aclarar duras cuando estas se presentaban, replantear los tiempos asignados para el cumplimiento de tareas tanto de codificación como de pruebas y tomar los correctivos necesarios a tiempo.

UNIVERSIDAD CÉSAR VALLEJO

Declaratoria de Autenticidad del Asesor

Yo, Chávez Pinillos Frey Elmer, docente de la Facultad de Ingeniería y Arquitectura y Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo sede Ate, asesor de la Tesis titulada:

"SGSI CON ISO 27001 APLICADO A LA EMPRESA SOLTESI S.A.C. DEL DISTRITO DE JESÚS MARÍA 2021"

del (los) autor (autores) **POMA RAMOS ALEXANDER,** constato que la investigación tiene un índice de similitud de **19%** verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

Ate,23 de mayo del 2023

<table>
<tr><td colspan="2">Apellidos y Nombres del Asesor:
Chávez Pinillos Frey Elmer</td></tr>
<tr><td>DNI
40074326</td><td rowspan="2">Firma
  </td></tr>
<tr><td>ORCID
0000-0003-3785-5259</td></tr>
</table>

INVESTIGA UCV