FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa ZEPPELIN INVERSIONES GENERALES S.R.L

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTORES:

Cruz Ruiz Alexander Jesus (0000-0002-7134-0489)
Huamani Cahuana Luis Miguel (0000-0003-3985-9587)

ASESORA:

Mg. Acuña Meléndez María Eudelia (0000-0002-5188-3806)

LÍNEA DE INVESTIGACIÓN:

Auditoría y seguridad de la información

LIMA – PERÚ

2019

Dedicatoria

Dedicamos al todopoderoso, que con su gran amor todo es posible. A nuestros papás, por su ayuda y soporte fidedigno. A nuestros familiares, por todo su apoyo. Además, a nuestros profesores, que con sus enseñanzas nos brindaron valores y sabiduría. Y cada una de las personas que nos incentivaron y ayudaron a cumplir nuestro objetivo.

Luis Huamani y Alexander Cruz

Agradecimientos

A nuestra Universidad Cesar Vallejo, a nuestra respetable facultad de Ingeniería de Sistemas y a cada uno de los Docentes que en el transcurso de nuestra formación académica nos brindaron todos sus conocimientos relacionados a la ingeniería y todas las áreas correspondientes a nuestra carrera. A nuestras familias que han estado a lo largo del desarrollo de la tesis.

Luis Huamani y Alexander Cruz

Índice de contenidos

Índice de figuras

Índice de tablas

Índice de anexos

Índice de abreviaturas

Sigla	Significado	Pagina
IS	Information security	XII
TIC	Tecnología de la información y comunicación	2
NTP	Norma técnica peruana	2
ONGEI	Oficina Nacional de Gobierno Electrónico e Informática	2
PCM	Presidencia del consejo de ministros	2
TI	Tecnología de la información	3
SGSI	Sistema de gestión de seguridad de la información	7
GSI	Gestión de seguridad de la información	7
SI	Seguridad de información	7
SBS	Superintendencia de banca y seguros	8
SSI	Sistema de seguridad de la información	9
PDCA	P (plan), d (do), c (check), a (action)	12
ISO	Organización Internacional de Normalización	18
SPSS	Paquete Estadístico para las Ciencias Sociales	33

PRESENTACIÓN

La investigación se realizó gracias a un análisis aplicado a la empresa Zeppelin Inversiones Generales S.R.L., el cual refleja cómo se encuentra actualmente la SI, nosotros nos enfocamos en el problema actual que es la carencia de un SGI el cual va permitir garantizar que los activos e información de la empresa sea confidencial, integra y disponible, la cual debe ser usada de forma correcta resguardada por las TIC. Al no existir un sistema automatizado puede desencadenar muchos problemas, como la perdida de información dentro de la organización, además al no contar con políticas de seguridad exponen su información diversos riesgos, puesto que al ocurrir cualquier evento no sabrían cómo reaccionar y usarían las TIC de manera incorrecta.

Al observar este problema nos planteamos esta pregunta: ¿Qué efectos produce la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa ZEPPELIN Inversiones Generales S.R.L.?; ante esta interrogante afirmamos con el objetivo: Determinar el efecto de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa ZEPPELIN Inversiones Generales S.R.L. ; es por esto que esta investigación está enfocada en la automatización de un sistema de seguridad de la información el cual nos facilite controlar y asegurar la información de esta empresa mediante la automatización de un SI, además de implementar normas de seguridad que controlen las incidencias, y de esta manera ejecutar el ciclo de PDCA que es planificar, hacer, verificar y monitorear la seguridad de la organización, aplicándolo a nuestra población y muestra que son 1000 registros de las diferentes áreas.

En cuanto a los inconvenientes presentados el principal fue la ubicación geográfica, puesto que la empresa está ubicada en lima, y la investigación se realizó en los meses de diciembre y enero del 2018 y 2019 respectivamente.

Finalmente, nuestra investigación tuvo éxito puesto que logramos implementar un sistema de automatización de la seguridad de la información basado en la norma ISO 27001 en la empresa.

RESUMEN

Esta investigación tiene como finalidad la automatización de la seguridad de la información basada en la norma técnica peruana ISO 27001 para mejorar la seguridad en cuanto al uso de la información, ya que se observaron problemas de SI como la mala gestión y perdida de la información en la empresa Zeppelin Inversiones Generales S.R.L.

Planteando como objetivo observar el impacto que causa la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa Zeppelin Inversiones Generales S.R.L., ya que con la implementación de esta norma y sus controles se podrá corregir los puntos débiles y gestionar correctamente cada riesgo con la SI.

Obteniendo como resultado que con la implementación de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa Zeppelin Inversiones Generales S.R.L., se logró corregir y mejorar la SI.

Palabras claves: *norma, seguridad informática, sistemas de información.*

ABSTRACT

The purpose of the investigation is the automation of information security based on the Peruvian technical standard ISO 27001 to improve security regarding the use of information, since IS problems such as mismanagement were observed. and loss of information in the company Zeppelin Inversiones Generales SRL

Setting the objective of observing the impact caused by the automation of information security based on the Peruvian technical standard ISO 27001 in the company Zeppelin Inversiones Generales SRL, since with the implementation of this standard and its controls, risks can be corrected and managed to which the information and the IS may be exposed.

Obtaining as a result that with the implementation of information security automation based on the Peruvian technical standard ISO 27001 in the company Zeppelin Inversiones Generales S.R.L., it was possible to correct and improve the IS (Information Security).

Keywords: *standard, computer security, information systems.*

I. INTRODUCCIÓN

Hoy en día vivimos en un mundo donde lo más importante es la información tanto para una organización o empresa sin importar el rubro o giro a lo que se dedique, si pasara alguna ocurrencia con la confidencialidad, esto podría ser una desventaja o hasta podría quedar expuesta a la quiebra de dicha empresa, por ello las organizaciones han invertido en mejorar su infraestructura para prevenir que roben o manipulen su información con la creación y compra de nuevas TIC.

Es por esto que la PCM (2012) aprobó el uso obligatorio de la norma técnica peruana "NTP-ISO/IEC 27001:2008 EDI" el cual tiene como objetivo aumentar los niveles de SI con el fin de proteger la información en las organizaciones y otorgando la responsabilidad a la ONGEI para que regule y controle esto.

En nuestro país las instituciones estatales están obligadas a seguir el diseño e implementación de un SGSI, basándose en la NTP ISO/IEC 27001:2014 aprobada el 8 de enero del 2016 por la resolución ministerial N°004-2016-PCM.

Del punto de vista de los negocios, los sistemas de información son muy importantes y les dan un valor adicional a las empresas, ya que les permite manejar mejor la información adquiriéndola, transformándola y distribuyéndola de una mejor manera para que los jefes de la empresa puedan tomar mejores decisiones, mejorando el desempeño de la organización e incrementan su rentabilidad (Laudon y Laudon, 2012).

Además, realizar mantenimientos tanto preventivos como correctivos a los equipos, manejar las altas y bajas, gestionar los equipos con garantía y los movimientos de los equipos informáticos. Esta oficina identifico distintos problemas, como por ejemplo no cuentan con una base de datos donde almacenar sus datos y solo usan un archivo de Excel que está expuesto y toda persona que tiene acceso a las computadoras pueden manipular esta información arriesgando la confidencialidad de estos. Asimismo, no poseen servidores de base de datos donde pueden guardar todos los archivos de Excel que son la información de la empresa.

Por ello en la empresa Zeppelin Inversiones Generales S.R.L, se observa que no conocen la normativa, por lo tanto, no han establecido limitaciones de SI que se utilicen basándose en la NTP ISO/IEC 27001/20014, que les ayudara a prevenir,

proteger y recuperara su información ante cualquier percance o atentado que pueda dañarlos.

Las TI y los SI constantemente están expuestos a diversos riesgos e inseguridades ya que con el avance de la tecnología se crean nuevos virus, ataques informáticos los cuales rompen la seguridad de estos y es ahí donde ocurren los robos, fraudes y perdidas de información (Wenceslao, Vásquez Montenegro, & De la Cruz Guerrero, 2008).

Para sobreguarda sus activos de ciertas amenazas se necita conocerlas y conocer a que activos afecta para afrontarlas correctamente.
Es por eso que debemos implantar una correcta metodología y controles de seguridad enfocados en evaluar los riegos y medir su eficacia e información de la empresa Zeppelin Inversiones Generales S.R.L.

Después de todo lo expuesto párrafos arriba se llega tomar como una solución al problema identificado la automatización de la seguridad de la información basado en la norma técnica peruana ISO/IEC 27001 en dicha empresa.

El estudio se justifica de manera teórica porque a través de su desarrollo se pretende aportar más conocimientos sobre la norma aplicada y además se justifica de manera económica porque permitirá minimizar precios. A continuación, se sustenta las justificaciones planteadas.

Esta investigación se desarrolló con el propósito de aporta con los conocimientos que ya existen sobra la NTP ISO 27001 en la seguridad informática, buscando sistematizar la implementación, ya que con ello conseguiremos reducir la perdida de activos, porque está demostrado que con la ejecución de la NTP ISO 27001 se puede corregir todas las vulnerabilidades encontradas. Es importarte que el SGSI forme parte de los procesos en la empresa (NTP ISO/IEC 2013, 2014).

Atreves del desarrollo de la tesis, tienen como propósito promover el apoyo al área de TI y activos de la empresa, debido a que no tiene varias seguridades de información para controlar activos de TI, con el cual nos permitiría minimizar precios cada vez que suceda alguna incidencia de seguridad de información; ya que con esta medida de utilización de la automatización de la SI bajo la norma técnica

peruana ISO 27001, contribuirá a obtener los métodos precisos a la hora de detectar y evaluar cada peligro, amenaza y vulnerabilidad que se pueda presentar.

De acuerdo a la realidad problemática presentada se expone el problema general y los problemas específicos de esta investigación. El problema general es: ¿Qué efectos produce la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa ZEPPELIN Inversiones Generales S.R.L.? Los problemas específicos fueron:

PE1: ¿Qué efectos produce la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la confidencialidad de la empresa ZEPPELIN Inversiones Generales S.R.L.?

PE2: ¿Qué efectos produce la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la disponibilidad de la empresa ZEPPELIN Inversiones Generales S.R.L.?

PE3: ¿Qué efectos produce la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la integridad de la empresa ZEPPELIN Inversiones Generales S.R.L.?

El objetivo general del proyecto fue determinar el efecto de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa ZEPPELIN Inversiones Generales S.R.L.. Los objetivos específicos fueron los siguientes:

OE1: Determinar el efecto de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la confidencialidad de la empresa ZEPPELIN Inversiones Generales S.R.L.

OE2: Determinar el efecto de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la disponibilidad de la empresa ZEPPELIN Inversiones Generales S.R.L.

OE3: Determinar el efecto de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la integridad de la empresa ZEPPELIN Inversiones Generales S.R.L.

La hipótesis general de la investigación fue: La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 produce un efecto positivo la empresa ZEPPELIN Inversiones Generales S.R.L... Las hipótesis especificas fueron las siguientes:

HE1: La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 produce un efecto positivo en la confidencialidad de la empresa ZEPPELIN Inversiones Generales S.R.L.

HE2: La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 produce un efecto positivo en la disponibilidad de la empresa ZEPPELIN Inversiones Generales S.R.L.

HE3: La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 produce un efecto positivo en la integridad de la empresa ZEPPELIN Inversiones Generales S.R.L.

II. MARCO TEÓRICO

Este capítulo presenta antecedentes relacionados al proyecto los cuales permitieron tener mayores conocimientos sobre el tema como el diseño de un SGIS basándose en la ISO 27001 entre otros. Además, se detallan las teorías relacionadas a la investigación como la automatización, la SI, la ISO27001, gestión de riesgos, sistema web, etc.

Ochoa Andrea (2017) busca desarrollar un sistema web de GSI aplicado todos los pasos de SI de la norma ISO 27001 el cual permitirá evaluar, verificar y gestionar los riesgos de manera más fácil y tener el grado de importancia de los activos para la correcta GSI y de esta manera mejorarán los procesos y protegerán la información. Concluyendo que mediante el uso del sistema web se pudo desarrollar e implementar los procesos de la ISO 27001 de una mejor manera.

Talavera Vasco (2015) busca diseñar un SGSI para la protección y el uso correcto de la información mediante el uso de la ISO 27001:2013 el cual le permite aplicar correctamente los procesos del SGSI evitando la perdida de información y permitiendo que sea confiable, integra y disponible cuando lo necesiten. Concluyendo que se desarrolló con éxito el estudio y diseño del SGSI revelando diversos inconvenientes con el manejo de la información y demostrando que se necesita del apoyo de los líderes de la institución para la correcta aplicación del SGSI.

Yáñez Nelson (2017) busca aplicar un grupo de sistemas apoyado en open source para el diseño de un SGSI con precio accesible obedeciendo lo indicado en la ISO 27001:2013, mediante mejoras continuas de procesos de la institución. El SGSI debe alcanzar rangos apropiados de integridad, confidencialidad y disponibilidad de información institucional de modo que garantice la continuidad de los procesos en la institución, utilizando la ISO27001 con la finalidad de seguir el proceso de mejora continua de un SGSI en la empresa. Llegando a la conclusión que lograron reforzar sus conocimientos de SI de manera más estratégica y organizacional para la protección de activo más valioso que es la información. Permitiendo implementar nuevos procesos de control y políticas siendo estas el primer paso para el desarrollo un sistema de monitoreo que asegure el mejoramiento continuo de las políticas y procedimientos.

Moscaiza Omar (2018) busca diseñar un SGSI apoyado en la ISO 27001:2013, para poder gestionar los riesgos y asegurar un grado apropiado de SI, permitiendo adecuarse a lo que requiere la SBS. Concluyendo que con esta implementación y ejecución del proyecto pudieron gestionar mejor los activos y riesgos en la empresa y se cumplió lo requerido por la SBS.

Torres Martin (2018) busca diseñar un SGSI bajo la ISO/IEC 27001:2013 para preservar la información asociada al servicio Post-Venta del integrador de telecomunicaciones, el cual permitirá que esta sea más confiable, integra y disponible. Llegando a la conclusión que se logró establecer una estructura organizacional del SGSI el cual permitió implantar roles, responsabilidades y obligaciones con el manejo y cuidado del SI en la empresa.

Díaz Moisés (2016) busca elaborar una propuesta de SI para las TI, que minimice las amenazas y vulnerabilidades que atañen al robo de información en la empresa Care Enterprise Networs, aplicando la norma ISO 27001 que pertenece a la ISO, ya que esta explica la manera correcta de gestionar la SI de una organización, concluyendo que la SI y al ejecución de las TI en la empresa, no son bien aplicadas en la áreas principales de la organización y que hace falta utilizar software y hardware especializado que contrarreste los ataques que ha tenido la empresa, así como el robo y perdida de información a lo largo del tiempo.

Zacarías Jean (2017) busca determinar la influencia de un modelo de SI usando la ISO/IEC 27001:2013 el cual controlar los riesgos que puedan ocurrirle a los activos de información, debido a que la ISO/IEC 27001 es una norma internacional, que explica cómo manejar la SI. Concluyendo que gracias al desarrollo del proyecto se logró controlar los riegos a los que están expuestos los activos de información y además se logró concientizar al personal policial sobre la mitigación de los riesgos.

Santos Daniel (2016) busca desarrollar un SGSI usando la ISO/IEC 27001:2013, visto que el SGSI el cual permitirá que todos los involucrados pueda tomar mejores decisiones con la SI, permitiendo que la información sea confiable, integra y disponible en sus procesos mejorando continuamente y manejando correctamente la SI, concluyendo que se logró desarrollar nuevas ideas de gestión de riesgos,

normalizando los procesos de los sistemas y verificando todo lo requerido por la ISO/IEC 27001:2013.

Contreras Lidia (2017) busca diseñar un SGSI usando la norma ISO/IEC 27001 para cuidar la información de la institución ante cualquier riesgo de SI que pueda ocurrir, como la perdida de información, que está ya no sea confiable, integra y disponible cuando se necesite para los procesos, y con la aplicación de esta norma se podrá alinear y manejar la GSI correctamente. Concluyendo que lograron observar mejoras en la GSI de la institución permitiendo prevenir y gestionar mejor los incidentes que ocurren.

Betancur S., García H. y Largo J. (2016) busca por medio del marco de referencia ISO 27001:2013, una guía la cual permita definir políticas que establezcan el tratado de la información del proceso de gestión administrativa de manera confiable, confidencial y disponible para todas las áreas de la entidad, buscando que estas falencias sean controladas con un alto nivel de calidad para un SGSI para el proceso de gestión administrativa de forma tal que trascienda al interior de los programas de la universidad., llegando a la conclusión que por medio de este proyecto, se realizó un análisis de aquellas vulnerabilidades que frecuenta el área de gerencia de sistemas de la Fundación Universitaria María Cano y se estructuró una serie de políticas a partir de un SGSI para la gestión administrativa en la oficina mencionada, aplicando aquellos requerimientos que permitan obtener una serie de diagnósticos, estableciendo un grado de madurez de la institución frente a la GSI.

Molina Andrés (2015) busca identificar los procesos precisos para la GSI aplicando la ISO/IEC 27001:2013, ya que gracias a esta se podrá definir los requerimientos necesarios para la implementación de un SGSI y todos sus procesos el cual mejore constantemente para el beneficio de la empresa. Concluyendo que gracias al desarrollo del proyecto lograron mejorar los procesos de SI ya que lograron mejorar sus procesos para el cumplimiento de las políticas de seguridad.

Nieves Arlenys (2017) busca diseñar un SSI sustentados en la norma ISO/IEC 27001:2013, ya que esta permitirá controlar todos los posibles riesgos que le puedan ocurrir a la organización, sirviendo como modelo para las distintas instituciones de tecnología, puesto que la norma más reconocida es la ISO/IEC

27001:2013, concluyendo que se pudo detectar y medir esos riesgos a los que están expuestos la información permitiendo observa el impacto que pueden tener estos en los procesos de la empresa y además permitiendo tener la información disponible, integra y confiable.

Camargo Juan (2017) busca elaborar un SGSI basado en la norma ISO 27000 e ISO 27001 porque no cuenta con uno y es muy importante que lo tenga para que pueda proteger toda la información de la institución y de esta manera pueda reconocer, manejar y minimizar esos riesgos a los que se expone toda su información mediante normas y procesos que le permitirán llevar acabo todo eso. En el proceso de la investigación se llegó a la conclusión de que gracias al análisis de riesgos realizado dentro de la misma se pudo identificar de manera temprana un resultado negativo en el cuál se presencia que la empresa no cuenta con controles para la información pudiendo contener problemas en la protección y su seguridad.

Baca Víctor (2016) tiene como finalidad el desarrollo de un SGSI basándose en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 en especial al marco de trabajo COBIT 5, todo esto con la finalidad de satisfacer los caracteres de seguridad puesto que los anteriores han sido poco efectivos. El SGSI permitirá determinar procesos y procedimientos para llevar una política de seguridad adecuada puesto que ayudará a gestionar controles de seguridad y de esta manera mejorar el proceso de gestión de incidentes detectados.

Doria Andrés (2015) busca elaborar un SGSI aplicando la ISO/IEC 27001:2013, ya que esta especifica lo que se requiere para elaborar, ejecutar, y perfeccionar un SGSI documentado, considerando los riesgos empresariales que se puedan presentar en la organización. Puesto que esta norma nos expone la manera la manera en la que se debe trabajar para establecer un diseño SGSI y controles de seguridad según lo requiera la organización, concluyendo que gracias a este proyecto podremos identificar los pros y contra que se puede formar a partir del SGSI en cualquier organización moderna y/o en las oficinas TI de la Universidad de Córdoba. Así mismo se puede conocer atreves de un análisis diferencial los procesos de seguridad, además permitió elaborar políticas de seguridad que deben ser informadas a los funcionarios de la Universidad con la finalidad de mantener los niveles de riesgos aceptables.

Oidor Juan (2016) busca diseñar un SGSI usando la ISO/IEC 27001:2013, ya que permitirá amortiguar y reducir los peligros a los cuales están expuestos los activos de información, y a administrar correctamente la SI de la empresa, concluyendo que gracias al proyecto lograron identificar que el activo más valioso que tienen es su información y es el principal para obtener todos los objetivos que se plantearon y asegurar la constancia del negocio, es por esto que tienen claro que necesitan implementar un marco de trabajo para proteger la información correctamente sin importar el proceso en el que se utilice.

Olaza Hugo (2017) pretende implementar la NTP ISO/IEC 27001 para mejorar la SI ya que tiene varias problemas de TI y de manejo de información porque está constantemente expuesta y en peligro de ser manipulada y plantea corregir todo esto aplicando como metodología a MAGERIT ya que le permite gestionar los riesgos de manera correcta y así ayudar a la entidad a tomar decisiones, concluyendo que la utilización de la norma logro mejorar la seguridad en un alto nivel ya que lograron alcanzar el 95% en confidencialidad de la información.

Berrio Juan (2016) busca desarrollar una metodología para evaluar el funcionamiento de los SGSI usando la norma ISO/IEC 27001, aplicando la metodología Delphi ya que esta permite gracias a los conocimientos y experiencias de los expertos seleccionar adecuadamente las opciones que necesita un proyecto y descartar las que no son necesarias. Concluyendo que a pesar de que existan normas establecidas internacionalmente para el manejo un SGSI, se podría implementar una metodología adaptable a nuestro rubro y de estar manera contribuya al crecimiento y a mejorar continuamente el negocio, cumpliendo todos los objetivos de la organización.

Maureira Daniel (2017) busca implementar la ISO27001, con el fin de plantear un SGSI que asegure que se cumpla todos los procesos de seguridad para la información siendo auditable, disponible, confiable e integra, usando la metodología MAGERIT la cual permite proteger nuestros activos de información porque permite analizar y gestionar esos riesgos a los cuales son vulnerables los sistemas de información, concluyendo que el desarrollo del proyecto permitió desarrollar políticas de SI, además lograron detectar el estado del SI de la entidad y los beneficios que trae implementar esta norma.

Espinosa J., García R. y Giraldo A. (2016) busca diseñar y desarrollar un SGSI apoyado en las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013, para resguardar la información ya que no cuentan con acciones para protegerla de esos riesgos que están expuestas como la perdida de información o ingreso no permitido a esta, la metodología aplicada es la MAGERIT ya que MAGERIT es utilizada para mitigar y controlar esos riesgos los cuales se enfrentan las empresas al momento de la implantación y uso de las TIC, concluyendo que el análisis e identificación de riesgos ha permito conocer a profundidad los puntos más vulnerables de la entidad y de esta manera permitió hallar la mejor forma de mitigarlos.

Chipulina, L. (2018) tenía como objetivo implementar un sistema web el cual le permita observar el impacto que logra en la gestión de incidencias, usando SCRUM como la metodología, como lenguaje de programación PHP y MariaDB como base de datos para el desarrollo del proyecto. Concluyendo que la implementación del proyecto logro mejorar la gestión de incidencias.

Nilton Niño (2018) tienen como objetivo implementar un SGSI para para proteger su data de cualquier evento que pueda perjudicar la continuidad de los servicios en la institución, mejoran la confidencialidad, integridad, disponibilidad y el monitoreo de sus activos de información, utilizando el modelo PDCA y la metodología Magerit VS3 que les permitirá obtener un SGI, tomando en cuenta todos los aspectos y procesos administrativos de la NTP ISO/IEC 27001:2014. Concluyendo que lograron identificar los riesgos a los que están expuestos los activos de información mediante la seguridad implementada.

Bermúdez Kelly, Bailón Edber (2015) ofrecen analizar la seguridad informática y SI mediante el uso de la norma ISO/IEC 27001 para establecer los riesgos que puedan ocasionar por la ausencia de controles de SI. Llegando a identificar la necesaria implementación de controles de seguridad para proteger su información y fortalecer la confidencialidad, integridad y disponibilidad de ella. Además de mejorar el compromiso de los trabajadores y su trabajo en equipo con la empresa para el correcto cumplimiento de la seguridad.

Gonzales Iván, (2017) se plantea diseñar e implementar controles de seguridad para el mejoramiento de las redes de comunicaciones en un centro de datos, de

una entidad del estado, para que manipule la información de manera correcta con los controles de seguridad que brinda la NTP-ISO/IEC 27001:2014 que mejorar la seguridad y controlar los riesgos a los que son vulnerables. Obteniendo la conclusión que es una buena opción la implementación del proyecto, que mejora la seguridad y la comunicación en la red, ayudando a detectar mejor los riesgos gracias a la correcta aplicación de los controles de seguridad.

Herrera Francisco, Olivos Frank, Guevara Erick (2017) pretende formular políticas de seguridad para proteger en área de TI y los accesos a la ellos, usando la NTP-ISO/IEC 17799, en los ambientes de computo de la Universidad de Lambayeque, ya que no tienen las políticas de SI. Y de esta manera evaluar el estado de la SI de la dicha universidad y llegando a la conclusión que la implementación de todas las medidas de seguridad conlleva a un esfuerzo grande ya que no pose con los controles necesarios de SI.

Alcántara Julio, (2015) pretende desarrollar una guía de seguridad para mejorar la de los sistemas de información usando la ISO/IEC 27001, puesto que tienen muchas deficiencias en cuanto a la SI. Para la elaboración de la guía recolectaron información la cual les ayudo a logrando identificar los problemas a los que están propensos y definir los parámetros de seguridad y de confiabilidad. Concluyendo que gracias a esto detectar y controlar a tiempo las amenazas mediante estrategias y además lograron concientizar a los trabajadores sobre el manejo correcto de las políticas de seguridad.

Quispe José (2018) pretende proponer un plan de SI usando la ISO /IEC 27001:210 para mejorar el proceso de obtención de brevetes, ya que este proceso presenta muchas deficiencias en cuanto a información porque a veces la información está expuesta a cualquiera, o cuando es solicitada es errónea o no existe, y con la norma se podrá mejorar la SI. Concluyendo que para la aplicación del pal se necesita la ayuda de la gerencia para poder aplicarla correctamente y se respeten los procesos.

Merino José, Torres Edgar (2016) proponen poner en práctica un modelo de GSI con ITIL v3 que se pueda implementar en empresas pequeñas y medianas, para que puedan controlar los peligros y amenazas que puedan tener diariamente

mediante la gestión de seguridad. Esto se aplicó en la Pyme de TI IT-EXPERT y se logró mejorar la operatividad y calidad en los servicios de TI de la empresa.

Encala Reinaldo (2017) buscan desarrollar un sistema llamado XSIS el cual detecte las vulnerabilidades y peligros que puedan sucederle a los activos de información, basándose en la NTP ISO 27001:2013 e ISO 27002:2013, acoplando a COBIT 5 y sus buenas prácticas, para la correcta protección de la información. Teniendo como resultado que gracias a la aplicación del sistema se logró el objetivo mencionado y se pudo identificar que se puede realizar auditorías de SI con el personal de la empresa.

Vilca Ehytel, (2017) diseño un SGSI usando la ISO 27002 para cuidar las tecnologías y activos de información de la empresa Geosurvey, aplicando las cuatro fases PDCA de la ISO 27002 ayudando a controlar, mejorar la gestión de riesgos de incidentes y elaborar políticas de seguridad para obtener una mejor SI en la empresa, consiguiendo mejorar los procesos de la empresa.

Tola Diana (2015) se pretende mejorar la seguridad de la empresa A&CGROUP S.A. implementando un SGSI usando la ISO 27001:2005 para ayudar a cuidar la información y los procesos de la empresa utilizando correctamente la gestión de riesgos mediante la técnica MAGERIT. Luego de la puesta en marcha se observó que se necesita el apoyo de la cabeza de la empresa para conseguir que se efectúe de manera correcta y con el personal adecuado el SGSI para que todo se pueda llevar de la mejor manera.

De La Cruz Ronald (2016) propone mediante la ISO 27001 evaluar, aplicar políticas, normas y buenas prácticas para la GSI en la municipalidad de Paita de acuerdo a lo solicitado por el estado para mejorar sus procesos y proteger el manejo de su data. Luego de evaluar y sondear a los trabajadores realizamos el diagnóstico de la SI en la empresa, obteniendo la siguiente conclusión que están propensos a correr peligros, riesgos y necesitan tener controles, políticas y normas para cuidar de la información, las cuales permitirán no perder la información.

Cueva Paul y Ríos Juan (2017) pretende mejorar la gestión de historias clínicas y la SI usando la ISO/IEC 27001:2014 ya que el hospital cuenta con varias deficiencias en cuanto a información, como la perdida, la duplicidad y el mal ingreso

de las historias, además de que no están disponibles porque se encuentran dispersas en diferentes locales. Concluyen que lograron mejorar parcialmente la SI y la gestión de historias clínicas ya que hay información de historias clínicas que tienen que ser digitalizada que es parte de la SI que está en proceso de adaptación porque cuentan con demasiados procesos los cuales tienen que ir adaptándose de acuerdo a lo que exige el estado.

Tarrillo Marleni (2016) busca identificar la influencia que existe entre la gestión de riesgos y la SI para lograr reducir y controlar los peligros a los que esta propensa la información y sus activos, mejorando la integridad, confidencialidad y disponibilidad de ellos y poder protegerlos. Concluyendo que si tienen gran influencia estos procesos y que con una correcta gestión se puede proteger la información de cualquier amenaza

Llontop Gianmarco (2018) busca evaluar y optimizar el patrón de gestión de riesgos utilizado en todas las entidades a las cuales les ofrece soporte como servicio para su gestión de TI, basándose en la ISO 27001 y utilizando la metodología Magerit para gestionar los riesgos correctamente. Concluyendo que su efectividad de la gestión de riesgos aplicada varia de acuerda al tipo de negocio al cual le dan soporte, planeando mejorar la efectividad de este patrón para mejorar la gestión de riesgo en las empresas a las cuales ofrece soporte.

Moyano Luz y Suarez Yasmin (2017) busca implementar un SGSI bajo a ISO 27001:2013 con fin de mejorar el proceso de su área de Tecnológica y garantiza su seguridad, identificando los riesgos para ser analizados y tratados mediante la metodología PHVA (planificar, hacer, verificar y actuar) trabajando en conjunto con las normas de la empresa. Concluyendo que con la implementación de este proyecto se logró identificar carencias que tienen en cuanto a seguridad de información, como procesos, documentos y el correcto manejo de la información.

Agurto Manuel (2017) buscó desarrollar este diagnóstico para identificar como manejan los activos de información ya que producen mucha información que está expuesta a pérdidas o modificaciones y buscan mejorarla basándose en la ISO 27001 para el correcto desarrollo del proyecto. Llegando a la conclusión que a la hora de manejar los activos de información detectaron diversas irregularidades lo

cual llevo a planificar técnicas de control de seguridad basados en la ISO 27001 y ISO 9001 para gestionar los procesos correctamente.

Molano Rafael (2017) busca establecer la estrategia correcta para la implementación de un SGSI que le permita mejorar las carencias en la SI de la empresa ya que están expuestos a muchos ataques de robo o pérdida de información por internet, basándose en la ISO 27001 para la correcta evaluación de los riesgos. Llegando a la conclusión que luego de establecer la correcta estrategia que se debe desarrollar para la implementación de un SGSI se logró detectar los riesgos a los que son propensos y poder corregirlos para poder cuidar la información y que la empresa no sea afectada.

Martínez Alexander, Ramírez Erney, Merchán María y Suarez Yaditza (2016) diseñaron un SGSI basándose en la ISO 27001 para el área de sistemas de la Cámara de Comercio de Aguachica, para detectar y minimizar los riesgos a los que son propensos constantemente, implementando técnicas e instrumentos para recolectar información, de esta manera luego de la implantación se lograron evidenciar la falta de manejo correcto de información en sus procesos basándose en las normas de SI que asegure que esta sea confiable, integra y disponible según ISO27001.

Fernández Dámaris (2015) propone implementar una metodología y buenas prácticas para la gestión de riesgos, que se acomoden a los requerimientos de la SBS en CRAC Sipán SAC una entidad de crédito, usando la norma ISO/IEC 27001, ISO 17799 y Magerit como metodología de referencia para la gestión de riesgos de TI, para mejorar sus procesos financieros, proteger su información y mejorar el tratamiento de los riesgos. Concluyendo que mejoraron la efectividad del SGSI y la toma de decisiones en la organización basándose en los requerimientos establecidos por la SBS.

Rudas, L. (2017) quiere diseñar un modelo de Gestión de riesgo el cual permita unir todos los instrumentos necesarios para prevenir y controlar situaciones de peligro que puedan afectar el desarrollo de los proyectos y tenga impactos negativos en cuanto dinero y tiempo para la empresa Industrial Automation México. Aplicando las mejores prácticas analizadas y alineándolas con las características de la

organización, el cual tiene procesos y actividades que permite el desarrollo del modelo. Concluyendo que gracias a este proyecto lograron identificar la importancia de tener este tipo de modelos para el desarrollo de la empresa ya que permite implementar la cultura de prevención reactiva en los proyectos para evitar riesgos.

En esta sección se describe las teorías relacionadas al tema los cuales permitirán tener mejores conceptos del tema para un mejor entendimiento de la investigación.

Automático es la “Ciencia que trata de reemplazar al humano por una maquina o equipo electrónico.” (Real Academia Española, 2018, párr. 9).

Automatización es sustituir las tareas manuales de un proceso para realizarlas de forma autónica ya sea por una máquina, un robot u otro tipo de automatismo (Departamento de Ingeniería Eléctrica, Electrónica y de Control, pág. 3).

Es un sistema de control que manipula de forma indirecta los valores de un sistema controlado. Su propósito es administrar un sistema sin la intervención del operario sobre los recursos. El operario dirige los valores de referencia y el sistema de control se encarga de enviarlos al sistema manejado por los accionamientos de salidas (FIUBA).
Torres F. es un sistema el cual realiza tareas con parámetros ya establecidos sin que una persona lo maneje, mejorando el rendimiento en procesos manuales y repetitivos con una producción continua de mayor velocidad y de calidad (PP. 5-6).

Gestión de riesgos “se debe considerarse un proceso repetitivo que analiza y prioriza los riesgos, esta actividad da la posibilidad de tener una perspectiva descriptiva y precisa de los riesgos, además conforma una herramienta de elección de ellos que se seleccionan en ámbitos con recursos limitados.” (Gestión de los Riesgos Tecnológicos, 2008).

ISOTools Excellence indica que la gestión de riesgos es un proceso que idéntica riesgos y ejecuta controles adecuados que se usan cuando ocurren estos eventos y puedan controlarlos eficientemente brindando seguridad y confianza a la empresa (p. 11).

Riesgo de TI se describe como el riesgo del negocio ya que estos eventos afectan a la propiedad y operación de las TI afectando el funcionamiento de estos dentro de una empresa (Zúñiga A. y Solano M., PP. 3).

ISAC (2019) monitoreo de riesgos, en la informática sería más simple si los riesgos aparecieran luego de haber desarrollados las estrategias para manejarlos. Pero estos están desapareciendo y apareciendo por lo que necesitan ser monitoreados para proteger el control de los riesgos y detectar si existen nuevos sucesos que dañen a la compañía.

La norma ISO/IEC 27001 para ISO esta norma es perteneciente a la norma ISO 2700 ya que ayuda a conservar los activos de información de forma segura de las empresas. Su uso beneficiara a la empresa a dirigir la seguridad de los activos, como los datos financieros, propiedad intelectual, trabajadores e información compartida a terceros (iso2700).

Mintinick, K. (2017) “Las empresas invierten mucho dinero en dispositivos de seguridad y firewall, pero solo mal gastan su dinero ya que estos equipos no cubren al punto más frágil toda la cadena de seguridad que son los trabajadores y los equipos que administran.”

Núñez, A. (2007) “Es importante decir que el alcance que se ha definido para el proyecto sólo se toma la fase de Planificación del ciclo de Deming, dado que no se realizara la implantación del SGSI que se dé como resultado del mismo.” (p. 13).

ISOTools Excellence la norma ISO 27001 es un proceso de mejora continua que permite desarrollar un SGSI el permite detectar las amenazas o riesgos a los que están expuestas las empresas y pongan en peligro su información, permitiendo controlarlos y minimizarlas mediante estrategias y controles (p.4).

ISO 27001 es muy importante para las empresas porque permite que cumplan con los requerimientos legales ya que existen muchas leyes y nomas de SI, también brinda una ventaja comercial ya que les brinda mayor seguridad a su información, además ahorras costos ya que permite evitar incidentes que pueden afectar a la empresa y generar gastos, y por ultimo permite tener una mejor empresa más

organizada con procedimientos y procesos bien definidos (¿Qué es norma ISO 27001?).

Musayon y Vásquez (2011) un sistema web es un conjunto de procesos que trabajan con una serie de datos, que están estructurados de acuerdo a lo que necesita la organización, juntan, preparan y reparten la información necesaria con la que trabaja la organización, que sirve para las tareas de dirección y control que se encargan de desarrollar las estrategias de negocio.

Centro de investigación de la Web Universidad de chile (2008) la estructura y visibilidad de una página web está conformada en su mayoría por lenguaje HTML que es el más usado para el desarrollo de la estructura de estas, siendo el 75 % de las páginas que lo utilizan.

Centro de investigación de la Web Universidad de chile (2008) nos dice para saber la conectividad web que una página apunta a otra página se necesita recorrer toda la web, esto lo realizan los buscadores grandes periódicamente. El primer estudio de la web fue hecho en mayo y octubre de 1990 y se dio por 2 recorridos de AltaVista, con 200 millones de páginas cada uno y 1500 millones de enlaces. Esto quiere decir que es muy pequeño la cantidad de páginas apuntadas y enlaces.

Centro de investigación de la Web Universidad de chile (2008) nos dice que para saber la estructura de una web se debe buscar las partes del grafo que están unidas entre ellas. Muestra que el centro lo conformaban más de 56 millones de páginas, habiendo una trayectoria para ir de diferentes paginas a otras, en otras palabras, la vía más corta entre las páginas implicaba visitar 28 de ellas. De igual manera, la cantidad no es muy grande considerando que existen cientos de millones de páginas.

Cobarsí Josep (2013) nos dice que un SI es un grupo de servicios y contenidos que trabajan de manera conjunta, utilizando la tecnología, que es proporcionada por la organización para los trabajadores que sirve para producir y consumir los datos e información que son activos muy valiosos.

Mateu Carlos (2004) indica que el internet es un protocolo de datos o internet protocol, nos permitiría a que un grupo de ordenadores comunicarse a través de

una red, interconectadas de diversas redes. El Internet se convirtió en una necesidad fundamental, a tal punto que creció a un ritmo exponencial, hasta que en el año 2002 tuvo una pequeña pausa.

Gómez y Suarez (2009) la información “es un grupo de datos convertidos para minimizar las dudas lo cual ayuda a tomar decisiones.”

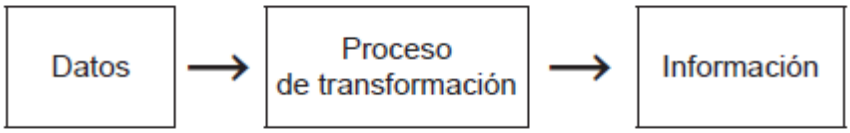


Figura 1 Proceso de trasformación de datos de información

Además, la información que se recibe después de que se procesan los hechos, añaden y muestran la mejor forma, para que sean útiles para cualquier trabajador de la empresa.

Aguilera, López (2011) características de un sistema de información se hace cargo de brindar información conveniente y exacta de forma adecuada a los trabajadores que lo necesiten y puedan tomar decisiones y operaciones en el momento exacto en que lo necesiten.

Universidad de Alicante (2013) como todos sabemos, la función de un navegador web es visualizar todo el documento relacionado a las páginas web que están compuestos por todo elemento de multimedia, que mayormente se guardan en los ordenadores remotos que están conectados al internet. Mediante los protocolos y normas de comunicación que a subes son conocidos como HTTP (protocolo de transferencia de hipertexto).

Gutiérrez, A. (2013) base de datos es un depósito de datos que se relacionan de diferentes maneras en la empresa. Estas son muy importantes en nuestra realidad, ya que son importantes tanto para el usuario, como para quien almacena de los datos en una tarea específica. el termino datos se refiere a la posibilidad de registrar, celulares, direcciones, apellidos, etc.

Gutiérrez, A. (2013) concepto de datos son sucesos de la empresa, que se refiere a algo que ocurrió, estos sucesos simples se les nombra "Data-ítem" o elemento de dato. Estos datos se pueden organizar o reorganizar de manera que se logra usar y se transforma en información.

Gutiérrez, A. (2013) una base de datos dinámica te permite hacer cualquier movimiento en cualquier momento permitiendo que se pueda actualizar, aumentar y consultar la información.

Peralta, A. (2003) la metodología Scrum es un proceso ágil que nos ayuda a desarrollar software y está centrada en actividades gerenciales, siendo Ken Schwaber y Jeff Sutherland quienes lo utilizaron primera vez y lo documentaron en el libro Agile Software Development With Scrum.

Scrum Manager (2016) indica que Scrum cuenta con 3 tipos de roles que son el product owner, el equipo de desarrollo y scrum master los cuales se detallara a continuación:

Scrum Manager (2016) el product owner es quien toma las mejores decisiones en base al producto, ya que es la persona que conoce perfectamente el negoció, las necesidades exactas del proyecto y adonde quiere llegar con el producto, dando prioridad a las necesidades del negocio (Scrum Manager, 2016, p. 32, 33).

Scrum Manager (2016) el equipo de desarrollo es un grupo multifuncional que está formado entre 3 a 9 personas que trabajan de manera generosa compartiendo responsabilidades, con tareas y responsabilidades específicas que siguen los pasos para ejecutar, colaborando con el desarrollo del proyecto en cada sprint y logro ya que todos conocen el objetivo del product owner (p. 33).

Scrum Manager (2016) el scrum master es el encargado de que se cumpla las normas de scrum capacitando al product owner y el equipo de desarrollo para que cumplan con el objetivo del producto bajo las normas de scrum, gestionando y revisando al grupo ante las dificultades que se puedan presentar (p. 33, 34).

Scrum Manager (2016) los artefactos son las herramientas utilizadas para la correcta gestion de scrum que son la pila del producto, pila del sprint y el incremento, los cuales sirven para ver los requisitos del usuario, los trabajos que tiene que realizar el equipo y ver los resultados de cada avance del proyecto (p. 21).

Lenguaje de programación es el idioma artificial de la computación que nos permite producir programas que manejen la conducta física y lógica de una máquina, mediante el uso de algoritmos exactos.

Todo lo mencionado, por medio de un lenguaje que aspira ser el próximo lenguaje humano o natural, así como sucede con el lenguaje léxico. Además, tiene como característica que puede utilizar grupos de instrucciones que son comprendidos entre ellos para la creación de un programa (Lenguaje de Programación).

Martínez, A. (1995) HTML es un lenguaje simple que nos posibilita hacer hipertextos, en otras palabras, textos estructurados y agradables, mediante un link que lleva a otros archivos o fuentes de información relacionados, con gráficos, sonidos, etc. se centra en detallar la estructura lógica, títulos, párrafos, enumeraciones, definiciones, etc., y los distintos efectos que les quieras dar.

Martínez, A. (1995) su estructura comienza con una etiqueta <HTML> y finaliza con </HTML>. Además, cuenta con diferentes zonas como el encabezado que está definido por <head> y </body> que es donde se definen los valores para todo el documento y su cuerpo y <body> y </body> que es donde radica la información del documento. Asimismo, la directiva <title> del encabezado permite detallar el título del documento HTML.

Martínez, A. (1995) URL es el nombre que reconoce el servicio que brinda dentro del enlace, uniendo la información mediante el WWW que era incompatible, pero utilizando el esquema http del mismo WWW.

Gabor, H. (2005) PHP es un lenguaje de acceso libre de nivel alto utilizado en HTML y ejecutado en servidores cortos y concisos. Asimismo, lo diferencia de JavaScript ya que se realiza en los servidores y no en el equipo del usuario. Además, una de sus ventajas es que es sencillo para los novatos, pero con propiedades avanzadas para los programadores expertos.

HTML5 es la quinta versión del estándar que se creó en 1990, siendo es un lenguaje markup utilizado para la estructura y presentación del contenido web, siendo uno de los puntos primordiales para el funcionamiento de los sitios. Además, la W3C recomienda ser utilizado de forma estándar para los proyectos futuros, ya que este formatea el layout de las páginas y los ajustes en su aspecto.

Asimismo, con HTML5 los navegadores tienen la posibilidad de saber mostrar ciertas páginas web. Sin embargo, la diferencia primordial es el de complejidad del código que podemos crear utilizando HTML5 (Entendiendo HTM5).

Solis, J. (2014) Bootstrap es una gran herramienta para generar interfaces que se adapten a cualquier dispositivo sin importar el tamaño que tenga utilizando JavaScript y CSS, esta característica se le conoce como responsive desing o diseño adaptativo y lo creo Twitter. Siendo muy útil ya que tiene mucha compatibilidad con la mayor parte de los navegadores web.

Areitio, J. (2008) la seguridad informática de toda organización es un desarrollo que mejora continuamente, en la que han de estar implicados todo el departamento de la empresa, las cuales deben de estar bajo un modelo de madurez eficaz que monitorea con valores cuantitativos y cualitativos, los riesgos de seguridad no solo de forma reactiva, si no proactiva y preventiva. Además, tiene que permitir controlar y observar con el máximo grado de detalle y profundidad, todo el aspecto del ciclo de vida infinito de mejora de la seguridad del negocio, haciéndolo acorde con los objetivos de productibilidad, competitividad y supervivencia, a veces cambiante.

Un SGSI según ISO 27001:2013, la SI es la conservación de la confidencialidad, integridad y disponibilidad, de los sistemas involucrados en el procedimiento, de la empresa. Asimismo, estos conceptos son la raíz de toda la seguridad de la información ya que la confidencialidad es no bridad información a procesos no autorizados, la integridad conserva la información y los procesos de manera precisa y completa y la disponibilidad es el uso de la información y sistemas de manera autorizada cuando es necesitada (Ávila, F., 2013).

Costas (2010) confidencialidad es la protección especial de la información para prevenir que se divulgue y cause daños considerables a la organización (ejemplificando, una estrategia que hará crecer a la organización es divulgada a la competencia, esto haría que la organización ya no pueda aplicarla como ellos querían y no le permitiría crecer).

Según Costas S., Jesús (2010) integridad es la eventualidad de un archivo de no ser modificado lo que concede que se pueda probar que es un archivo original que

no fue modificado. Además, esto asegura que el archivo es verdadero y exacto, sin necesidad de verificar su autenticidad o alguna modificación no permitida.

Costas (2010) disponibilidad según el programa MAGERIT, es el instante en que el dato está presente a la hora de ser solicitado por el por el usuario autorizado, y esto se da cuando te dan acceso a un sistema por un tiempo determinado de acuerdo a los elementos del sistema. Protegiendo la información y creando copias de seguridad, que sirve para reestablecer datos que puedan ser eliminados o afectados de forma accidentada o intencionada.

Alemany, J. (2004) ciclo de deming esta técnica la desarrollo W.A. Shewart y sirve para ordenar y dar seguimiento a toda clase de proyectos. E. Deming coge y extiende esto como opción para cualquier tipo de proyecto y acción del proceso, ya sea propio externo o interno.

¿CUÁNDO SE USA?

- Equipos de diseño.
- Equipos para analizar y solucionar problemas.
- Equipos de mantenimientos preventivos.
- Equipos de Logística.
- Etcétera.

Jimeno, J. (2008) el ciclo PDCA es el ciclo de Deming o de mejora continua, es la metodología que explica los cuatro pasos que se debe seguir de forma sistemática para alcanzar la mejora continua. los cuales integran las 4 fases periódicas del circulo de Deming que son planificar, hacer, controlar y actuar.

Análisis de riesgo es el proceso donde se ddetectan y ordenan los riesgos, se analizan las probabilidades y efectos de cada riesgo estableciendo así el grado de riesgo que tiene el proyecto (Gestión de Riesgos).

Existen 3 tipos de metodologías utilizadas para calcular el grado de riesgo.

- **MÉTODOS CUALITATIVOS:** Este método es el más utilizado para una decisión en un proyecto de empresas, además los emprendedores se sostienen de su juicio, vivencias y corazonadas para tomar decisiones. Pidiéndose emplear cuando el grado de riesgo es pequeño y no se tiene los

medios precisos para un análisis completo, o también cuando los datos numéricos no son los correctos para ser analizados de forma cuantitativa y pueda arrojar un resultado detallado del riesgo en general.

- **MÉTODOS CUANTITATIVOS:** Se da cuando se puede fijar valores a los riesgos detectados, en otras palabras, cuantificar el grado de riesgo del proyecto. Esto abarca el análisis de probabilidad, consecuencias y simulación computacional.
- **MÉTODO MONTECARLO:** representa la realidad por medio de un modelo de riesgo matemático, asignando valores aleatoriamente a las variables del modelo para obtener distintos enfoques y resultados. Realizando varias interacciones para que la muestra sea lo bastante grande para que represente la realidad.

"En informática, un sistema de información cumple varias funciones, administra, recolecta, recupera, procesa, almacena y distribuye toda la información que es importante para que se ejecute los procesos de las organizaciones." (Significados Informáticos, pág. 1).

Existen diferentes tipos de sistemas de información:

- **Sistemas de Procesamiento de Transacciones (TPS)**. Es conocidos como sistemas de gestión operativa, recolectan la información adecuada para de la organización, es decir, de su funcionamiento.
- **Sistemas de Información Ejecutiva (EIS)**. Controla las variables gerenciales de un área determinada de la empresa, partiendo de la información interna y externa de la empresa.
- **Sistemas de Información Gerencial (MIS)**. Observan la data general de la empresa y la perciben como un todo.
- **Sistemas de soporte de decisiones (DSS)**. Enfocados al proceso de data y extra organizacional, para el soporte en la conducción de la empresa (Conceptos de Sistemas).

III. MÉTODO

En este capítulo se redacta el tipo de investigación que fue aplicada, de diseño pre experimental y de enfoque cuantitativo, además se definen las variables del estudio como automatización y seguridad de la información. La población utilizada fueron 1000 registros del área de ventas para trabajar, usando como instrumento de recolección de datos la ficha de observación.

Según Hernández S. Roberto (2014) “El enfoque cuantitativo recolecta los datos para justificar premisas basadas en mediciones numéricas y estudios estadísticos, teniendo como objetivo implantar ejemplos de comportamientos y demostrar teorías” (p. 4).

Esta investigación usa un enfoque cuantitativo ya que con la recolección de datos generamos información la cual se puede medir mediante cuadros estadísticos y nos permite comprobar el impacto de la investigación frente al problema presentado, mostrando con números estadísticos si es positivo o no el impacto que se tuvo frente a la investigación planteada.

1.1 Tipo y diseño de investigación

Hernández S. Roberto (2014) la investigación aplicada, “tiene dos objetivos primordiales que son producir conocimientos y teorías que son las investigaciones básicas, y la resolución de problemas que se da en investigaciones aplicadas” (p. XXIV).

Esta investigación es una investigación aplicada ya que mediante nuestra investigación obtendremos nuevos conocimientos y aprenderemos teorías las cuales nos ayudaran a resolver el problema planteado aplicando los conocimientos y teorías aprendidas en nuestra investigación.

Hernández S. Roberto (2014) “El diseño pre experimental se enfoca en un grupo donde el control es mínimo y es utilizado para acercarse por primera vez al problema real que es investigado” (p. 130).

Se aplicará el diseño pre experimental en esta investigación ya que solo se manipulará la variable dependiente la cual es seguridad de la información, porque se pretende observar el impacto que tiene la variable independiente que es automatización sobre la variable dependiente que es seguridad de la información.

1.2 Variables y operacionalización

La variable manejada fue: Efecto de la Automatización de la seguridad de la información basado en la norma técnica peruana iso 27001 en la empresa zeppelin inversiones generales s.r.l.

Definición conceptual: La automatización tarea consta en reemplazar esas labores de manera manual por las mismas pero realizadas por una máquina, un robot o otro tipo de aparate que trabaje de manera automática. De esta manera, gracias al uso adicional de sensores, controladores y actuadores, así como de métodos y algoritmos de conmutación, se logra liberar a los humanos de algunas tareas (PAC- Performance-centered Adaptive Curriculum, p. 3).

- Seguridad de la información: La seguridad de la organización es un proceso de optimización continua, donde participan todos los trabajadores de la empresa, manejándose bajo un modelo eficaz que monitoree los valores cuantitativos y cualitativos, contra los riesgos de seguridad no solo reactivamente, sino proactiva y preventivamente. permitiendo observar y controlar al máximo detalle y profundidad el ciclo de vida de optimización de la seguridad del negocio de acuerdo a los objetivos de productividad, competitividad y supervivencia en ocasiones cambiante" (Areitio, 2008, p. 11).

Definición operativa: Permitirá automatizar, agilizar y mejorar los procesos manuales de la seguridad de la información basado en la norma técnica peruana ISO 27001 mediante un sistema.

1.3 Población, muestra y muestreo

Hernández S. Roberto (2014) la población es un con conjuntó de eventos los cuales tienen algunas características semejantes (p. 174).

La población está conformada por 1000 registros que pertenecen al área de ventas ya que es el área más importante para la organización porque maneja la información de los ingresos y egresos de la empresa, además se está tomando la información del mes de diciembre y enero las cuales son los meses donde se generan más ingresos a la empresa ZEPPELIN INVERSIONES GENERALES S.R.L. ya que las personas siempre consumen combustible porque salen de vacaciones y se movilizan constantemente con sus vehículos.

Hernández S. Roberto (2014) la muestra probabilística permite que cualquiera de los elementos encontrados en la población sean elegidos y sean usados en la muestra estableciendo los parámetros y el tamaño de la población seleccionando aleatoriamente o mecánicamente las unidades de muestreo o análisis (p. 175).

El tipo de muestra es probabilística ya que todos los registros de los procesos de ventas están en la base de datos de la empresa ZEPPELIN INVERSIONES GENERALES S.R.L. teniendo la misma posibilidad de ser seleccionados para la muestra ya que todos manejan información de la empresa y pueden ser vulnerables ante cualquier ataque o perdida de la información.

Hernández S. Roberto (2014) la muestra está conformada un segmento pequeño de la población del cual se recogen datos que son definidos y delimitados anticipadamente y con exactitud representando la población (p. 173).

La muestra de esta investigación es probabilística lo que significa que los 1000 archivos de información de la base de datos pueden ser escogidos para ser analizados para la muestra aplicando la siguiente formula:

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

Figura 2 Formula para calcular la muestra

Donde Z= Nivel de confianza, p= Porcentaje de la población que tiene el atributo deseado, q= Porcentaje de la población que no tiene el atributo deseado =1-p, N=

Tamaño del universo, e= Error de estimación máximo aceptado y n= Tamaño de la muestra, llegando a la conclusión que el tamaño de nuestra muestra es de 277.74.

1.4 Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Según Hernández S. Roberto (2014) “Instrumento que permite al investigador medir y registrar información o datos de las variables de su investigación” (p. 199).

Para recolectar la información de nuestras variables de la investigación utilizaremos la técnica de la observación, la cual trabajara con el instrumento de recolección de datos que es la ficha de observación.

Según Hernández S. Roberto (2014) “Este método que recolecta de datos se basa en registrar sistemática, valida y confiablemente las conductas y eventos que pueden ser examinados, por medio de un grupo de categorías y subcategorías” (p. 252).

Validez

Según Hernández S. Roberto (2014) “Es el nivel de veracidad de medición del instrumento al medir las variables” (p. 200).

Para validar nuestro instrumento de recolección de datos utilizaremos la técnica de criterio de jueces la cual consiste en evaluar le instrumento con 3 jueces especialistas los cuales nos ayudaran a mejorar la herramienta para la recolectar datos de la investigación.

Confiabilidad

Según Hernández S. Roberto (2014) “Es el nivel del instrumento para producir resultados consistentes y coherentes” (p. 200).

Según como se cita en apa (2017) “Existen instrumentos para recolectar de datos que no necesitan el cálculo de la confiabilidad como las entrevistas rubricas, hojas de registro, inventarios, entre otros, pero si se debe validar mediante la opinión de los juicios de expertos para revisar si la información planteada está bien redactada y permiten medir lo que se necesita medir” (p. 65).

De acuerdo a lo planteado nuestro instrumento de recolección de datos no necesita confiabilidad ya que utilizaremos la ficha de observación para recolectar los datos obtenidos de un sistema.

1.5 Procedimiento

La recolección de datos fue realizada con previa coordinación con el área encargada para que brinden de manera virtual los registros en Excel entre los meses de diciembre y enero pasados utilizados en la empresa, fueron elegidos estos registros ya que son los meses donde se encuentra más movimientos de datos en la empresa y poder aplicarlos al estudio.

1.6 Método de análisis de datos

Para analizar los datos utilizaremos la estadística descriptiva, la cual primero describe datos, valores o puntuaciones obtenidas por cada variable. (Hernández S. Roberto, 2014). Estos datos se obtendrán gracias a que aplicaremos la ficha de observación como instrumento para recolectar datos para cada una de nuestras variables y se analizará en el software estadístico SPSS.

Hernández S. Roberto (2014) la estadística inferencial tiene el objetivo es ir más afondo que explicar la distribución de las variables, es demostrar los resultados obtenidos con la muestra, población y/o universo demostrando la hipótesis (p.299).

1.7 Aspectos éticos

Este proyecto de investigación se compromete a tener mucha discreción con los datos e información brindada por la empresa y lo que se obtendrá al realizar la investigación, salva guardando la integridad de los encuestados y la información obtenida por ellos.

IV. RESULTADOS

En este capítulo se conoce los resultados de la investigación, que para realizar el análisis de los resultados obtenidos y describirlos se hizo uso de los indicadores de la investigación que son “gestión de claves”, “numero de información divulgada”, “accesos no autorizados”, “número de cambios no autorizados a los datos de producción”, “numero de virus informáticos” y “tiempo disponible del sistema para el usuario”.

Además, se observó la implementación de la automatización de la seguridad de la seguridad de la información basado en la Norma Técnica Peruana ISO 27001 en la empresa ZEPPELIN INVERSIONES GENERALES S.R.L., visualizando los resultados del procesamiento de los datos obtenidos por cada indicador en el pre test y post test con el software IBM SPSS Statistics 25.

A continuación, se realizó el análisis descriptivo del indicador gestión de claves de la dimensión confidencialidad de la variable seguridad de la información.

Análisis Descriptivo

Cálculo de Datos Descriptivos

Estadísticos

		Gestión de claves - PRE	Gestión de claves - POST	DiferenciaClaves
N	Válidos	1000	1000	1000
	Perdidos	0	0	0
Media		,16	,95	-,7870
Desv. típ.		,365	,228	,52717
Varianza		,133	,052	,278
Mínimo		0	0	-1,00
Máximo		1	1	1,00

Tabla 1 Cálculos Estadísticos Descriptivos de la gestión de claves

Tablas de Frecuencia

Gestión de claves - PRE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	842	84,2	84,2	84,2
	SI	158	15,8	15,8	100,0
	Total	1000	100,0	100,0	

Tabla 2 Tabla de Frecuencia Pre test de la gestión de claves

Gestión de claves - POST

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	55	5,5	5,5	5,5
	SI	945	94,5	94,5	100,0
	Total	1000	100,0	100,0	

Tabla 3 Tabla de Frecuencia Post test de la gestión de claves

Histograma

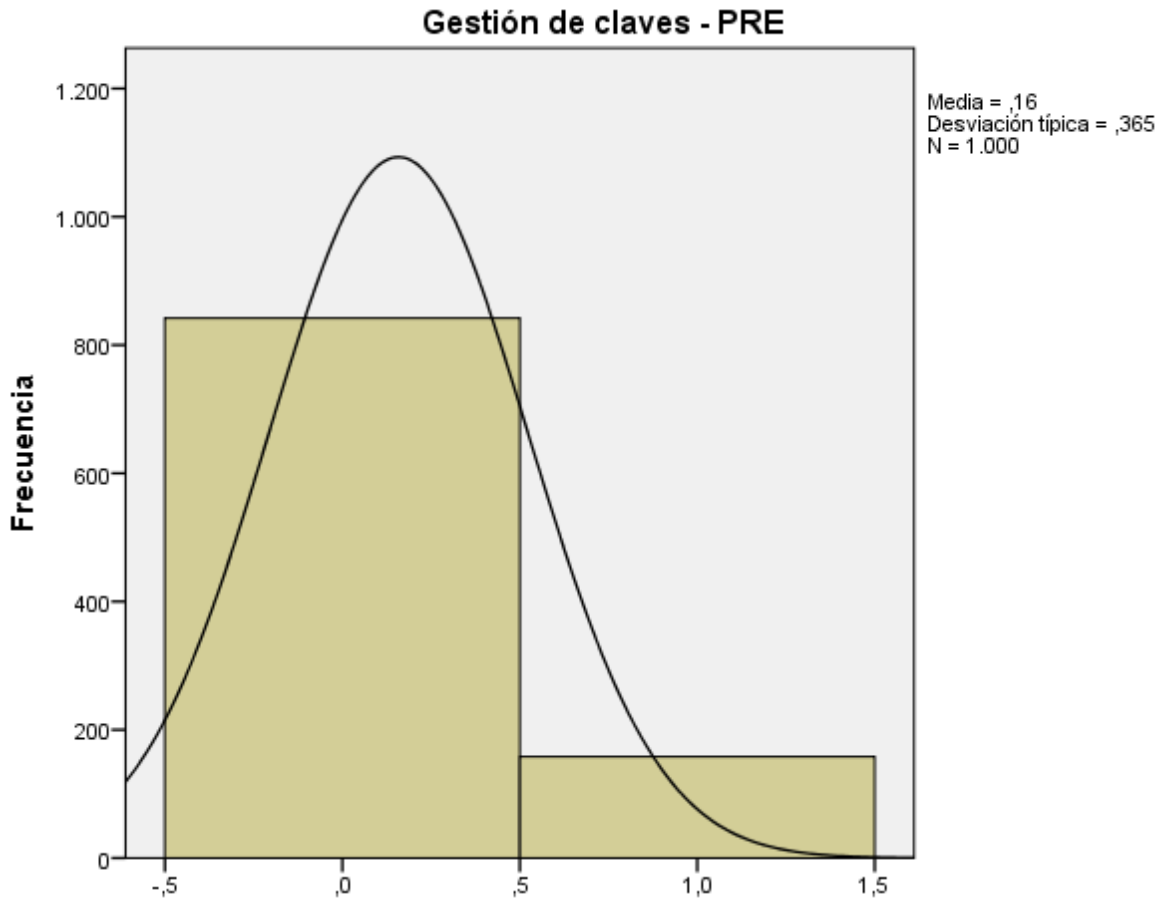


Figura 3 Gráfico de puntajes obtenidos en el Pre Test de la gestión de claves

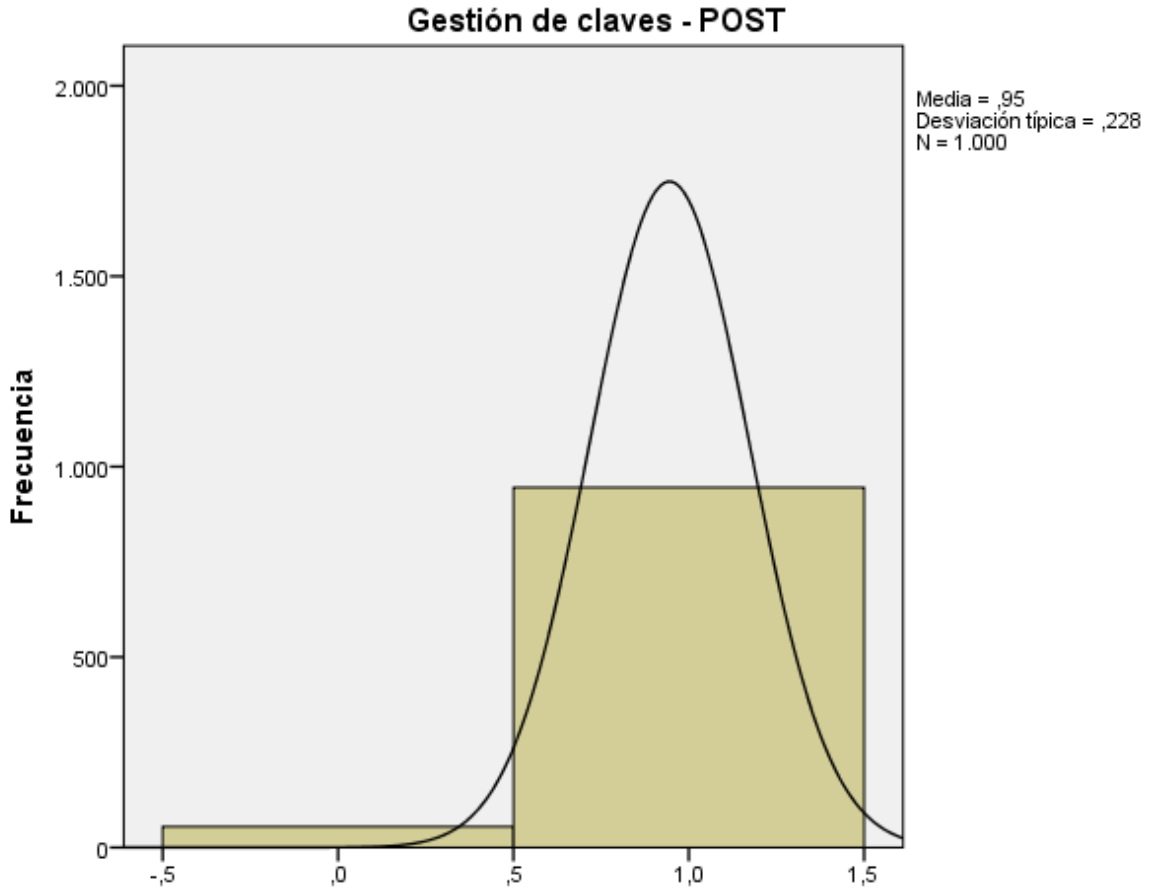


Figura 4 Gráfico de puntajes obtenidos en el Post Test de la gestión de claves

El resultado obtenido en el análisis del pre test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.16 en los resultados de la gestión de claves, con una desviación estándar de 0.365.

El resultado obtenido en el análisis del post test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.95 en los resultados de la gestión de claves, con una desviación estándar de 0.228.

Análisis Inferencial

Prueba de Normalidad

A continuación, aplicamos la Prueba de Kolmogoroc – Smirnov para determinar si una muestra es normal o no.

Prueba de Kolmogorov-Smirnov para una muestra

		Gestión de claves - PRE	Gestión de claves - POST	DiferenciaClaves
N		1000	1000	1000
Parámetros normales[a,b]	Media	,16	,95	-,7870
	Desviación típica	,365	,228	,52717
Diferencias más extremas	Absoluta	,509	,540	,499
	Positiva	,509	,405	,499
	Negativa	-,333	-,540	-,343
Z de Kolmogorov-Smirnov		16,111	17,085	15,777
Sig. asintót. (bilateral)		,000	,000	,000

a. La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

Tabla 4 Prueba de Kolmogorov – Smirnov de la gestión de claves

Como podemos observar, la tabla muestra que en la columna Diferencia la Significancia(Sig.) tiene un valor menor a 0.05 lo cual nos permite asegurar que la distribución del indicador es no normal.

Prueba de Hipótesis

Al tener la muestra una distribución no normal, utilizan la Prueba Estadística No Paramétrica, aplicando la prueba de rangos de Wilcoxon la cual nos da la hipótesis nula y alterna de la siguiente manera:

Hipótesis Nula (H0): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **no produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Hipótesis Alterna (H1): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Aplicación de prueba de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
Gestión de claves - POST - Gestión de claves - PRE	Rangos negativos	55[a]	449,00	24695,00
	Rangos positivos	842[b]	449,00	378058,00
	Empates	103[c]		
	Total	1000		

a. Gestión de claves - POST < Gestión de claves - PRE

b. Gestión de claves - POST > Gestión de claves - PRE

c. Gestión de claves - POST = Gestión de claves - PRE

Estadísticos de contraste[a]

	Gestión de claves - POST - Gestión de claves - PRE
Z	-26,277[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Tabla 5 Aplicación de Prueba No Paramétrica de Wilcoxon de la gestión de claves

Siendo el valor de Sig. (bilateral) 0 que es menor que 0.05, desechan la hipótesis nula y se aprueba la hipótesis alterna que es La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

A continuación, se realizó el análisis descriptivo del indicador número de información divulgada de la dimensión confidencialidad, de la variable seguridad de la información.

Análisis Descriptivo

Cálculo de Datos Descriptivos

Estadísticos

		Número de información divulgada - PRE	Número de información divulgada- POST	DiferenciaDivulgada
N	Válidos	1000	1000	1000
	Perdidos	0	0	0
Media		,84	,06	,7870
Desv. típ.		,365	,228	,52717
Varianza		,133	,052	,278
Mínimo		0	0	-1,00
Máximo		1	1	1,00

Tabla 6 Cálculo Estadísticos Descriptivos del número de información divulgada

Tabla de Frecuencia

Número de información divulgada - PRE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	158	15,8	15,8	15,8
	SI	842	84,2	84,2	100,0
	Total	1000	100,0	100,0	

Tabla 7 Tabla de Frecuencia Pre test del número de información divulgada

Número de información divulgada- POST

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	945	94,5	94,5	94,5
	SI	55	5,5	5,5	100,0
	Total	1000	100,0	100,0	

Tabla 8 Tabla de Frecuencia Post test del número de información divulgada

Histograma

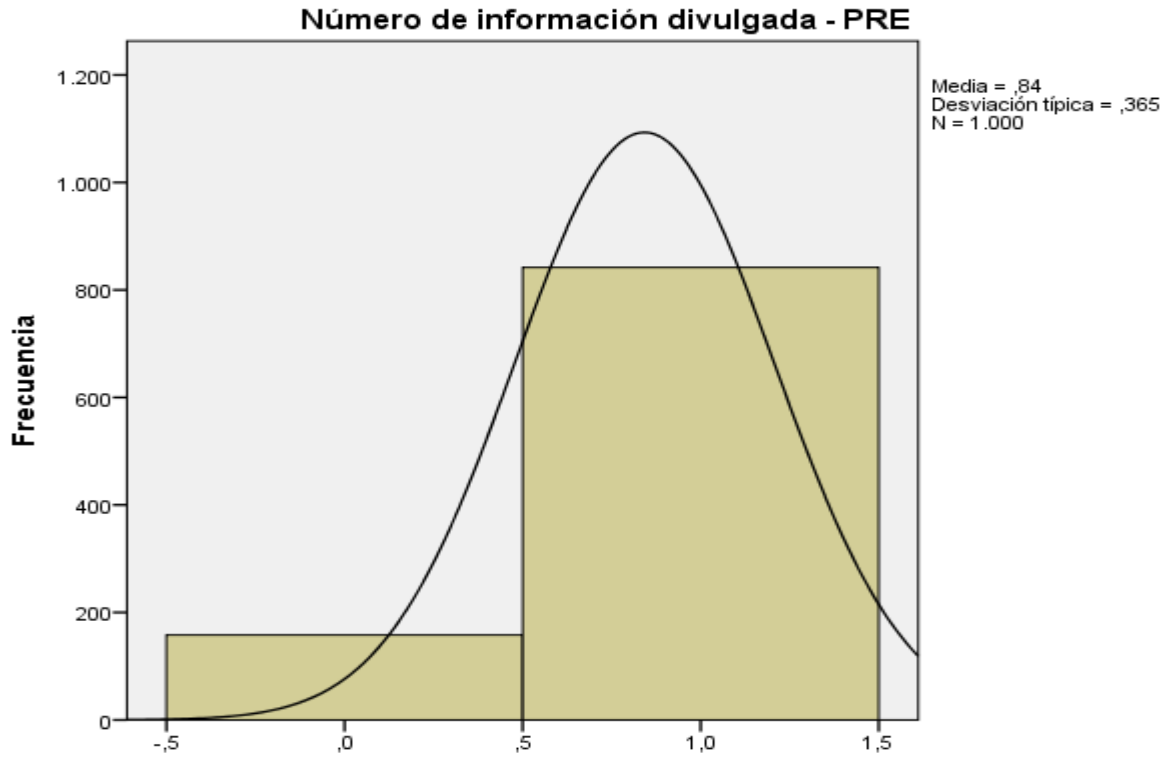


Figura 5 Gráfico de puntajes obtenidos en el Pre test del número de información divulgada

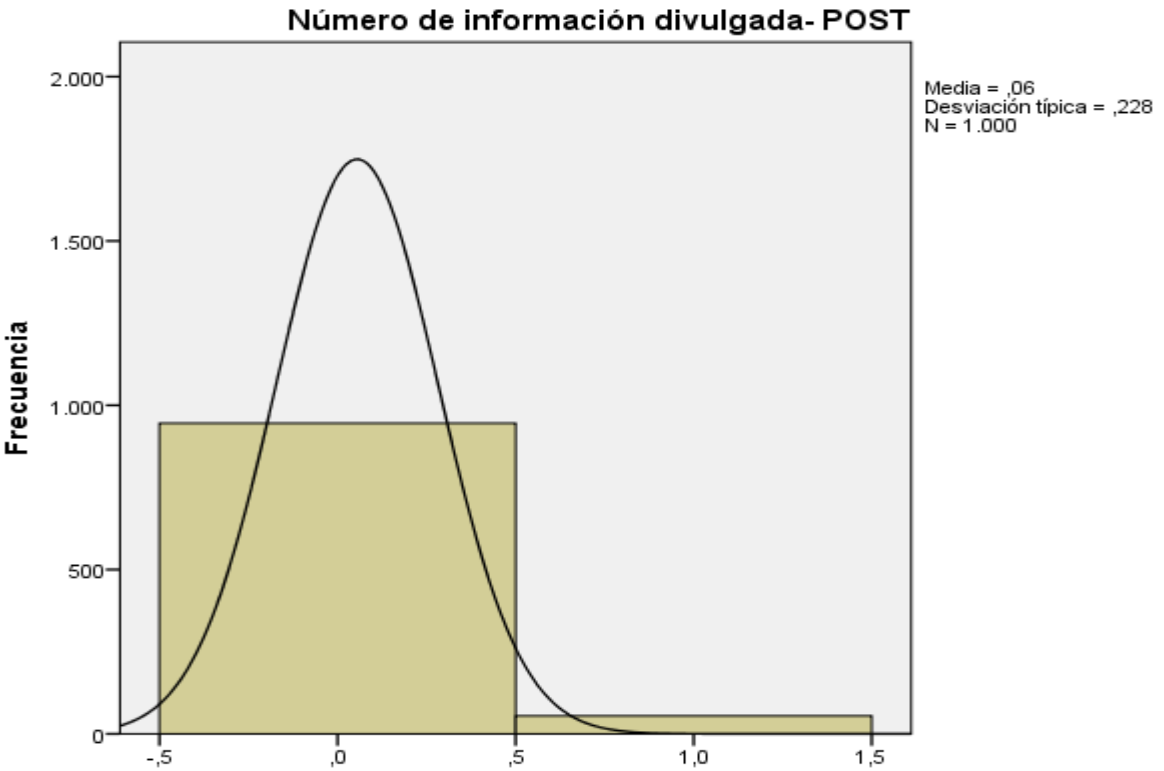


Figura 6 Gráfico de puntajes obtenidos en el Post test del número de información divulgada

El resultado obtenido en el análisis del pre test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.84 en los resultados del número de información divulgada, con una desviación estándar de 0.365.

El resultado obtenido en el análisis del post test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.06 en los resultados del número de información divulgada, con una desviación estándar de 0.228.

Análisis Inferencial

Prueba de Normalidad

A continuación, aplicamos la Prueba de Kolmogoroc – Smirnov para determinar si una muestra es normal o no.

Prueba de Kolmogorov-Smirnov para una muestra

		Número de información divulgada - PRE	Número de información divulgada- POST	DiferenciaDivulgada
N		1000	1000	1000
Parámetros normales[a,b]	Media	,84	,06	,7870
	Desviación típica	,365	,228	,52717
Diferencias más extremas	Absoluta	,509	,540	,499
	Positiva	,333	,540	,343
	Negativa	-,509	-,405	-,499
Z de Kolmogorov-Smirnov		16,111	17,085	15,777
Sig. asintót. (bilateral)		,000	,000	,000

a. La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

Tabla 9 Prueba de Kolmogorov – Smirnov del número de información divulgada

Como podemos observar, la tabla muestra que en la columna Diferencia la Significancia(Sig.) tiene un valor menor a 0.05 lo cual nos permite asegurar que la distribución del indicador es no normal.

Prueba de Hipótesis

Al tener la muestra una distribución no normal, utilizan la Prueba Estadística No Paramétrica, aplicando la prueba de rangos de Wilcoxon la cual nos da la hipótesis nula y alterna de la siguiente manera:

Hipótesis Nula (H0): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **no produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Hipótesis Alterna (H1): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Aplicación de prueba de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
Número de información divulgada- POST - Número de información divulgada - PRE	Rangos negativos	842[a]	449,00	378058,00
	Rangos positivos	55[b]	449,00	24695,00
	Empates	103[c]		
	Total	1000		

a. Número de información divulgada- POST < Número de información divulgada - PRE

b. Número de información divulgada- POST > Número de información divulgada - PRE

c. Número de información divulgada- POST = Número de información divulgada - PRE

Estadísticos de contraste[a]

	Número de información divulgada- POST - Número de información divulgada - PRE
Z	-26,277[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos positivos.

Tabla 10 Aplicación de Prueba No Paramétrica de Wilcoxon del número de información divulgada

Siendo el valor de Sig. (bilateral) 0 que es menor que 0.05, desechan la hipótesis nula y se aprueba la hipótesis alterna que es La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

A continuación, se realizó el análisis descriptivo del indicador accesos no autorizados de la dimensión confidencialidad, de la variable seguridad de la información.

Análisis Descriptivo

Cálculo de Datos Descriptivos

Estadísticos

		Accesos no autorizados - PRE	Accesos no autorizados - POST	DiferenciaAccesos
N	Válidos	1000	999	999
	Perdidos	0	1	1
Media		,84	,05	,7888
Desv. típ.		,365	,226	,52439
Varianza		,133	,051	,275
Mínimo		0	0	-1,00
Máximo		1	1	1,00

Tabla 11 Cálculo de Datos Estadísticos Descriptivos de los accesos no autorizados

Tablas de Frecuencia

Accesos no autorizados - PRE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	158	15,8	15,8	15,8
	SI	842	84,2	84,2	100,0
	Total	1000	100,0	100,0	

Tabla 12 Tabla de Frecuencia Pre test de los accesos no autorizados

Accesos no autorizados - POST

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	945	94,5	94,6	94,6
	SI	54	5,4	5,4	100,0
	Total	999	99,9	100,0	
Perdidos	Sistema	1	,1		
Total		1000	100,0		

Tabla 13 Tabla de Frecuencia Post test de los accesos no autorizados

Histograma

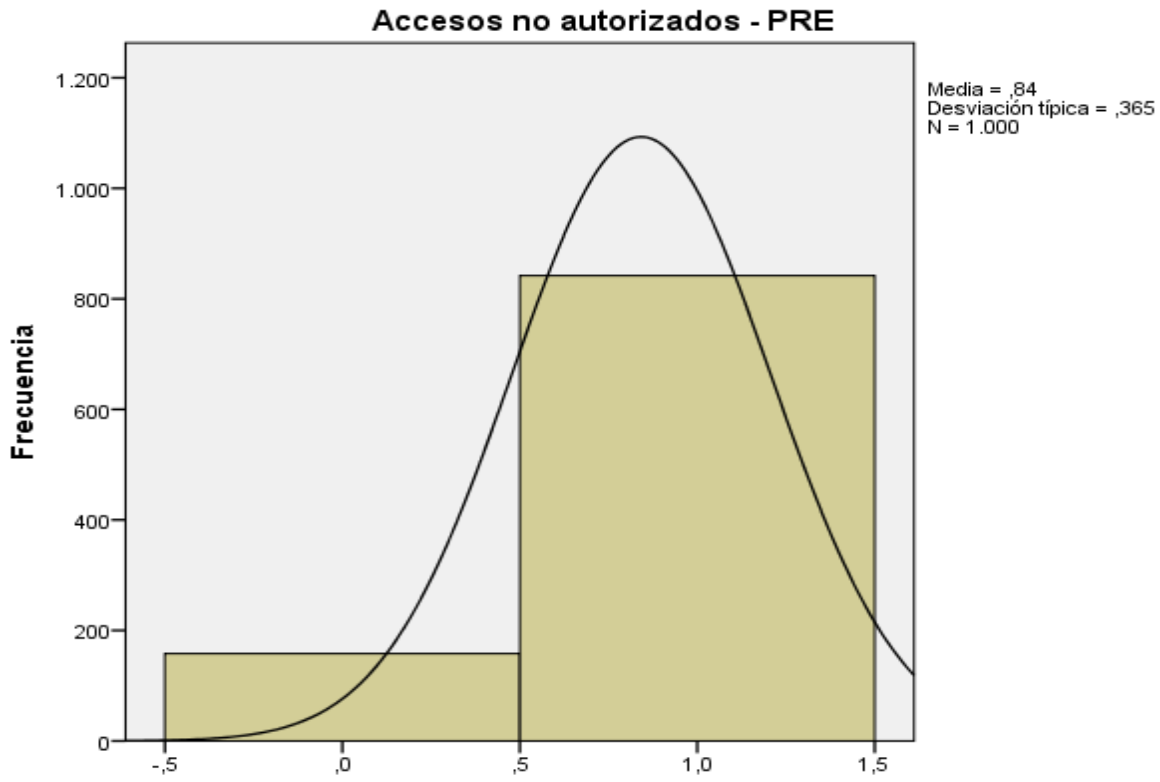


Figura 7 Gráfico de puntajes obtenidos en el Pre test de los accesos no autorizados

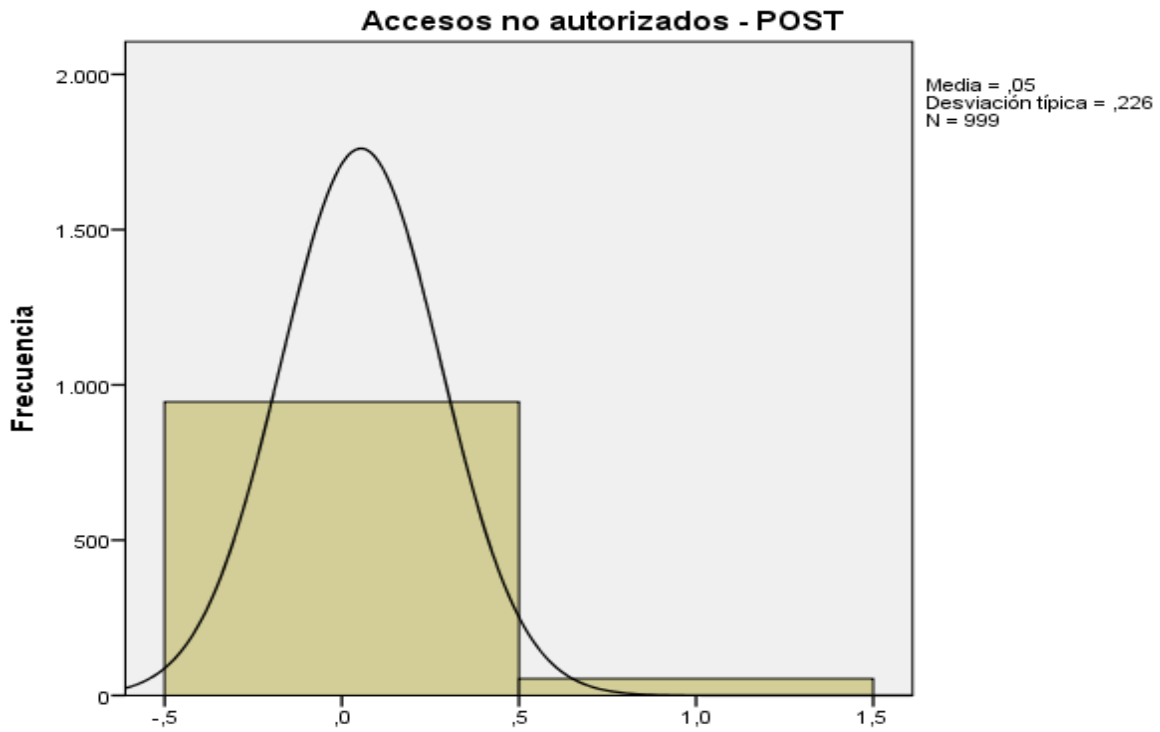


Figura 8 Gráfico de puntajes obtenidos en el Post test de los accesos no autorizados

El resultado obtenido en el análisis del pre test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.84 en los resultados de los accesos no autorizados, con una desviación estándar de 0.365.

El resultado obtenido en el análisis del post test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.05 en los resultados de la gestión de claves, con una desviación estándar de 0.226.

Análisis Inferencial

Prueba de Normalidad

A continuación, aplicamos la Prueba de Kolmogoroc – Smirnov para determinar si una muestra es normal o no.

Prueba de Kolmogorov-Smirnov para una muestra

		Accesos no autorizados - PRE	Accesos no autorizados - POST	DiferenciaAccesos
N		1000	999	999
Parámetros normales[a,b]	Media	,84	,05	,7888
	Desviación típica	,365	,226	,52439
Diferencias más extremas	Absoluta	,509	,540	,499
	Positiva	,333	,540	,344
	Negativa	-,509	-,406	-,499
Z de Kolmogorov-Smirnov		16,111	17,079	15,781
Sig. asintót. (bilateral)		,000	,000	,000

a. La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

Tabla 14 Prueba de Kolmogorov – Smirnov de los accesos no autorizados

Como podemos observar, la tabla muestra que en la columna Diferencia la Significancia(Sig.) tiene un valor menor a 0.05 lo cual nos asegurar que la distribución del indicador es no normal.

Prueba de Hipótesis

Al tener la muestra una distribución no normal, utilizan la Prueba Estadística No Paramétrica, aplicando la prueba de rangos de Wilcoxon la cual nos da la hipótesis nula y alterna de la siguiente manera:

Hipótesis Nula (H0): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **no produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Hipótesis Alterna (H1): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Aplicación de prueba de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
Accesos no autorizados - POST - Accesos no autorizados - PRE	Rangos negativos	842[a]	448,50	377637,00
	Rangos positivos	54[b]	448,50	24219,00
	Empates	103[c]		
	Total	999		

a. Accesos no autorizados - POST < Accesos no autorizados - PRE

b. Accesos no autorizados - POST > Accesos no autorizados - PRE

c. Accesos no autorizados - POST = Accesos no autorizados - PRE

Estadísticos de contraste[a]

	Accesos no autorizados - POST - Accesos no autorizados - PRE
Z	-26,325[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos positivos.

Tabla 15 Aplicación de Prueba No Paramétrica de Wilcoxon de los accesos no autorizados

Siendo el valor de Sig. (bilateral) 0 que es menor que 0.05, desechan la hipótesis nula y se aprueba la hipótesis alterna que es La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la confidencialidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

A continuación, se realizó el análisis descriptivo del indicador número de cambios no autorizados a los datos de producción de la dimensión integridad, de la variable seguridad de la información.

Análisis Descriptivo

Cálculo de Datos Descriptivos

Estadísticos

		Número de cambios no autorizados a los datos de producción - PRE	Número de cambios no autorizados a los datos de producción - POST	DiferenciaCambios
N	Válidos	999	999	999
	Perdidos	1	1	1
Media		,84	,05	,7888
Desv. típ.		,364	,226	,52439
Varianza		,133	,051	,275
Mínimo		0	0	-1,00
Máximo		1	1	1,00

Tabla 16 Cálculo Estadísticos Descriptivos del número de cambios no autorizados a los datos de producción

Tablas de Frecuencia

Número de cambios no autorizados a los datos de producción - PRE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	157	15,7	15,7	15,7
	SI	842	84,2	84,3	100,0
	Total	999	99,9	100,0	
Perdidos	Sistema	1	,1		
Total		1000	100,0		

Tabla 17 Tabla de Frecuencia Pre test del número de cambios no autorizados a los datos de producción

Número de cambios no autorizados a los datos de producción - POST

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	945	94,5	94,6	94,6
	SI	54	5,4	5,4	100,0
	Total	999	99,9	100,0	
Perdidos	Sistema	1	,1		
Total		1000	100,0		

Tabla 18 Tabla de Frecuencia Post test del número de cambios no autorizados a los datos de producción

Histograma

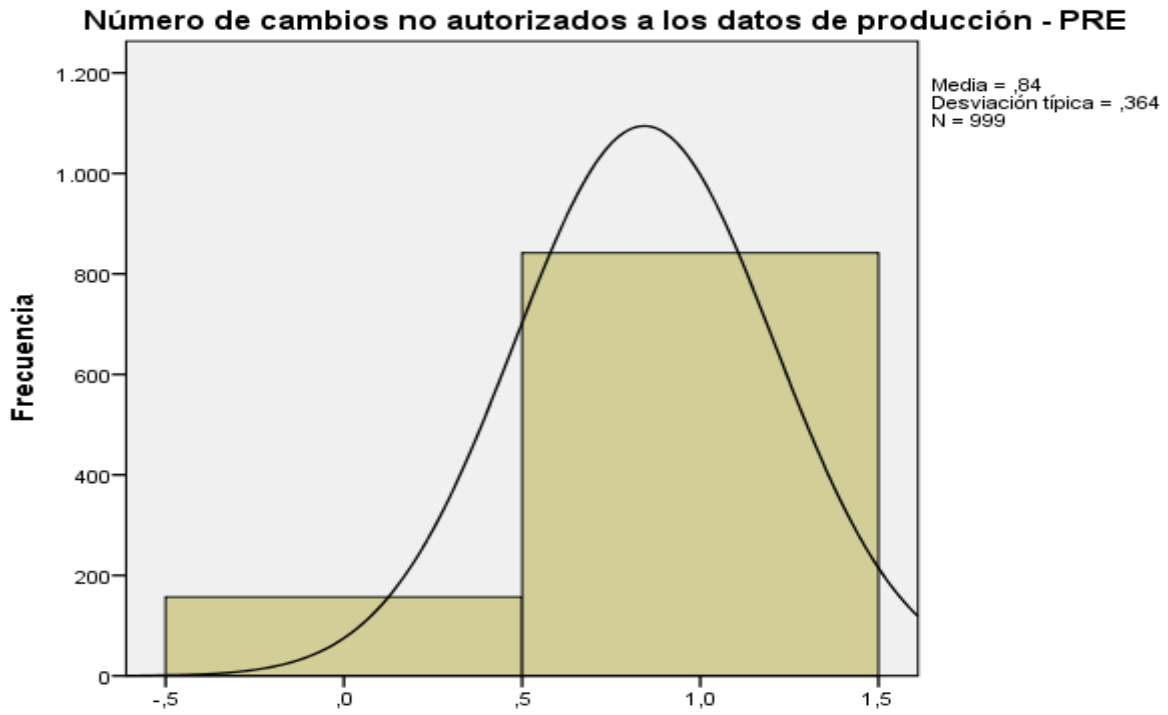


Figura 9 Gráfico de puntajes obtenidos en el Pre test del número de cambios no autorizados a los datos de producción

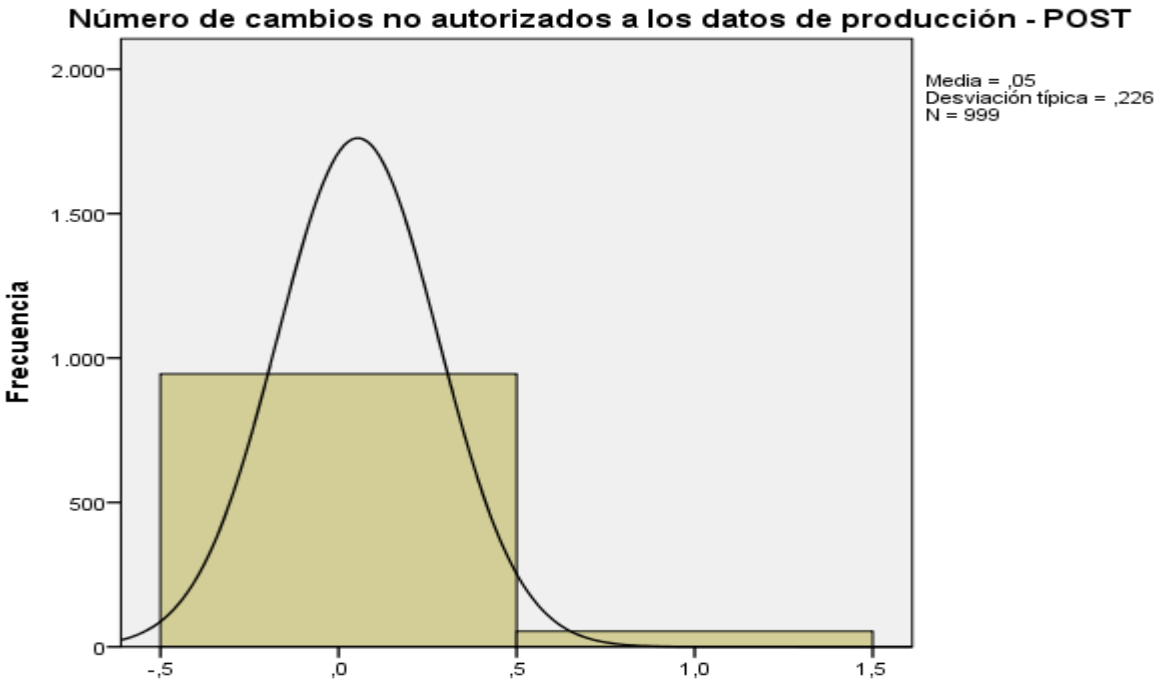


Figura 10 Gráfico de puntajes obtenidos en el Post test del número de cambios no autorizados a los datos de producción

El resultado obtenido en el análisis del pre test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de

0.84 en los resultados número de cambios no autorizados a los datos de producción, con una desviación estándar de 0.364.

El resultado obtenido en el análisis del post test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.05 en los resultados de la gestión de claves, con una desviación estándar de 0.226.

Análisis Inferencial

Prueba de Normalidad

A continuación, aplicamos la Prueba de Kolmogoroc – Smirnov para determinar si una muestra es normal o no.

Prueba de Kolmogorov-Smirnov para una muestra

		Número de cambios no autorizados a los datos de producción - PRE	Número de cambios no autorizados a los datos de producción - POST	DiferenciaCambios
N		999	999	999
Parámetros normales[a,b]	Media	,84	,05	,7888
	Desviación típica	,364	,226	,52439
Diferencias más extremas	Absoluta	,510	,540	,499
	Positiva	,333	,540	,344
	Negativa	-,510	-,406	-,499
Z de Kolmogorov-Smirnov		16,114	17,079	15,781
Sig. asintót. (bilateral)		,000	,000	,000

a. La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

Tabla 19 Prueba de Kolmogorov – Smirnov del número de cambios no autorizados a los datos de producción

Como podemos observar, la tabla muestra que en la columna Diferencia la Significancia(Sig.) tiene un valor menor a 0.05 lo cual nos permite asegurar que la distribución del indicador es no normal.

Prueba de Hipótesis

Al tener la muestra una distribución no normal, utilizan la Prueba Estadística No Paramétrica, aplicando la prueba de rangos de Wilcoxon la cual nos da la hipótesis nula y alterna de la siguiente manera:

Hipótesis Nula (H0): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **no produce un efecto positivo en la integridad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Hipótesis Alterna (H1): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la integridad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Aplicación de prueba de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
Número de cambios no autorizados a los datos de producción - POST - Número de cambios no autorizados a los datos de producción - PRE	Rangos negativos	842[a]	448,50	377637,00
	Rangos positivos	54[b]	448,50	24219,00
	Empates	103[c]		
	Total	999		

a. Número de cambios no autorizados a los datos de producción - POST < Número de cambios no autorizados a los datos de producción - PRE

b. Número de cambios no autorizados a los datos de producción - POST > Número de cambios no autorizados a los datos de producción - PRE

c. Número de cambios no autorizados a los datos de producción - POST = Número de cambios no autorizados a los datos de producción - PRE

Estadísticos de contraste[a]

	Número de cambios no autorizados a los datos de producción - POST - Número de cambios no autorizados a los datos de producción - PRE
Z	-26,325[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos positivos.

Tabla 20 Aplicación de Prueba No Paramétrica de Wilcoxon del número de cambios no autorizados en los datos de producción

Siendo el valor de Sig. (bilateral) 0 que es menor que 0.05, desechan la hipótesis nula y se aprueba la hipótesis alterna que es La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la integridad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

A continuación, se realizó el análisis descriptivo del indicador número de virus informáticos de la dimensión integridad de la variable seguridad de la información.

Análisis Descriptivo

Cálculo de Datos Descriptivos

Estadísticos

		Número de virus informáticos - PRE	Número de virus informáticos - POST	DiferenciaVirus
N	Válidos	999	999	999
	Perdidos	1	1	1
Media		,84	,14	,7007
Desv. típ.		,364	,349	,70321
Varianza		,133	,122	,494
Mínimo		0	0	-1,00
Máximo		1	1	1,00

Tabla 21 Cálculo de Datos Descriptivos del número de virus informáticos

Tablas de Frecuencia

Número de virus informáticos - PRE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	157	15,7	15,7	15,7
	SI	842	84,2	84,3	100,0
	Total	999	99,9	100,0	
Perdidos	Sistema	1	,1		
Total		1000	100,0		

Tabla 22 Tabla de Frecuencia Pre test del número de virus informáticos

Número de virus informáticos - POST

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	857	85,7	85,8	85,8
	SI	142	14,2	14,2	100,0
	Total	999	99,9	100,0	
Perdidos	Sistema	1	,1		
Total		1000	100,0		

Tabla 23 Tabla de Frecuencia Post test del número de virus informáticos

Histograma

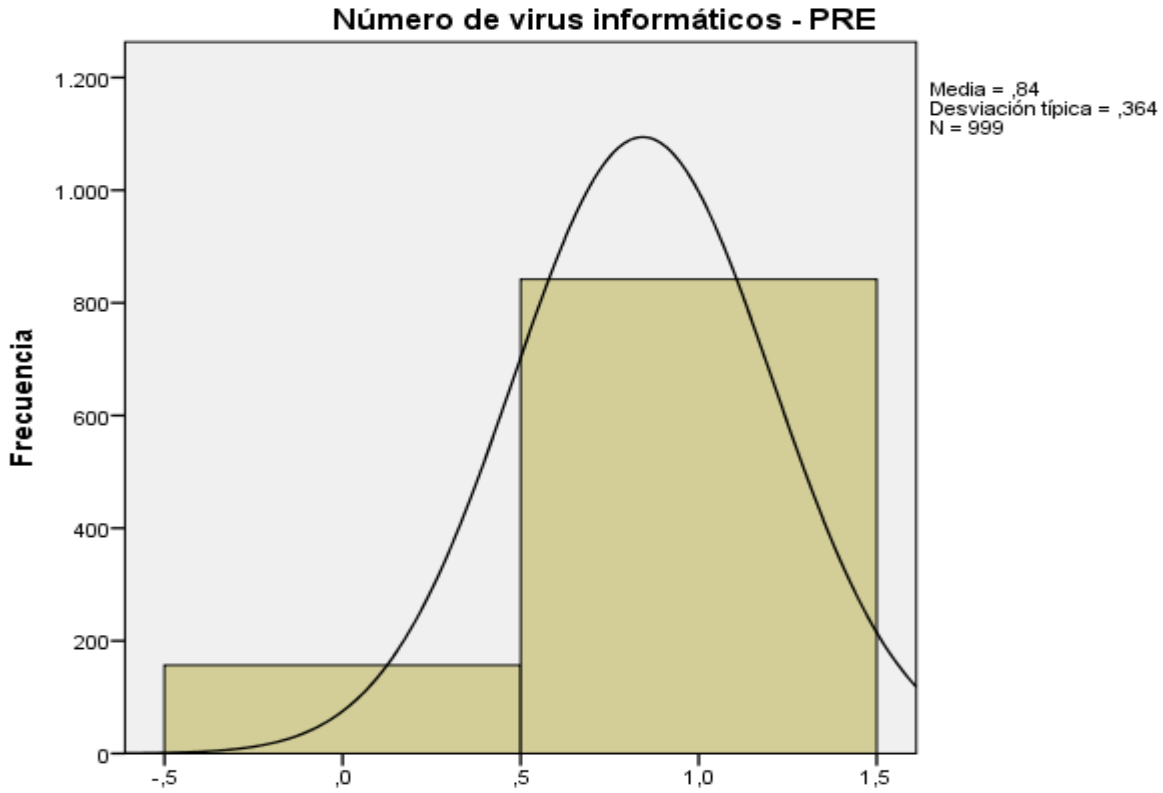


Figura 11 Gráfico de puntajes obtenidos en el Pre test del número de virus informáticos

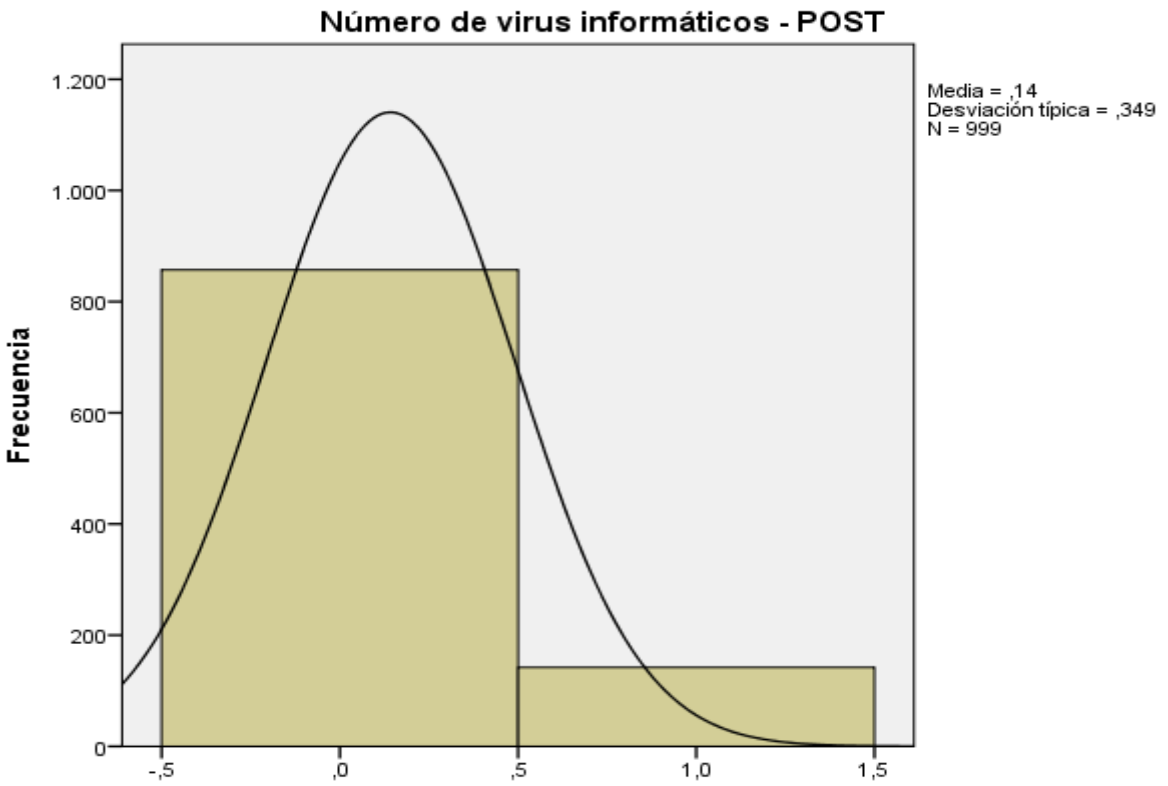


Figura 12 Gráfico de puntajes obtenidos en el Post test del número de virus informáticos

El resultado obtenido en el análisis del pre test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.84 en los resultados de la gestión de claves, con una desviación estándar de 0.364.

El resultado obtenido en el análisis del post test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.14 en los resultados de la gestión de claves, con una desviación estándar de 0.349.

Análisis Inferencial

Prueba de Normalidad

A continuación, aplicamos la Prueba de Kolmogoroc – Smirnov para determinar si una muestra es normal o no.

Prueba de Kolmogorov-Smirnov para una muestra

		Número de virus informáticos - PRE	Número de virus informáticos - POST	DiferenciaVirus
N		999	999	999
Parámetros normales[a,b]	Media	,84	,14	,7007
	Desviación típica	,364	,349	,70321
Diferencias más extremas	Absoluta	,510	,516	,508
	Positiva	,333	,516	,335
	Negativa	-,510	-,342	-,508
Z de Kolmogorov-Smirnov		16,114	16,303	16,045
Sig. asintót. (bilateral)		,000	,000	,000

a. La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

Tabla 24 Prueba de Kolmogorov – Smirnov del número de virus informáticos

Como podemos observar, la tabla muestra que en la columna Diferencia la Significancia(Sig.) tiene un valor menor a 0.05 lo cual nos permite asegurar que la distribución del indicador es no normal.

Prueba de Hipótesis

Al tener la muestra una distribución no normal, utilizan la Prueba Estadística No Paramétrica, aplicando la prueba de rangos de Wilcoxon la cual nos da la hipótesis nula y alterna de la siguiente manera:

Hipótesis Nula (H0): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **no produce un efecto positivo en la integridad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Hipótesis Alterna (H1): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la integridad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Aplicación de prueba de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
Número de virus informáticos - POST - Número de virus informáticos - PRE	Rangos negativos	842[a]	492,50	414685,00
	Rangos positivos	142[b]	492,50	69935,00
	Empates	15[c]		
	Total	999		

a. Número de virus informáticos - POST < Número de virus informáticos - PRE

b. Número de virus informáticos - POST > Número de virus informáticos - PRE

c. Número de virus informáticos - POST = Número de virus informáticos - PRE

Estadísticos de contraste[a]

	Número de virus informáticos - POST - Número de virus informáticos - PRE
Z	-22,315[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos positivos.

Tabla 25 Aplicación de Prueba No Paramétrica de Wilcoxon del número de virus informáticos

Siendo el valor de Sig. (bilateral) 0 que es menor que 0.05, desechan la hipótesis nula y se aprueba la hipótesis alterna que es La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la disponibilidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

A continuación, se realizó el análisis descriptivo del indicador tiempo disponible del sistema para el usuario de la dimensión disponibilidad, de la variable seguridad de la información.

Análisis Descriptivo

Cálculo de Dataos Descriptivos

Estadísticos

		Tiempo disponible del sistema para el usuario - PRE	Tiempo disponible del sistema para el usuario - POST	DiferenciaTiempo
N	Válidos	999	999	999
	Perdidos	1	1	1
Media		,16	,86	-,7007
Desv. típ.		,364	,349	,70321
Varianza		,133	,122	,494
Mínimo		0	0	-1,00
Máximo		1	1	1,00

Tabla 26 Cálculos Estadísticos Descriptivos del tiempo disponible del sistema para el usuario

Tablas de Frecuencia

Tiempo disponible del sistema para el usuario - PRE

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	842	84,2	84,3	84,3
	SI	157	15,7	15,7	100,0
	Total	999	99,9	100,0	
Perdidos	Sistema	1	,1		
Total		1000	100,0		

Tabla 27 Tabla de Frecuencia Pre test del tiempo disponible del sistema para el usuario

Tiempo disponible del sistema para el usuario - POST

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	142	14,2	14,2	14,2
	SI	857	85,7	85,8	100,0
	Total	999	99,9	100,0	
Perdidos	Sistema	1	,1		
Total		1000	100,0		

Tabla 28 Tabla de Frecuencia Post test del tiempo disponible del sistema para el usuario

Histograma

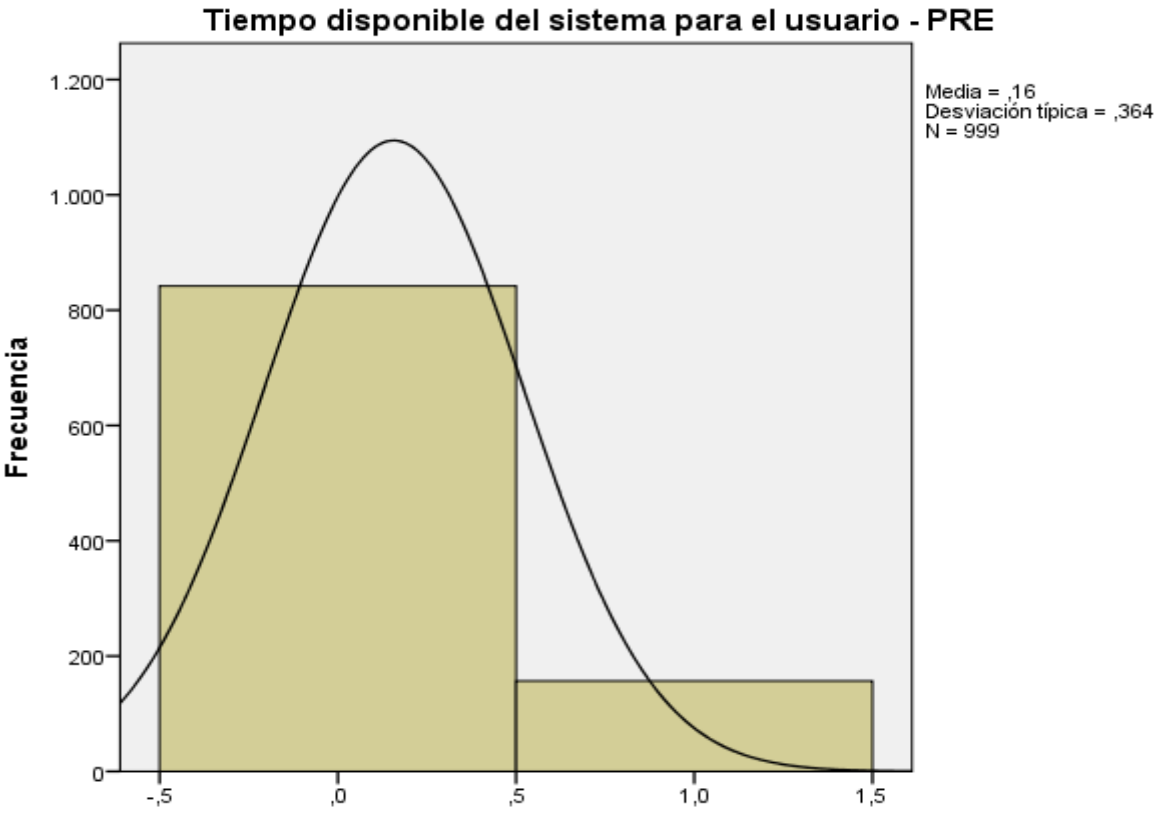


Figura 13 Gráfico de puntaje obtenido en el Pre test del tiempo disponible del sistema para el usuario

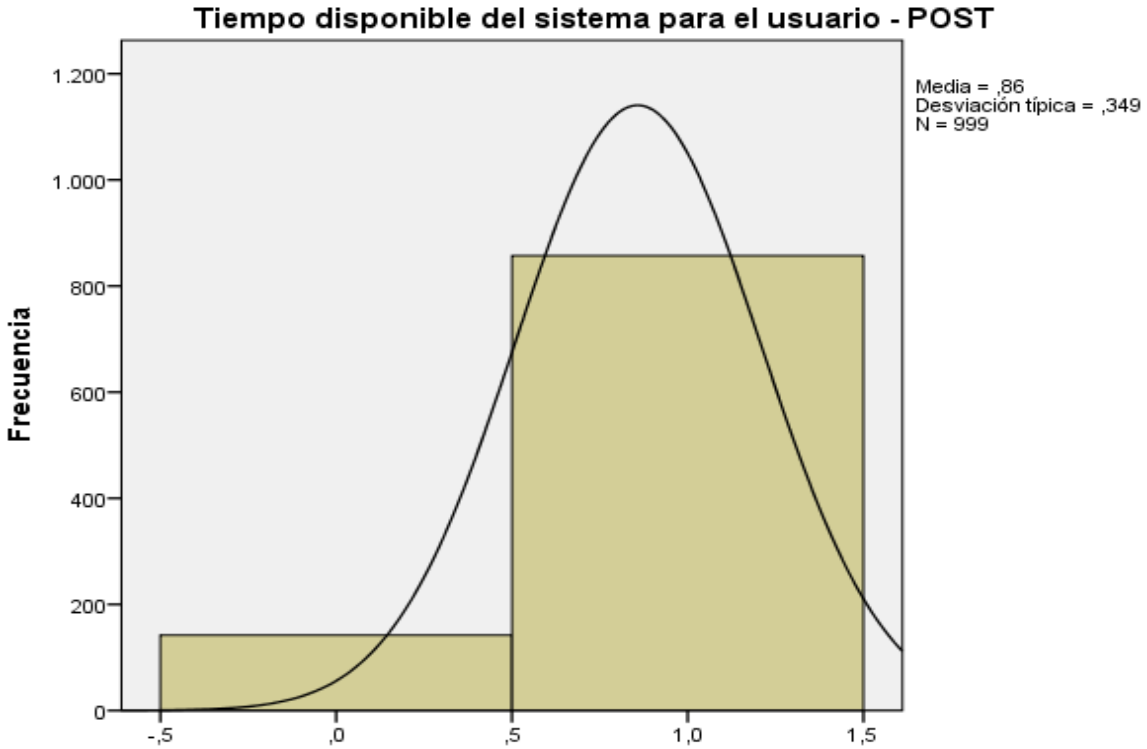


Figura 14 Gráfico de puntaje obtenido en el Post test del tiempo disponible del sistema para el usuario

El resultado obtenido en el análisis del pre test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.16 en los resultados de la gestión de claves, con una desviación estándar de 0.364.

El resultado obtenido en el análisis del post test en el cálculo de datos descriptivos podemos observar que el resultado obtenido por el indicador tiene una media de 0.86 en los resultados de la gestión de claves, con una desviación estándar de 0.349.

Análisis Inferencial

Prueba de Normalidad

A continuación, aplicamos la Prueba de Kolmogoroc – Smirnov para determinar si una muestra es normal o no.

Prueba de Kolmogorov-Smirnov para una muestra

		Tiempo disponible del sistema para el usuario - PRE	Tiempo disponible del sistema para el usuario - POST	DiferenciaTiempo
N		999	999	999
Parámetros normales[a,b]	Media	,16	,86	-,7007
	Desviación típica	,364	,349	,70321
Diferencias más extremas	Absoluta	,510	,516	,508
	Positiva	,510	,342	,508
	Negativa	-,333	-,516	-,335
Z de Kolmogorov-Smirnov		16,114	16,303	16,045
Sig. asintót. (bilateral)		,000	,000	,000

a. La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

Tabla 29 Prueba de Kolmogorov – Smirnov del tiempo disponible del sistema para el usuario

Como podemos observar, la tabla muestra que en la columna Diferencia la Significancia(Sig.) tiene un valor menor a 0.05 lo cual nos permite asegurar que la distribución del indicador es no normal.

Prueba de Hipótesis

Al tener la muestra una distribución no normal, utilizan la Prueba Estadística No Paramétrica, aplicando la prueba de rangos de Wilcoxon la cual nos da la hipótesis nula y alterna de la siguiente manera:

Hipótesis Nula (H0): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **no produce un efecto positivo en la disponibilidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Hipótesis Alterna (H1): La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la disponibilidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

Aplicación de prueba de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
Tiempo disponible del sistema para el usuario - POST - Tiempo disponible del sistema para el usuario - PRE	Rangos negativos	142[a]	492,50	69935,00
	Rangos positivos	842[b]	492,50	414685,00
	Empates	15[c]		
	Total	999		

a. Tiempo disponible del sistema para el usuario - POST < Tiempo disponible del sistema para el usuario - PRE

b. Tiempo disponible del sistema para el usuario - POST > Tiempo disponible del sistema para el usuario - PRE

c. Tiempo disponible del sistema para el usuario - POST = Tiempo disponible del sistema para el usuario - PRE

Estadísticos de contraste[a]

	Tiempo disponible del sistema para el usuario - POST - Tiempo disponible del sistema para el usuario - PRE
Z	-22,315[b]
Sig. asintót. (bilateral)	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Tabla 30 Aplicación de Prueba No Paramétrica de Wilcoxon del tiempo disponible del sistema para el usuario

Siendo el valor de Sig. (bilateral) 0 que es menor que 0.05, desechan la hipótesis nula y se aprueba la hipótesis alterna que es La automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo en la disponibilidad** de la empresa ZEPPELIN Inversiones Generales S.R.L.

V. DISCUSIÓN

Este capítulo presenta la discusión, aquí comparan los resultados conseguidos para comprobar la hipótesis general y específicas. Detallando cada resultado alcanzado con la investigación, analizando y comparando cómo se comporta la media de los indicadores de la confidencialidad, integridad y disponibilidad, antes y después de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001.

Podemos observar que el indicador de gestión de claves que pertenece a la hipótesis especifica número 1 en el pre test obtuvo un 15.8% en equipos que si tenían una gestión de claves y un 84.2% no tenían una gestión de claves y después de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en el post test obtuvo un 94.5% en equipos que si contaban con gestión de claves y un 5.5% en equipos que no contaba con la gestión de claves, con lo que se puede afirmar que se incrementó un 78.7% en los equipos que si contaban con gestión de claves, anulando la hipótesis nula y concluyendo que la automatización de la seguridad de la información basada en la ISO 27001 produce un efecto positivo en la confidencialidad de la empresa Zeppelin inversiones generales S.R.L.

Podemos observar que en el indicador de número de información divulgada que pertenece a la hipótesis especifica número 1 en el pre test obtuvo un 84.2 % en equipos que contaban con un número de información divulgada y un 15.8% en equipos que no contaban con un número de información divulgada y al realizar la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en el post test obtuvo un 5.5% en equipos que contaban con un número de información divulgada y un 94.5% en equipos que no contaban con un número de información divulgada, con lo que se puede afirmar que se redujo un 78.7% en equipos que contaban con un número de información divulgada, anulando la hipótesis nula y concluyendo que la automatización de la seguridad de la información basada en la ISO 27001 produce un efecto positivo en la confidencialidad de la empresa Zeppelin inversiones generales S.R.L.

Podemos observar que en el indicador de accesos no autorizados que pertenece a la hipótesis especifica número 1 en el pre test obtuvo un 84.2% en equipos que contaban con accesos no autorizados y un 15.8% en equipos que no contaban con

accesos no autorizados y después de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en el post test obtuvo un 5.4% en equipos que contaban con accesos no autorizados y un 94.5% en equipos que no contaban con accesos no autorizados, con lo que se puede afirmar que se redujo un 78.8% en equipos que contaban con accesos no autorizados, anulando la hipótesis nula y concluyendo que la automatización de la seguridad de la información basada en la ISO 27001 produce un efecto positivo en la confidencialidad de la empresa Zeppelin inversiones generales S.R.L.

Podemos observar que en el indicador de número de cambios no autorizados a los datos de producción que pertenece a la hipótesis especifica número 2 en el pre test obtuvo un 84.2 % en equipos que contaban con un número de cambios no autorizados a los datos de producción y un 15.7% en equipos que no contaban con un número de cambios no autorizados a los datos de producción y al realizar la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en el post test obtuvo un 5.4% en equipos que contaban con un número de cambios no autorizados a los datos de producción y un 94.5% en equipos que no contaban con un número de cambios no autorizados a los datos de producción, con lo que se puede afirmar que se redujo un 78.8% en equipos que contaban con un número de cambios no autorizados a los datos de producción, anulando la hipótesis nula y concluyendo que la automatización de la seguridad de la información basada en la ISO 27001 produce un efecto positivo en la integridad de la empresa Zeppelin inversiones generales S.R.L.

Podemos observar que en el indicador de número de virus informáticos que pertenece a la hipótesis especifica número 2 en el pre test obtuvo un 84.2 % en equipos que contaban con un número de virus informáticos y un 15.7% en equipos que no contaban con número de virus informáticos y después de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en el post test obtuvo un 14.2% en equipos que contaban con un número de virus informáticos y un 85.7% en equipos que no contaban con un número de virus informáticos, con lo que se puede afirmar que se redujo un 70% en equipos que contaban con un número de virus informáticos, anulando la hipótesis nula y concluyendo que la automatización de la seguridad de la información basada en la

ISO 27001 produce un efecto positivo en la integridad de la empresa Zeppelin inversiones generales S.R.L.

Podemos observar que en el indicador de tiempo disponible del sistema para el usuario que pertenece a la hipótesis especifica número 3 en el pre test obtuvo un 15.7% en equipos que contaban con un tiempo disponible del sistema para el usuario y un 84.2% en equipos que no contaban con un tiempo disponible del sistema para el usuario y después de la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en el post test obtuvo un 85.7% en equipos que contaban con un tiempo disponible del sistema para el usuario y un 14.2% en equipos que no contaban con un tiempo disponible del sistema para el usuario, con lo cual pueden asegurar que se incrementó un 70% en equipos que contaban con un tiempo disponible del sistema para el usuario, anulando la hipótesis nula y concluyendo que la automatización de la seguridad de la información basada en la ISO 27001 produce un efecto positivo en la disponibilidad de la empresa Zeppelin inversiones generales S.R.L.

Estas mejoras en los puntajes de los indicadores gracias a la implementación de la automatización de la seguridad de la información basada en la norma técnica peruana ISO 27001 reflejan la aceptación y mejora de este proceso, además, Ochoa, A. (2017) demostró que con el desarrollo de un SGSI web usando la ISO 27001 por computadora obtuvieron resultados positivos para el área de sistemas en una universidad ya que lograron implementar detalladamente los procesos y controles específicos para mejorar la SI.

Por tal motivo se concluye que la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 produce un efecto positivo en la empresa ZEPPELIN INVERSIONES GENERALES S.R.L.

VI. CONCLUSIONES

Las conclusiones obtenidas fueron:

El puntaje obtenido por la gestión de claves antes de la automatización de la seguridad de la información es de 15.8% y luego de la automatización de la seguridad de la información fue de 94.5%, lo cual indica un aumento del 78.7% entre las puntuaciones. Demostrando que la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo** en la confidencialidad de la empresa ZEPPELIN INVERSIONES GENERALES S.R.L.

El puntaje obtenido por el número de información divulgada antes de la automatización de la seguridad de la información es de 84.2% y luego de la automatización de la seguridad de la información fue de 5.5%, que representa una reducción del 78.7% entre ambos puntajes. Con ello se demostró que la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo** en la confidencialidad de la empresa ZEPPELIN INVERSIONES GENERALES S.R.L.

El puntaje obtenido por los accesos no autorizados antes de la automatización de la seguridad de la información es de 84.2% y luego de la automatización de la seguridad de la información fue de 5.4%, que representa una reducción del 78.8% entre ambos puntajes. Con ello se demostró que la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo** en la confidencialidad de la empresa ZEPPELIN INVERSIONES GENERALES S.R.L.

El puntaje obtenido por el número de cambios no autorizados a los datos de producción antes de la automatización de la seguridad de la información es de 84.2% y luego de la automatización de la seguridad de la información fue de 5.4%, que representa una reducción del 78.8% entre ambos puntajes. Con ello se demostró que la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo** en la integridad de la empresa ZEPPELIN INVERSIONES GENERALES S.R.L.

El puntaje obtenido por el número de virus informático de la automatización de la seguridad de la información es de 84.2% y luego de la automatización de la

seguridad de la información fue de 14.2%, que representa una reducción del 70% entre ambos puntajes. Con ello se demostró que la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo** en la integridad de la empresa ZEPPELIN INVERSIONES GENERALES S.R.L.

El puntaje obtenido por el tiempo disponible del sistema para el usuario antes de la automatización de la seguridad de la información es de 15.7% y luego de la automatización de la seguridad de la información fue de 85.7%, lo cual indica un aumento del 70% entre las puntuaciones. Demostrando que la automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 **produce un efecto positivo** en la disponibilidad de la empresa ZEPPELIN INVERSIONES GENERALES S.R.L.

VII. RECOMENDACIONES

Las recomendaciones para futuras investigaciones son las siguientes:

- Se recomienda aumentar el alcance de la automatización de la seguridad de la información, permitiendo realizar reportes del esta de los activos evaluados para un mejor análisis e implementación de los controles.
- Se recomienda aumentar el alcance de la automatización de la seguridad de la información, permitiendo brindar recomendaciones de cómo aplicar cada control evaluado.

REFERENCIAS

- ACHOUR, M., BETZ, F., DOVGAL, A., LÓPEZ, N., et al. Manual de PHP [en línea]. 2005. [Consulta: 15 de mayo de 2019]. Disponible en: http://www1.herrera.unt.edu.ar/biblcet/wp-content/uploads/2014/12/Manual-de-PHP-Oficial-21-02-2005-3214-paginas-espa%C3%B1ol-spanish.pdf
- Advisera. ¿Qué es norma ISO 27001? [en línea]. advisera.com. [Consulta: 10 de octubre de 2018]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/
- AGURTO, M. Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C. Talara, basado en la norma ISO 27001 [en línea]. Tesis de pre-grado. Universidad Cesar Vallejo, 2017. [Consulta: 12 de octubre de 2018]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/11917
- AGUILERA, L. Seguridad Informática [en línea]. Editex, 2017. [Consulta: 19 de mayo de 2019]. Disponible en: https://datospdf.com/download/seguridad-informatica-porcf-_5a4b933fb7d7bcb74fbb5de9_pdf
- ALCÁNTARA, J. Guía de Implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad del Chiclayo [en línea]. Tesis de Pre-Grado. Universidad Católica Santo Toribio De Mogrovejo, 2015. [Consulta: 12 de octubre de 2018]. Disponible en: https://tesis.usat.edu.pe/bitstream/20.500.12423/539/1/TL_Alcantara_Flores_JulioCesar.pdf
- AMPUERO, C. Diseño de un sistema de gestión de seguridad de información para una compañía de seguros [en línea]. Tesis de Pre-Grado. Pontificia Universidad Católica Del Perú, 2011. [Consulta: 15 de octubre de 2018]. Disponible en: https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/933/AMPUERO_CHANG_CARLOS_INFORMACION_COMPA%c3%91IA_SEGUROS.pdf?sequence=1&isAllowed=y
- ARIASCA, F. Y QUISPE, S. Desarrollo de una propuesta de implementación de la ntp iso/iec 27001 :2014, sistema de gestión de seguridad de la información, para la oficina funcional de informática del gobierno regional

Cusco [en línea]. Tesis de Pre-Grado. Universidad Nacional De San Antonio Abad Del Cusco, 2016. [Consulta: 15 de octubre de 2018]. Disponible en: http://repositorio.unsaac.edu.pe/bitstream/handle/20.500.12918/2454/253T20170100.pdf?sequence=1&isAllowed=y

- ÁVILA, J. Confidencialidad de la Informática [en línea]. incmnsz.mx, 2013. [Consulta: 5 de mayo de 2019]. Disponible en: http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html
- BACA, V. Diseño de un sistema de gestión de la seguridad de la información para la unidad de gestión educativa local – Chiclayo [en línea]. Unidad de Gestión Educativa Local – Chiclayo, 2016, **3**(1), pp.1-16. [Consulta: 10 de octubre de 2018]. ISSN 2313-1926. Disponible en: http://revistas.uss.edu.pe/index.php/ING/article/view/357/346
- BERRIO, J. Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001 [en línea]. Tesis de maestría. Universidad Nacional de Colombia, 2016. [Consulta: 10 de octubre de 2018]. Disponible en: https://repositorio.unal.edu.co/bitstream/handle/unal/59020/1128401087.2017.pdf?sequence=1&isAllowed=y
- BERNAL, J. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua [en línea]. Pdcahome.com, 2013. [Consulta: 19 de mayo de 2019]. Disponible en: https://www.pdcahome.com/5202/ciclo-pdca/
- BETANCUR S., GARCÍA H. Y LARGO J. Análisis y estructuración de un sistema de gestión de seguridad de la información basado en la norma iso 27001:2013 para el proceso de gestión administrativa en la gerencia de sistemas y tecnología de la fundación universitaria maría cano sede Medellín [en línea]. Fundación Universitaria María Cano, 2016. [Consulta: 10 de octubre de 2018]. Disponible en: https://www.researchgate.net/publication/315675292_ANALISIS_Y_ESTRUCTURACION_DE_UN_SISTEMA_DE_GESTION_DE_SEGURIDAD_DE_LA_INFORMACION_BASADO_EN_LA_NORMA_ISO_270012013_PARA_E

L_PROCESO_DE_GESTION_ADMINISTRATIVA_EN_LA_GERENCIA_DE_SISTEMAS_Y_TECNOLOGIA_DE_

- BERMÚDEZ, K. Y BAILÓN, E. Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001-Sistemas de Gestión de Seguridad de la información dirigido a una empresa de servicios financieros [en línea]. Tesis de pre-grado. Universidad Politécnico Salesiana Sede Guayaquil, 2015. [Consulta: 12 de octubre de 2018]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf
- CAMARGO, J. Diseño de un sistema de gestión de la seguridad de la información (SGSI) en el área tecnológica de la comisión nacional del servicio civil- CNSC basado en la norma ISO 27000 E ISO 27001 [en línea]. Tesis Pre-Grado. Universidad Nacional Abierta y a Distancia, 2017. [Consulta: 12 de octubre de 2018]. Disponible en: https://repository.unad.edu.co/bitstream/10596/11992/1/75104100.pdf
- CAMARGO, J. Diseño de un sistema de gestión de la seguridad de la información (sgsi) en el área tecnológica de la comisión nacional del servicio civil - cnsc basado en la norma iso27000 e iso27001 [en línea]. Tesis de pregrado. Universidad Nacional Abierta y a Distancia, 2017. [Consulta: 10 de octubre de 2018]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11992/1/75104100.pdf
- CCESA, M. Diseño de un sistema de gestión de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016 [en línea]. Tesis de Pre-Grado. Universidad Nacional De San Cristóbal De Huamanga, 2017. [Consulta: 15 de octubre de 2018]. Disponible en: http://repositorio.unsch.edu.pe/bitstream/handle/UNSCH/1751/TESIS%20SIS48_Cce.pdf?sequence=1&isAllowed=y
- CHEN, C. Significados de Sistemas de Información [en línea]. Significados.com, 2019. [Consulta: 19 de mayo de 2019]. Disponible en: https://www.significados.com/sistema-de-informacion/

- COMUNIDAD DE MADRID. Gestión de riesgos y análisis cuantitativa [en línea]. [Consulta: 5 de mayo de 2019]. Disponible en: http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo%28AR%29_es.pdf
- CONTRERAS, L. Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para la dirección de sistemas de la gobernación de Boyacá [en línea]. Tesis de pregrado. Universidad Nacional Abierta y a Distancia, 2017. [Consulta: 10 de octubre de 2018]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11895/33367604.pdf?sequence=1&isAllowed=y
- CUEVA, P. Y RÍOS, J. Gestión de la historia clínica y seguridad de la información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014 en la universidad Privada del Norte [en línea]. Tesis de Maestría. Universidad Privada del Norte, 2017. [Consulta: 12 de octubre de 2018]. Disponible en: http://repositorio.upn.edu.pe/bitstream/handle/11537/13676/Cueva%20Araujo%20Paul%20Omar%20-%20R%C3%ADos%20Mercado%20Juan%20Antonio.pdf?sequence=1&isAllowed=y
- CHIPULINA, L. Sistema web para la gestión de incidencias en la empresa consulit S.A.C. [en línea]. Tesis de pre-grado. Universidad Cesar Vallejo, 2018. [Consulta: 15 de octubre de 2018]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/21275
- COBARSÍ, J. Gestión de información en organizaciones 2012: perspectivas y tendencias [en línea].2012. [Consulta: 15 de octubre de 2018]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4234698.pdf
- DEPARTAMENTO DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y DE CONTROL. Funciones básicas, características y arquitectura de los sistemas automatizados [en línea]. PAC- Performance-centered Adaptive Curriculum. [Consulta: 10 de mayo de 2019]. Disponible en: http://www.ieec.uned.es/investigacion/Dipseil/PAC/archivos/Informacion_de_referencia_ISE2_1_1.pdf

- DE LA CRUZ, R. Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016 [en línea]. Tesis de pre-grado. Universidad Católica Los Ángeles Chimbote, 2016. [Consulta: 15 de octubre de 2018]. Disponible en: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/885/ACTIVO_SEGURIDAD%20DE%20LA%20INFORMACION_DE%20LA%20CRUZ_VARGAS_RONALD%20_EDUARDO%20.pdf?sequence=1&isAllowed=y
- DÍAZ, M. Propuesta para mejorar la seguridad de la información con base en las TI en la empresa “CARE ENTERPRISE NETWORK” [en línea]. Tesis de maestría. Instituto Politécnico Nacional, 2016. [Consulta: 10 de octubre de 2018]. Disponible en: https://tesis.ipn.mx/bitstream/handle/123456789/24016/MAN2016%20D535m%20Mois%C3%A9s%20D%C3%ADaz%20D%C3%ADaz.pdf?sequence=1&isAllowed=y
- DORIA, A. Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de Córdoba [en línea]. Tesis de pregrado. Universidad Nacional Abierta y a Distancia, 2015. [Consulta: 10 de mayo de 2018]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/3624/1067846426.pdf?sequence=1&isAllowed=y
- ESPINOSA J., GARCÍA R. Y GIRALDO A. Sistema de gestión de seguridad de la información para los tres procesos misionales de la corporación autónoma regional de Risaralda (CARDER) [en línea]. Tesis de maestría. Universidad Autónoma de Manizales, 2016. [Consulta: 10 de octubre de 2018]. Disponible en: http://repositorio.autonoma.edu.co/jspui/bitstream/11182/656/1/Sistema_gesti%c3%b3n_seguridad_informaci%c3%b3n_tres_procesos_misionales_Corporaci%c3%b3n_Aut%c3%b3noma_Regional_Risaralda_CARDER.pdf
- ENCALA, R. Y QUISPE, J. Sistema experto en auditoria de seguridad de la información basado en las NTP ISO 27001 y 27002 y cobit [en línea]. Tesis Pre-Grado. Universidad Privada Antenor Orrego, 2017. [Consulta: 12 de octubre de 2018]. Disponible en: https://hdl.handle.net/20.500.12759/2816

- ESPINOZA, H. Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo [en línea]. Pontificia Universidad Católica Del Perú, 2013. [Consulta: 15 de octubre de 2018]. Disponible en: https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/4957/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC%2027001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf?sequence=1&isAllowed=y
- FERNÁNDEZ, D. Modelo de Gestión de riesgos de TI de acuerdo con las exigencias de la sbs, basados en las ISO/IEC 27001, ISO/IEC 17799, Magerit para la caja de ahorro y crédito sipan SA. [en línea]. Tesis de Pre-grado. Universidad Católica Santo Toribio De Mogrovejo, 2015. [Consulta: 12 de octubre de 2018]. Disponible en: http://tesis.usat.edu.pe/xmlui/bitstream/handle/20.500.12423/540/TL_FernandezFernandezDamaris.pdf?sequence=1&isAllowed=y
- FIUBA. Automatización [en línea]. [Consulta: 10 de mayo de 2019]. Disponible en: http://materias.fi.uba.ar/7566/Automatizacion.pdf
- GOMES, A. Y SUÁREZ, C. Sistemas de Información. Herramientas prácticas para la gestión. 3ª. Ed. MEXICO: Alfa y Omega Grupo Editor, 2011. ISBN: 978-607-7854-45-6
- GONZALES, A. Y MARAÑÓN, P. Seguridad Informática para la empresa y particulares. España: S.A McGraw-Hill/Interamericana de España, 2004. ISBM: 9788448140083
- GONZALES, I. Diseño e implementación de controles de seguridad para las comunicaciones de red en un centro de datos de una entidad del estado basado en la NTP-ISO/IEC 27001:2014 [en línea]. Tesis Pre-Grado. Universidad Tecnológica del Perú, 2017. [Consulta: 12 de octubre de 2018]. Disponible en: https://repositorio.utp.edu.pe/handle/20.500.12867/914
- GUTIÉRREZ, A. Base de Datos [en línea]. 2013. [Consulta: 9 de mayo de 2019]. Disponible en: https://aiu.edu/cursos/base%20de%20datos/pdf%20leccion%201/lecci%C3%B3n%201.pdf

- GUTIÉRREZ, C., BAEZA YATES, R., PIQUER GARDNER, J., NAVARRO, G., MARÍN, M., ARENAS, M., RODRÍGUEZ TASTETS, A., RUIZ DEL SOLAR, J., VELASCO, J. Y HURTADO LARRAÍN, C. Como funciona una web [en línea]. 1a. Ed. Santiago de Chile: Gutiérrez, C. 2008. [Consulta: 20 de mayo del 2019]. ISBN: 978-956-319-225-1 (Online). Disponible en: https://www.alejandrobarros.com/wp-content/uploads/old/libroWeb-NV.pdf
- ISOTools Excellence. La norma ISO 27001: Aspectos claves de su diseño e implantación [en línea]. [Consulta: 5 de mayo de 2019]. Disponible en: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf
- Iubaris Info 4 Media SL. Scrum manager [en línea].2016. [Consulta: 5 de mayo de 2019]. Disponible en: https://www.scrummanager.net/files/sm_proyecto.pdf
- Lenguaje de Programación (informática) [en línea]. ecured.cu. [Consulta: 10 de mayo de 2019]. Disponible en: https://www.ecured.cu/Lenguaje_de_programaci%C3%B3n_(inform%C3%A1tica)
- LLONTOP, G. Gestión de riesgo de Tecnologías de Información de las empresas de Nephila Networks [en línea]. Tesis de post-grado. Universidad Cesar Vallejo, 2018. [Consulta: 12 de octubre de 2018]. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/17596
- MARTÍNEZ, A. Manual Práctico de HTML [en línea]. Madrid, España, 1995. [Consulta: el 5 de mayo de 2019]. Disponible en: http://bioinf.ibun.unal.edu.co/servicios/electiva/manhtlm/HTML.pdf
- MANTILLA GUERRA, A. Diseño de un sistema de gestión de seguridad de la información para Cooperativas de Ahorro y Crédito en base a la norma ISO 27001 [en línea]. Tesis de Post-Grado. Escuela Politécnica Nacional, 2009. [Consulta: 15 de octubre de 2018]. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/8108/1/CD-2254.pdf
- MAUREIRA, D. Norma ISO/IEC 27001 aplicada a una carrera universitaria [en línea]. Tesis de pregrado. Universidad Andrés Bello, 2017. [Consulta: 10 de octubre de 2018]. Disponible en:

http://repositorio.unab.cl/xmlui/bitstream/handle/ria/3720/a118929_Maureira_D_Norma_ISO_IEC_27001_aplicada_2017_Tesis.pdf?sequence=1

- MENESES, A., RAMÍREZ, E., MERCHÁN, M. Y SUAREZ, Y. Diseño del sistema de gestión de seguridad de la información sgsi basado en el estándar iso 27001, para los procesos soportados por el área de sistemas en la cámara de comercio de Aguachica, cesar [en línea]. Tesis de Maestría. Universidad Francisco de Paula Santander Ocaña, 2016. [Consulta: 12 de octubre de 2018]. Disponible en: http://repositorio.ufpso.edu.co/jspui/handle/123456789/2872
- MERINO, J. Y TORRES, E. Implementación de un modelo de la seguridad de la información basados en ITIL v3 para una pyme de TI [en línea]. Tesis de pre-grado. Universidad Peruana de Ciencias Aplicadas, 2016. [Consulta: 15 de octubre de 2018]. Disponible en: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/614076/Memoria_ITILGSI_TITULACION_VFinal.pdf?sequence=6&isAllowed=y
- MOLANO, R. Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa Market Mix [en línea]. Tesis de Maestría. Universidad Católica de Colombia, 2017. [Consulta: 12 de octubre de 2018]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/15240/1/Esp%20Auditoria%20de%20sistemas.pdf
- MOLINA, A. Definición y validación de procesos de gestión de seguridad de la Información para la empresa amisoft [en línea]. Tesis de maestría. Universidad De Chile, 2015. [Consulta: 10 de octubre de 2018]. Disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/136243/Definicion-y-validacion-de-procesos-de-gestion-de-seguridad-de-la-informacion.pdf;sequence=1
- MOYANO, L. Y SUAREZ, Y. Plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa interfaces y soluciones en la universidad distrital Francisco José de Caldas [en línea]. Tesis de pre-grado. Universidad Distrital Francisco José de Caldas, 2017. [Consulta: 12 de octubre de 2018]. Disponible en:

http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

- MOZCAIZA, O. Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013 [en línea]. Tesis de pregrado. Universidad Peruana De Ciencias Aplicadas, 2018. [Consulta: 10 de octubre de 2018]. Disponible en: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/623063/MOSCAIZA_MO.pdf?sequence=5&isAllowed=y
- MUSAYON, E. Y VÁSQUEZ, W. Implementación de un sistema de información utilizando tecnología web y basado en el enfoque de gestión de recursos empresariales aplicado al proceso de comercialización para la empresa MBN exportaciones S.R.L. & CIA de la ciudad de Lambayeque [en línea]. Tesis de pre-grado. Universidad Señor de Sipán, 2011. [Consulta: 15 de octubre de 2018]. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/2060/INGENIERIA%20DE%20SISTEMAS.pdf?sequence=1&isAllowed=y
- NIEVES, A. Diseño de un sistema de gestión de la seguridad de la información (sgsi) basados en la norma Iso/iec 27001:2013 [en línea]. Tesis de pregrado. Institución Universitaria Politécnico Gran colombiano, 2017. [Consulta: 10 de octubre de 2018]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y
- Norma Técnica Peruana NTP-ISO/IEC 27001:2014 [CD-ROM]. 2da Ed. INDECOPI, 2014. I.C.S.:35.040
- NIÑO, N. Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el instituto nacional de estadística e informática – INEI Filial Lambayeque [en línea]. Tesis de maestría. Universidad Nacional “Pedro Ruiz Gallo”, 2018. [Consulta: 12 de octubre de 2018]. Disponible en: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5935/BC-

TES-TMP-788%20NI%c3%91O%20MORANTE.pdf?sequence=1&isAllowed=y

- OCHOA, A. Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la universidad nacional José María Arguedas [en línea]. Tesis de pregrado. Universidad Nacional José María Arguedas, 2017. [Consulta: 10 de octubre de 2018]. Disponible en: https://repositorio.unajma.edu.pe/bitstream/handle/123456789/291/Andrea_Tesis_Bachiller_2017.pdf?sequence=1&isAllowed=y
- OLAZA, H. Implementación de NTO ISO/IEC 27001 para la seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin [en línea]. Tesis de pregrado. Universidad Cesar Vallejo, 2017. [Consulta: 10 de octubre de 2018]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/9927/Olaza_AHD.pdf?sequence=1&isAllowed=y
- OIDOR, J. Diseño de un sistema de gestión de seguridad de la información – SGSI bajo la norma ISO/IEC 27001:2013 para la empresa "EN LÍNEA FINANCIERA" de la ciudad de Cali – Colombia [en línea]. Tesis de pregrado. Universidad Nacional Abierta y a Distancia, 2016. [Consulta: 10 de octubre de 2018]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11907/76041068.pdf?sequence=1&isAllowed=y
- OLIVOS, F. Y GUEVARA, E. Formulación de políticos de control de accesos y seguridad física y del entorno basado en la norma técnica peruana NTP-ISO/IEC 17799 para la mejora de la gestión en la oficina central de computo – Universidad de Lambayeque [en línea]. Tesis de Pre-Grado. Universidad de Lambayeque, 2017. [Consulta: 12 de octubre de 2018]. Disponible en: https://repositorio.udl.edu.pe/bitstream/UDL/110/3/E%26F_Tesis2018.pdf
- PALACIOS, D. Diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de informática de la cooperativa del magisterio de Túquerres bajo la norma ISO 27001:2013 [en línea]. Tesis de Pre-Grado. Universidad Nacional Abierta y a Distancia, 2015. [Consulta: 15 de octubre de 2018]. Disponible en:

https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3817/1/1085255001.pdf

- PAVÁN, B. Entendiendo HTML5: guía para principiantes [en línea]. eloriente.net, 2013. [Consulta: 20 de mayo de 2019]. Disponible en: http://www.eloriente.net/home/2013/06/01/entendiendo-html5-guia-para-principiantes/
- PERALTA, A. Metodología SCRUM [en línea]. Universidad ORT Uruguay, 2003. [Consulta: 12 de octubre de 2018]. Disponible en: https://fi.ort.edu.uy/innovaportal/file/2021/1/scrum.pdf
- Presidencia del Consejo de Ministros. A PRESIDENCIA DEL CONSEJO DE MINISTROS APRUEBA EL USO OBLIGATORIO DE LA NORMA TÉCNICA PERUANA "NTP-ISO/IEC 27001:2008 EDI" [en línea]. Lima. 2012. [Consulta: 10 de mayo de 2019]. Disponible en: http://www2.pcm.gob.pe/Prensa/ActividadesPCM/2012/Junio/04-06-12-b.html
- Qué es Bootstrap y cómo usarlo [en línea]. raiolanetworks.es, 2019. [Consulta: 20 de mayo de 2019]. Disponible en: https://raiolanetworks.es/blog/que-es-bootstrap/
- ¿Qué es norma ISO 27001? [en línea]. advisera.com. [Consulta: 10 de mayo de 2019]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/
- QUISPE, A. Y VARGAS, F. Implementación de un sistema de información web para optimizar la gestión administrativa de la empresa comercial angelito de la ciudad de Chepén [en línea]. Tesis de Pre-Grado. Universidad Nacional De Trujillo, 2016. [Consulta: 15 de octubre de 2018]. Disponible en: http://dspace.unitru.edu.pe/bitstream/handle/UNITRU/9330/QUISPE%20HERN%C3%81NDEZ%2C%20Amadeo%20%C3%81ngel%3B%20VARGAS%20CHAVARRI%2C%20Fanny.pdf?sequence=1&isAllowed=y
- QUISPE, J. Declaración de aplicabilidad mediante la NTP-ISO/IEC 27001:2014 para mitigar los siniestros de la información en la sub dirección de licencias de conducir de la dirección regional de transporte y comunicación de Ancash, 2018 [en línea]. Tesis-Pre-Grado. 2018. [Consulta: 12 de octubre de 2018]. Disponible en:

http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2883/T033_44943018_T.pdf?sequence=1&isAllowed=y

- REAL ACADEMIA ESPAÑOLA. Automático [en línea]. RAE, 2018. [Consulta: 10 de mayo de 2019]. Disponible en: https://dle.rae.es/?id=4TO3M08
- REY, C. Estudio de la efectividad de la aplicación de la metodología ágil de desarrollo scrum [en línea]. Tesis de Pre-Grado. Universidad Tecnológica Israel, 2017. [Consulta: 15 de octubre de 2018]. Disponible en: http://repositorio.uisrael.edu.ec/bitstream/47000/1324/1/UISRAEL-EC-SIS-378.242-2017-001.pdf
- RIBAGORDA, A. Seguridad de la Información redes, informática y sistemas de información [en línea]. 2008. [Consulta: 8 de mayo de 2019]. Disponible en: https://revistasic.com/revista81/pdf_81/sic81_bibliografia_seleccionada.pdf
- ROMERAL, L. Y TORRES, A. Gestión de los Riesgos Tecnológicos [en línea]. dialnet.unirioja.es, 2008. [Consulta: 19 de mayo de 2019]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4959507
- RUDAS, L. Modelo de gestión de riesgos para proyectos de desarrollo tecnológico [en línea]. Tesis de Maestría. Santiago de Querétaro, 2017. [Consulta: 15 de octubre de 2018]. Disponible en: https://ciateq.repositorioinstitucional.mx/jspui/bitstream/1020/86/1/RudasTayoLeidyP%20MDGPI%202017.pdf
- SÁNCHEZ, A. Diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001 para pequeña y mediana empresas en la ciudad de Quito [en línea]. Tesis de Pre-Grado. Pontificia Universidad Católica del Ecuador, 2013. [Consulta: 10 de octubre de 2018]. Disponible en: http://repositorio.puce.edu.ec/handle/22000/6293
- SANTOS, D. Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software [en línea]. Tesis pre-grado. Pontificia Universidad Católica del Perú, 2016. [Consulta: 15 de octubre de 2018]. Disponible en:

https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/7616/SANTOS_DANIEL_SISTEMA_GESTI%c3%93N.pdf?sequence=1&isAllowed=y

- SCHWABER, K Y SUTHERLAND, J. La Guía de Scrum [en línea]. 2016. [Consulta: 9 de mayo de 2019]. Disponible en: https://www.scrumguides.org/docs/scrumguide/v2016/2016-Scrum-Guide-Spanish.pdf#zoom=100
- SOFTENG. Metodología SCRUM para desarrollo de software – aplicaciones complejas [en línea]. [Consulta: 5 de mayo de 2019]. Disponible en: https://www.softeng.es/es-es/empresa/metodologias-de-trabajo/metodologia-scrum.html
- SOLIS, J. ¿Qué es Bootstrap y cómo funciona en el diseño web? [en línea]. arweb.com, 2014. [Consulta: 20 de mayo de 2019]. Disponible en: https://www.arweb.com/blog/%C2%BFque-es-bootstrap-y-como-funciona-en-el-diseno-web/
- TALAVERA, V. Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013 [en línea]. Tesis de pregrado. Pontificia Universidad Católica Del Perú, 2015. [Consulta: 10 de octubre de 2018]. Disponible en: https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/6092/TALAVERA_VASCO_DISE%c3%91O_SISTEMA_GESTION.pdf?sequence=1&isAllowed=y
- Taller de transición de la norma ISO/IEC 27001:2005 a la ISO/IEC 27001:2013 [en línea]. docplayer.es. [Consulta: 10 de octubre de 2018]. Disponible en: https://docplayer.es/1624175-Taller-de-transicion-de-la-norma-iso-iec-27001-2005-a-la-iso-iec-27001-2013.html
- TARRILLO, E. Influencia de la gestión de riesgos en la seguridad de activos de información de la zona registral III Sede Moyobamba, 2015 en la universidad Cesar Vallejo [en línea]. Tesis de post-grado. Universidad Cesar Vallejo, 2016. [Consulta: 12 de octubre de 2018]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/1286/tarrillo_se.pdf?sequence=1&isAllowed=y

- TOLA, D. Implementación de un Sistema de gestión de seguridad de la información para una empresa de consultoría de auditoria, aplicando la norma ISO/IEC 27001 [en línea]. Tesis de pre-grado. Escuela Superior Politécnica Del Litoral, 2015. [Consulta: 12 de octubre de 2018]. Disponible en: https://www.dspace.espol.edu.ec/retrieve/89073/D-84631.pdf
- TORRES, M. Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI), basada en la norma ISO/IEC 27001:2013, para el proceso de servicio Post- Venta de un integrador de soluciones en Telecomunicaciones [en línea]. Tesis de pregrado. Universidad Peruana De Ciencias Aplicadas, 2018. [Consulta: 10 de octubre de 2018]. Disponible en: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/624142/Torres_lm.pdf?sequence=12&isAllowed=y
- TORRES, F. Introducción a la automatización y el control [en línea]. Universidad de Alicante. [Consulta: 10 de mayo de 2019]. Disponible en: https://rua.ua.es/dspace/bitstream/10045/18432/1/Tema%201_Introduccion.pdf
- UNIVERSIDAD DE ALICANTE. Navegadores [en línea]. 2013. [Consulta: 10 de mayo de 2019]. Disponible en: https://rua.ua.es/dspace/bitstream/10045/46501/3/ci2_basico_2014-15_Navegadores.pdf
- VILCA, E. Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima [en línea]. Tesis Pre-Grado. Universidad De Huánuco, 2017. [Consulta: 12 de octubre de 2018]. Disponible en: http://repositorio.udh.edu.pe/bitstream/handle/123456789/809/T_047_43087253_T.pdf?sequence=1&isAllowed=y
- VILLALBA, L. Aplicación de Scrum en el desarrollo de software de TeamSoft S.A.C. [en línea]. Tesis de Pre-Grado. Universidad Cesar Vallejo, 2017. [Consulta: 15 de octubre de 2018]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/17710/Villalva_CL.pdf?sequence=1&isAllowed=y
- WESTERMAN. G. IT Risk Management: From IT Necessity to Strategic Business Value [en línea]. Massachusetts Institute of Technology, 2006.

[Consulta: 10 de octubre de 2018]. Disponible en: https://dspace.mit.edu/bitstream/handle/1721.1/39809/4658-07.pdf

- YÁÑEZ, N. Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño [en línea]. Tesis de maestría. Universidad de Chile, 2017. [Consulta: 10 de octubre de 2018]. Disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia- y-Empresas.pdf?sequence=1&isAllowed=y
- YÁÑEZ, N. Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño [en línea]. Tesis de maestría. Universidad de Chile, 2017. [Consulta: 10 de octubre de 2018]. Disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia- y-Empresas.pdf?sequence=1&isAllowed=y
- ZACARÍAS, J. Modelo de seguridad de la información basado en la Iso/Iec 27001:2013 para mitigar los riesgos de los activos de información en la central de Operaciones Policiales de la Región Policial Junín [en línea]. Tesis de pregrado. Universidad Continental, 2017. [Consulta: 10 de octubre de 2018]. Disponible en: https://repositorio.continental.edu.pe/bitstream/20.500.12394/4105/3/INV_FIN_103_TE_Zacarias_Villafranca_2017.pdf
- Zúñiga A. y Solano M. Riesgo de TI [en línea]. Slidesahre. 2013. [Consulta: 15 de octubre de 2018]. Disponible en: https://es.slideshare.net/LeoGomez3/riesgo-de-ti

Anexo 1: Ficha de observación

FICHA DE OBSERVACIÓN

EVALUACIÓN DEL CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

FECHA:

Marque con SI o NO en caso se cumpla o no con el proceso indicado.

Registros	Dimensiones											
	Confidencialidad						Integridad				Disponibilidad	
	Gestión de claves		Número de información divulgada		Accesos no autorizados.		Número de cambios no autorizados a los datos de producción		Número de virus informáticos		Tiempo disponible del sistema para el usuario	
	PRE TEST	POS TEST	PRE TEST	POS TEST	PRE TEST	POS TEST	PRE TEST	POS TEST	PRE TEST	POS TEST	PRE TEST	POS TEST
1.												
2.												
3.												
4.												
5.												
6.												
7.												
8.												
9.												
10.												
11.												
12.												
13.												
14.												
15.												
16.												
17.												
18.												
19.												
20.												
21.												
22.												
23.												
24.												
25.												
26.												
27.												
28.												
29.												
30.												
31.												
32.												
33.												
34.												
35.												
36.												
37.												

38.												
39.												
40.												
41.												
42.												
43.												
44.												
45.												
46.												
47.												
48.												
49.												
50.												

Tabla 31Intrumento de recolección de datos - Ficha de observación

Gestión de claves - PRE	Gestión de claves - POST	Número de información divulgada - PRE	Número de información divulgada- POST	Accesos no autorizados - PRE	Accesos no autorizados POST	Número de cambios no autorizados a los datos de producción - PRE	Número de cambios no autorizados a los datos de producción - POST	Número de virus informáticos - PRE	Número de virus informáticos - POST	Tiempo disponible del sistema para el usuario - PRE	Tiempo disponible del sistema para el usuario - POST
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1

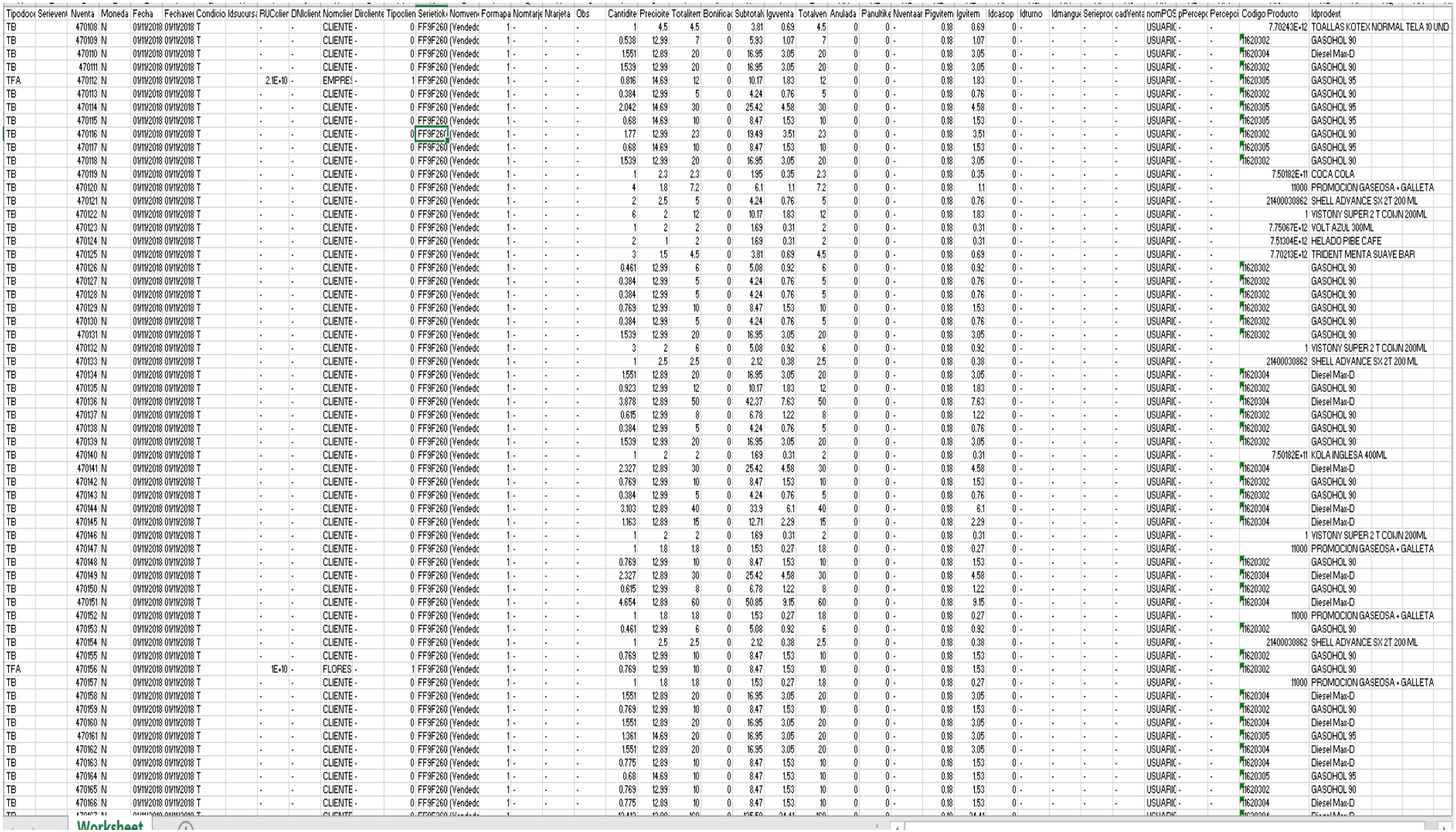
Tabla 32 Instrumento de recolección de datos - Ficha de observación evaluada

Gestión de claves - PRE	Gestión de claves - POST	Número de información divulgada - PRE	Número de información divulgada- POST	Accesos no autorizados - PRE	Accesos no autorizados POST	Número de cambios no autorizados a los datos de producción - PRE	Número de cambios no autorizados a los datos de producción - POST	Número de virus informáticos - PRE	Número de virus informáticos - POST	Tiempo disponible del sistema para el usuario - PRE	Tiempo disponible del sistema para el usuario - POST
1	1	0	0	0	0	0	0	0	0	1	1
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1

Tabla 33 Instrumento de recolección de datos - Ficha de observación evaluada

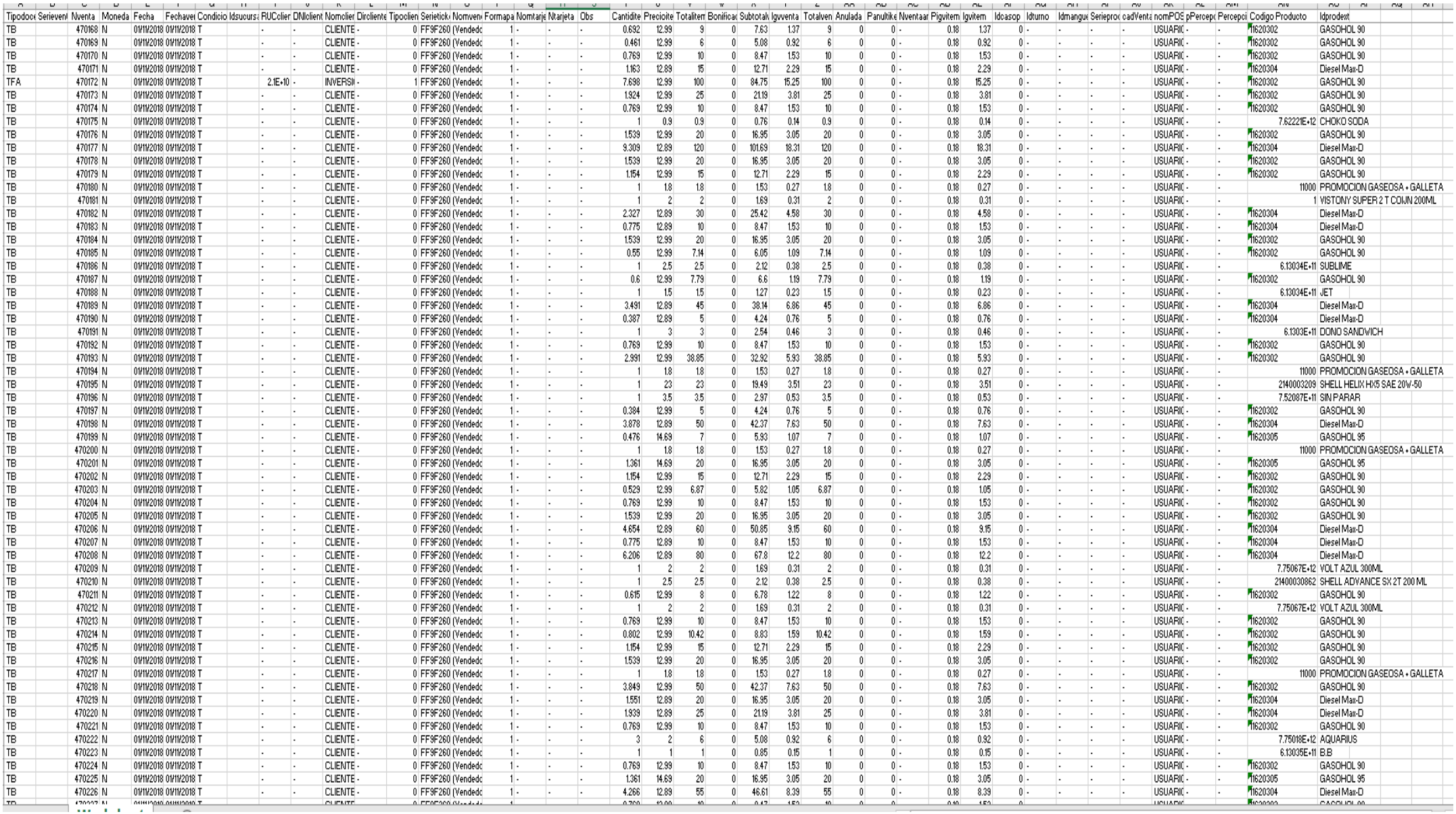
Gestión de claves - PRE	Gestión de claves - POST	Número de información divulgada - PRE	Número de información divulgada- POST	Accesos no autorizados - PRE	Accesos no autorizados POST	Número de cambios no autorizados a los datos de producción - PRE	Número de cambios no autorizados a los datos de producción - POST	Número de virus informáticos - PRE	Número de virus informáticos - POST	Tiempo disponible del sistema para el usuario - PRE	Tiempo disponible del sistema para el usuario - POST
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
1	1	0	0	0	0	0	0	0	0	1	1
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	1	0	0	0	0	0	0	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	0	1	0	1	0	1	1	0
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1
0	1	1	0	1	0	1	0	1	0	0	1

Tabla 34 Instrumento de recolección de datos - Ficha de observación evaluada



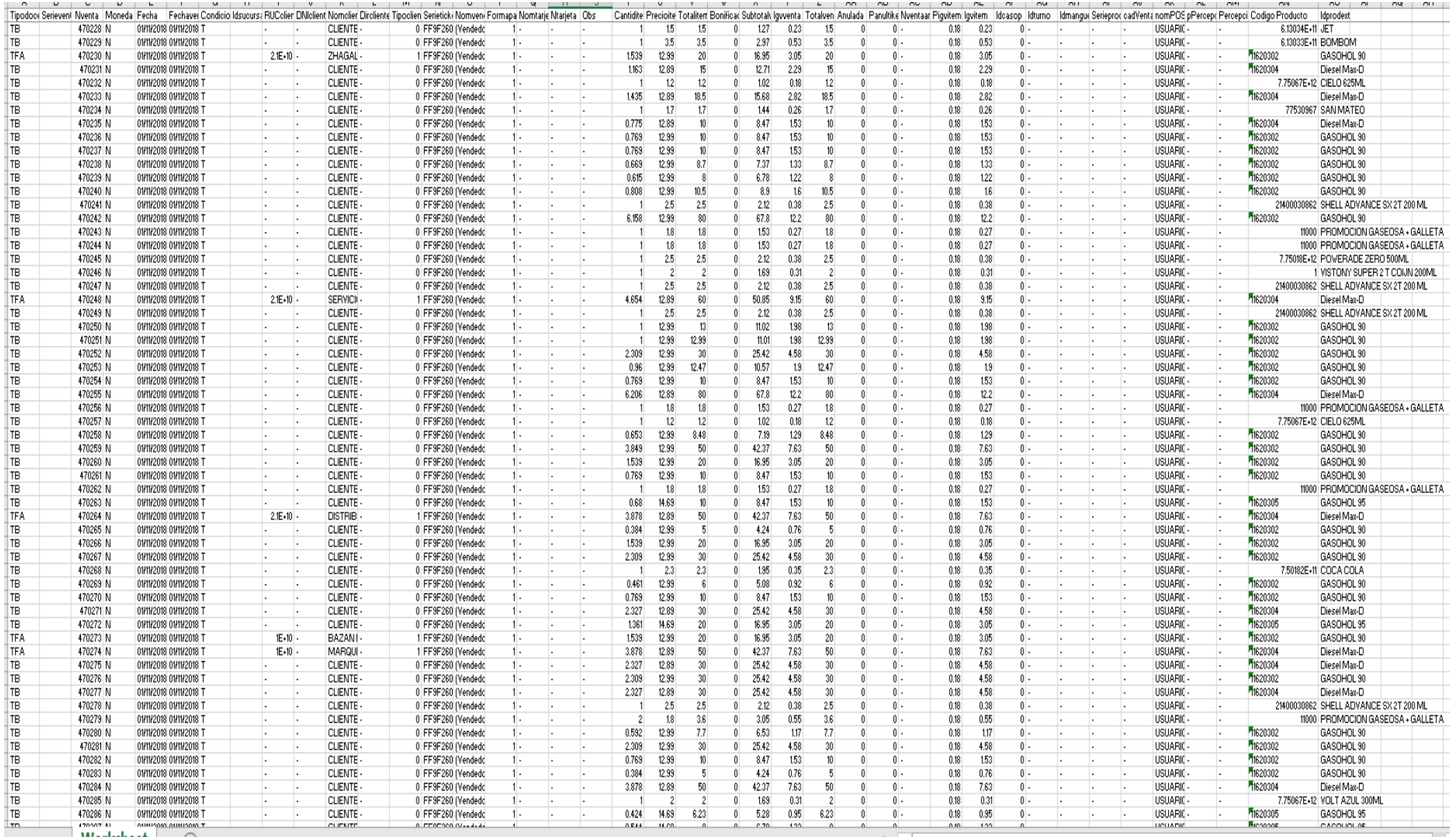
Tipodoc	Serievent	Nventa	Moneda	Fecha	Fechavei	Condicio	Idsucurs	RUCclier	DNIclient	Nomclier	Dircliente	Tipoclien	Serietick	Nomvend	Formapa	Nomtarje	Ntarjeta	Obs	Cantidite	Precioite	Totalitem	Bonificac	Subtotalv	Igvventa	Totalven	Anulada	Panultike	Nventaar	Pigvitem	Igvitem	Idcasop	Idturno	Idmangue	Serieproc	cadVenta	nomPOS	pPercep	Percepci	Codigo	Producto	Idprodeit
TB		470108	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	4.5	4.5	0	3.81	0.69	4.5	0	0	-	0.18	0.69	0	-	-	-	-	USUARIO -	-	7.70243E+12	TOALLAS KOTEX NORMAL TELA 10	UND
TB		470109	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.538	12.99	7	0	5.93	1.07	7	0	0	-	0.18	1.07	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470110	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.551	12.89	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470111	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TFA		470112	N	01/11/2018	01/11/2018	T		2.1E+10	-	EMPRES	-	1	FF9F260	(Vendedc	1	-	-	-	0.816	14.69	12	0	10.17	1.83	12	0	0	-	0.18	1.83	0	-	-	-	-	USUARIO -	-	1620305	GASOHOL 95	
TB		470113	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470114	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.042	14.69	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-	-	-	-	USUARIO -	-	1620305	GASOHOL 95	
TB		470115	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.68	14.69	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620305	GASOHOL 95	
TB		470116	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.77	12.99	23	0	19.49	3.51	23	0	0	-	0.18	3.51	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470117	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.68	14.69	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620305	GASOHOL 95	
TB		470118	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470119	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.3	2.3	0	1.95	0.35	2.3	0	0	-	0.18	0.35	0	-	-	-	-	USUARIO -	-	7.50182E+11	COCA COLA	
TB		470120	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	4	1.8	7.2	0	6.1	1.1	7.2	0	0	-	0.18	1.1	0	-	-	-	-	USUARIO -	-	11000	PROMOCION GASEOSA + GALLETA	
TB		470121	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2	2.5	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIO -	-	21400030862	SHELL ADVANCE SX 2T 200 ML	
TB		470122	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	6	2	12	0	10.17	1.83	12	0	0	-	0.18	1.83	0	-	-	-	-	USUARIO -	-	1	VISTONY SUPER 2 T COJIN 200ML	
TB		470123	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-	-	-	-	USUARIO -	-	7.75067E+12	VOLT AZUL 300ML	
TB		470124	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2	1	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-	-	-	-	USUARIO -	-	7.51304E+12	HELADO PIBE CAFE	
TB		470125	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3	1.5	4.5	0	3.81	0.69	4.5	0	0	-	0.18	0.69	0	-	-	-	-	USUARIO -	-	7.70213E+12	TRIDENT MENTA SUAVE BAR	
TB		470126	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.461	12.99	6	0	5.08	0.92	6	0	0	-	0.18	0.92	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470127	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470128	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470129	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470130	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470131	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470132	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3	2	6	0	5.08	0.92	6	0	0	-	0.18	0.92	0	-	-	-	-	USUARIO -	-	1	VISTONY SUPER 2 T COJIN 200ML	
TB		470133	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-	-	-	-	USUARIO -	-	21400030862	SHELL ADVANCE SX 2T 200 ML	
TB		470134	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.551	12.89	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470135	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.923	12.99	12	0	10.17	1.83	12	0	0	-	0.18	1.83	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470136	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3.878	12.89	50	0	42.37	7.63	50	0	0	-	0.18	7.63	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470137	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.615	12.99	8	0	6.78	1.22	8	0	0	-	0.18	1.22	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470138	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470139	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470140	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-	-	-	-	USUARIO -	-	7.50182E+11	KOLA INGLESA 400ML	
TB		470141	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.327	12.89	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470142	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470143	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470144	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3.103	12.89	40	0	33.9	6.1	40	0	0	-	0.18	6.1	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470145	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.163	12.89	15	0	12.71	2.29	15	0	0	-	0.18	2.29	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470146	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-	-	-	-	USUARIO -	-	1	VISTONY SUPER 2 T COJIN 200ML	
TB		470147	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-	-	-	-	USUARIO -	-	11000	PROMOCION GASEOSA + GALLETA	
TB		470148	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470149	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.327	12.89	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470150	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.615	12.99	8	0	6.78	1.22	8	0	0	-	0.18	1.22	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470151	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	4.654	12.89	60	0	50.85	9.15	60	0	0	-	0.18	9.15	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470152	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-	-	-	-	USUARIO -	-	11000	PROMOCION GASEOSA + GALLETA	
TB		470153	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.461	12.99	6	0	5.08	0.92	6	0	0	-	0.18	0.92	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470154	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-	-	-	-	USUARIO -	-	21400030862	SHELL ADVANCE SX 2T 200 ML	
TB		470155	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TFA		470156	N	01/11/2018	01/11/2018	T		1E+10	-	FLORES -		1	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470157	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-	-	-	-	USUARIO -	-	11000	PROMOCION GASEOSA + GALLETA	
TB		470158	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.551	12.89	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470159	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470160	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.551	12.89	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470161	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.361	14.69	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620305	GASOHOL 95	
TB		470162	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.551	12.89	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470163	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.775	12.89	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	
TB		470164	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.68	14.69	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620305	GASOHOL 95	
TB		470165	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620302	GASOHOL 90	
TB		470166	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.775	12.89	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIO -	-	1620304	Diesel Max-D	

Tabla 35 Registro de ventas



Tipodoc	Serievent	Nventa	Moneda	Fecha	Fechavei	Condicio	Idsucursa	RUCclier	DNIclient	Nomclier	Dircliente	Tipoclien	Serietick	Nomvend	Formapa	Nomtarje	Ntarjeta	Obs	Cantidite	Precioite	Totalitem	Bonificac	Subtotal	Igvventa	Totalven	Anulada	Panultike	Nventaar	Pigvitem	Igvitem	Idcasop	Idturno	Idmangue	Serieproc	cadVenta	nomPOS	pPercep	Percepci	Codigo	Producto	Idprodext
TB		470168	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.692	12.99	9	0	7.63	1.37	9	0	0	-	0.18	1.37	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470169	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.461	12.99	6	0	5.08	0.92	6	0	0	-	0.18	0.92	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470170	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470171	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.163	12.89	15	0	12.71	2.29	15	0	0	-	0.18	2.29	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TFA		470172	N	01/11/2018	01/11/2018	T		2.1E+10	-	INVERSIÓ	-	1	FF9F260	(Vendedc	1	-	-	-	7.698	12.99	100	0	84.75	15.25	100	0	0	-	0.18	15.25	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470173	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.924	12.99	25	0	21.19	3.81	25	0	0	-	0.18	3.81	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470174	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470175	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	0.9	0.9	0	0.76	0.14	0.9	0	0	-	0.18	0.14	0	-	-	-	-	USUARIC	-		7.62221E+12		CHOKO SODA
TB		470176	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470177	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	9.309	12.89	120	0	101.69	18.31	120	0	0	-	0.18	18.31	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470178	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470179	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.154	12.99	15	0	12.71	2.29	15	0	0	-	0.18	2.29	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470180	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-	-	-	-	USUARIC	-		11000		PROMOCION GASEOSA + GALLETA
TB		470181	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-	-	-	-	USUARIC	-		1		VISTONY SUPER 2 T COMN 200ML
TB		470182	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.327	12.89	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470183	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.775	12.89	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470184	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470185	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.55	12.99	7.14	0	6.05	1.09	7.14	0	0	-	0.18	1.09	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470186	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-	-	-	-	USUARIC	-		6.13034E+11		SUBLIME
TB		470187	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.6	12.99	7.79	0	6.6	1.19	7.79	0	0	-	0.18	1.19	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470188	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.5	1.5	0	1.27	0.23	1.5	0	0	-	0.18	0.23	0	-	-	-	-	USUARIC	-		6.13034E+11		JET
TB		470189	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3.491	12.89	45	0	38.14	6.86	45	0	0	-	0.18	6.86	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470190	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.387	12.89	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470191	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	3	3	0	2.54	0.46	3	0	0	-	0.18	0.46	0	-	-	-	-	USUARIC	-		6.1303E+11		DONO SANDVICH
TB		470192	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470193	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.991	12.99	38.85	0	32.92	5.93	38.85	0	0	-	0.18	5.93	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470194	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-	-	-	-	USUARIC	-		11000		PROMOCION GASEOSA + GALLETA
TB		470195	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	23	23	0	19.49	3.51	23	0	0	-	0.18	3.51	0	-	-	-	-	USUARIC	-		2140003209		SHELL HELIX HX5 SAE 20W-50
TB		470196	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	3.5	3.5	0	2.97	0.53	3.5	0	0	-	0.18	0.53	0	-	-	-	-	USUARIC	-		7.52087E+11		SIN PARAR
TB		470197	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470198	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3.878	12.89	50	0	42.37	7.63	50	0	0	-	0.18	7.63	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470199	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.476	14.69	7	0	5.93	1.07	7	0	0	-	0.18	1.07	0	-	-	-	-	USUARIC	-		1620305		GASOHOL 95
TB		470200	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-	-	-	-	USUARIC	-		11000		PROMOCION GASEOSA + GALLETA
TB		470201	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.361	14.69	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIC	-		1620305		GASOHOL 95
TB		470202	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.154	12.99	15	0	12.71	2.29	15	0	0	-	0.18	2.29	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470203	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.529	12.99	6.87	0	5.82	1.05	6.87	0	0	-	0.18	1.05	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470204	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470205	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470206	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	4.654	12.89	60	0	50.85	9.15	60	0	0	-	0.18	9.15	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470207	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.775	12.89	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470208	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	6.206	12.89	80	0	67.8	12.2	80	0	0	-	0.18	12.2	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470209	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-	-	-	-	USUARIC	-		7.75067E+12		VOLT AZUL 300ML
TB		470210	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-	-	-	-	USUARIC	-		21400030862		SHELL ADVANCE SX 2T 200 ML
TB		470211	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.615	12.99	8	0	6.78	1.22	8	0	0	-	0.18	1.22	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470212	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-	-	-	-	USUARIC	-		7.75067E+12		VOLT AZUL 300ML
TB		470213	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470214	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.802	12.99	10.42	0	8.83	1.59	10.42	0	0	-	0.18	1.59	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470215	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.154	12.99	15	0	12.71	2.29	15	0	0	-	0.18	2.29	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470216	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470217	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-	-	-	-	USUARIC	-		11000		PROMOCION GASEOSA + GALLETA
TB		470218	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3.849	12.99	50	0	42.37	7.63	50	0	0	-	0.18	7.63	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470219	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.551	12.89	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470220	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.939	12.89	25	0	21.19	3.81	25	0	0	-	0.18	3.81	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D
TB		470221	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470222	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3	2	6	0	5.08	0.92	6	0	0	-	0.18	0.92	0	-	-	-	-	USUARIC	-		7.75018E+12		AQUARIUS
TB		470223	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1	1	0	0.85	0.15	1	0	0	-	0.18	0.15	0	-	-	-	-	USUARIC	-		6.13035E+11		B.B
TB		470224	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-	-	-	-	USUARIC	-		1620302		GASOHOL 90
TB		470225	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.361	14.69	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-	-	-	-	USUARIC	-		1620305		GASOHOL 95
TB		470226	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	4.266	12.89	55	0	46.61	8.39	55	0	0	-	0.18	8.39	0	-	-	-	-	USUARIC	-		1620304		Diesel Max-D

Tabla 36 Registro de ventas



Tipodoc	Serievent	Nventa	Moneda	Fecha	Fechavei	Condicio	Idsucursa	RUCclier	DNIclient	Nomclier	Dircliente	Tipoclien	Serietick	Nomvend	Formapa	Nomtarje	Ntarjeta	Obs	Cantidite	Precioite	Totalitem	Bonificac	Subtotalv	Igvventa	Totalven	Anulada	Panultiks	Nventaar	Pigvitem	Igvitem	Idcasop	Idturno	Idmangue	Serieproc	cadVenta	nomPOS	pPercep	Percepci	Codigo	Producto	Idprodeit
TB		470228	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.5	1.5	0	1.27	0.23	1.5	0	0	-	0.18	0.23	0	-				USUARIC	-		6.13034E+11	JET	
TB		470229	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	3.5	3.5	0	2.97	0.53	3.5	0	0	-	0.18	0.53	0	-				USUARIC	-		6.13033E+11	BOMBOM	
TFA		470230	N	01/11/2018	01/11/2018	T		2.1E+10	-	ZHAGAL -		1	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470231	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.163	12.89	15	0	12.71	2.29	15	0	0	-	0.18	2.29	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470232	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.2	1.2	0	1.02	0.18	1.2	0	0	-	0.18	0.18	0	-				USUARIC	-		7.75067E+12	CIELO 625ML	
TB		470233	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.435	12.89	18.5	0	15.68	2.82	18.5	0	0	-	0.18	2.82	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470234	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.7	1.7	0	1.44	0.26	1.7	0	0	-	0.18	0.26	0	-				USUARIC	-		77530967	SAN MATEO	
TB		470235	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.775	12.89	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470236	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470237	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470238	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.669	12.99	8.7	0	7.37	1.33	8.7	0	0	-	0.18	1.33	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470239	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.615	12.99	8	0	6.78	1.22	8	0	0	-	0.18	1.22	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470240	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.808	12.99	10.5	0	8.9	1.6	10.5	0	0	-	0.18	1.6	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470241	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-				USUARIC	-		21400030862	SHELL ADVANCE SX 2T 200 ML	
TB		470242	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	6.158	12.99	80	0	67.8	12.2	80	0	0	-	0.18	12.2	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470243	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-				USUARIC	-		11000	PROMOCION GASEOSA + GALLETA	
TB		470244	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-				USUARIC	-		11000	PROMOCION GASEOSA + GALLETA	
TB		470245	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-				USUARIC	-		7.75018E+12	POWERADE ZERO 500ML	
TB		470246	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-				USUARIC	-		1	VISTONY SUPER 2 T COJIN 200ML	
TB		470247	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-				USUARIC	-		21400030862	SHELL ADVANCE SX 2T 200 ML	
TFA		470248	N	01/11/2018	01/11/2018	T		2.1E+10	-	SERVICII -		1	FF9F260	(Vendedc	1	-	-	-	4.654	12.89	60	0	50.85	9.15	60	0	0	-	0.18	9.15	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470249	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-				USUARIC	-		21400030862	SHELL ADVANCE SX 2T 200 ML	
TB		470250	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	12.99	13	0	11.02	1.98	13	0	0	-	0.18	1.98	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470251	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	12.99	12.99	0	11.01	1.98	12.99	0	0	-	0.18	1.98	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470252	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.309	12.99	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470253	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.96	12.99	12.47	0	10.57	1.9	12.47	0	0	-	0.18	1.9	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470254	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470255	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	6.206	12.89	80	0	67.8	12.2	80	0	0	-	0.18	12.2	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470256	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-				USUARIC	-		11000	PROMOCION GASEOSA + GALLETA	
TB		470257	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.2	1.2	0	1.02	0.18	1.2	0	0	-	0.18	0.18	0	-				USUARIC	-		7.75067E+12	CIELO 625ML	
TB		470258	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.653	12.99	8.48	0	7.19	1.29	8.48	0	0	-	0.18	1.29	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470259	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3.849	12.99	50	0	42.37	7.63	50	0	0	-	0.18	7.63	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470260	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470261	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470262	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	1.8	1.8	0	1.53	0.27	1.8	0	0	-	0.18	0.27	0	-				USUARIC	-		11000	PROMOCION GASEOSA + GALLETA	
TB		470263	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.68	14.69	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-				USUARIC	-		1620305	GASOHOL 95	
TFA		470264	N	01/11/2018	01/11/2018	T		2.1E+10	-	DISTRIB -		1	FF9F260	(Vendedc	1	-	-	-	3.878	12.89	50	0	42.37	7.63	50	0	0	-	0.18	7.63	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470265	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470266	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470267	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.309	12.99	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470268	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.3	2.3	0	1.95	0.35	2.3	0	0	-	0.18	0.35	0	-				USUARIC	-		7.50182E+11	COCA COLA	
TB		470269	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.461	12.99	6	0	5.08	0.92	6	0	0	-	0.18	0.92	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470270	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470271	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.327	12.89	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470272	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1.361	14.69	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-				USUARIC	-		1620305	GASOHOL 95	
TFA		470273	N	01/11/2018	01/11/2018	T		1E+10	-	BAZAN I -		1	FF9F260	(Vendedc	1	-	-	-	1.539	12.99	20	0	16.95	3.05	20	0	0	-	0.18	3.05	0	-				USUARIC	-		1620302	GASOHOL 90	
TFA		470274	N	01/11/2018	01/11/2018	T		1E+10	-	MARQUI -		1	FF9F260	(Vendedc	1	-	-	-	3.878	12.89	50	0	42.37	7.63	50	0	0	-	0.18	7.63	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470275	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.327	12.89	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470276	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.309	12.99	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470277	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.327	12.89	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470278	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2.5	2.5	0	2.12	0.38	2.5	0	0	-	0.18	0.38	0	-				USUARIC	-		21400030862	SHELL ADVANCE SX 2T 200 ML	
TB		470279	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2	1.8	3.6	0	3.05	0.55	3.6	0	0	-	0.18	0.55	0	-				USUARIC	-		11000	PROMOCION GASEOSA + GALLETA	
TB		470280	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.592	12.99	7.7	0	6.53	1.17	7.7	0	0	-	0.18	1.17	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470281	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	2.309	12.99	30	0	25.42	4.58	30	0	0	-	0.18	4.58	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470282	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.769	12.99	10	0	8.47	1.53	10	0	0	-	0.18	1.53	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470283	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.384	12.99	5	0	4.24	0.76	5	0	0	-	0.18	0.76	0	-				USUARIC	-		1620302	GASOHOL 90	
TB		470284	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	3.878	12.89	50	0	42.37	7.63	50	0	0	-	0.18	7.63	0	-				USUARIC	-		1620304	Diesel Max-D	
TB		470285	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	1	2	2	0	1.69	0.31	2	0	0	-	0.18	0.31	0	-				USUARIC	-		7.75067E+12	VOLT AZUL 300ML	
TB		470286	N	01/11/2018	01/11/2018	T		-	-	CLIENTE -		0	FF9F260	(Vendedc	1	-	-	-	0.424	14.69	6.23	0	5.28	0.95	6.23	0	0	-	0.18	0.95	0	-				USUARIC	-		1620305	GASOHOL 95	

Tabla 37 Registro de ventas

Anexo 2: Matriz de operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTO	ESCALA
VARIABLE INDEPENDIENTE AUTOMATIZACIÓN	"La automatización de un proceso se basa en la reemplazar las labores comúnmente manuales por las mismas llevadas a cabo de forma automática por máquinas, robots o cualquier otro tipo de automatismo. De esta manera, gracias al uso adicional de sensores, controladores y actuadores, así como de métodos y algoritmos de conmutación, se logra liberar a los humanos de algunas tareas." (PAC-Performance-centered Adaptive Curriculum, pág. 3).	Permitirá automatizar, agilizar y mejorar los procesos manuales de la seguridad de la información basado en la norma técnica peruana ISO 27001 mediante un sistema.	-	-	-	-
VARIABLE DEPENDIENTE SEGURIDAD DE LA INFORMACIÓN	"La seguridad de la organización es un proceso de optimización continua, donde participan todos los trabajadores de la empresa, manejándose bajo un modelo eficaz que monitoree los valores cuantitativos y cualitativos, contra los riesgos de seguridad no solo reactivamente, sino proactiva y preventivamente. permitiendo observar y controlar al máximo detalle y profundidad el ciclo de vida de optimización de la seguridad del negocio de acuerdo a los objetivos de productividad, competitividad y supervivencia en ocasiones cambiante." (Areitio, 2008, pág. 11).	Es el proceso que permitirá gestionar la confidencialidad, disponibilidad e integridad de la organización de manera correcta, siguiendo paso a paso sus normas para llegar a proteger la información de la organización y no sea vulnerada.	CONFIDENCIALIDAD	-Gestión de claves -Número de información divulgada -Accesos no autorizados	FICHA DE OBSERVACIÓN	DICOTÓMICA
			INTEGRIDAD	-Número de cambios no autorizados a los datos de producción -Número de virus informáticos	FICHA DE OBSERVACIÓN	DICOTÓMICA
			DISPONIBILIDAD	-Tiempo disponible del sistema para el usuario	FICHA DE OBSERVACIÓN	DICOTÓMICA

Anexo 3: Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPÓTESIS		DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTO	ESCALA
¿Qué efectos produce aplicar la automatización de la gestión de riesgos para la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L.?	Determinar qué efectos produce aplicar la automatización de la gestión de riesgos para la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L.	Aplicar la automatización de la gestión de riesgos produce efectos significativos en la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L..	AUTOMATIZACIÓN	"La automatización de un proceso consiste en la sustitución de aquellas tareas tradicionalmente manuales por las mismas realizadas de manera automática por máquinas, robots o cualquier otro tipo de automatismo. De este modo, gracias al uso adicional de sensores, controladores y actuadores, así como de métodos y algoritmos de conmutación, se consigue liberar al ser humano de ciertas tareas." (PAC- Performance-centered Adaptive Curriculum, pág. 3)	Permitirá automatizar, agilizar y mejorar los procesos manuales de la seguridad de la información basado en la norma técnica peruana ISO 27001 mediante un sistema.	-	-	-	-
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICOS**	SEGURIDAD DE LA INFORMACIÓN – VD	"La seguridad de toda organización es un proceso de mejora continua, en la que han de estar implicados todo el departamento de la empresa, las cuales deben de estar bajo un modelo de madurez eficaz que monitorea con	Es el proceso que permitirá gestionar la confidencialidad, disponibilidad e integridad de la organización de manera correcta, siguiendo paso a paso sus normas para llegar a proteger la información de la	CONFIDENCIALIDAD	-Gestión de claves -Número de información divulgada -Accesos no autorizados	FICHA DE OBSERVACIÓN	Dicotómica
¿Qué efectos produce aplicar la automatización de la gestión de riesgos en la confidencialidad para la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L.?	Determinar qué efecto produce aplicar la automatización de la gestión de riesgos en la confidencialidad para la seguridad de la información en	Aplicar la automatización de la gestión de riesgos produce efectos significativos en la confidencialidad para la seguridad de la información en la empresa ZEPPELIN							

	la empresa ZEPPELIN Inversiones Generales S.R.L.	inversiones generales S.R.L.		valores cuantitativos y cualitativos, los riesgos de seguridad no solo de forma reactiva, si no proactiva y preventiva. Además, tiene que permitir controlar y observar con el máximo grado de detalle y profundidad, todo el aspecto del ciclo de vida infinito de mejora de la seguridad del negocio, haciéndolo acorde con los objetivos de productibilidad, competitividad y supervivencia, a veces cambiante. Según Areitio (2008, pág. 11).	organización y no sea vulnerada.				
¿Qué efectos produce aplicar la automatización de la gestión de riesgos en la disponibilidad para la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L.?	Determinar qué efecto produce aplicar la automatización de la gestión de riesgos en la disponibilidad para la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L.	Aplicar la automatización de la gestión de riesgos produce efectos significativos en la disponibilidad para la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L.				INTEGRIDAD	-Número de cambios no autorizados a los datos de producción -Número de virus informáticos	FICHA DE OBSERVACIÓN	Dicotómica
¿Qué efectos produce aplicar la automatización de la gestión de riesgos en la integridad para la seguridad de la información en la empresa ZEPPELIN Inversiones S.R.L.?	Determinar qué efecto produce aplicar la automatización de la gestión de riesgos en la integridad para la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L.	Aplicar la automatización de la gestión de riesgos produce efectos significativos en la integridad para la seguridad de la información en la empresa ZEPPELIN Inversiones Generales S.R.L.				DISPONIBILIDAD	-Tiempo disponible del sistema para el usuario	FICHA DE OBSERVACIÓN	Dicotómica

Tabla 38 Matriz de consistencia

Anexo 4: Desarrollo

Inicio

Priorizado del Producto

La lista priorizada del producto estará dividida en historias de usuario con un código que las identifique para realizar el sistema de automatización de la seguridad de la información basado en la normativa ISO 27001 en la empresa Zeppelin Inversiones Generales, de contenido web, a continuación, se muestra la lista de requerimientos priorizadas.

CÓDIGO	Descripción
HU01	Como <<administrador>> quiero <<visualizar los registros ingresados>> para tener <<un mayor control>>
HU02	Como <<administrador>> quiero <<ingresar un registro de información>>
HU03	Como <<administrador>> quiero <<acceder a evaluar un registro ingresado>>
HU04	Como <<administrador>> quiero <<actualizar los registros ya evaluados>> para <<tener un mejor control >>
HU05	<<Panel de administrador>>

Tabla 39 Lista de requerimientos priorizadas

Planificación y Estimación

HU01	Como <<administrador>> quiero <<logueo de ingreso al sistema>> para tener <<un mayor control>>	
CRITERIOS DE ACEPTACIÓN		
1.	<<El logo de la empresa es necesario en todo el sistema web>>	dado <<un administrador está en el sistema>> cuando <<ingresa sistema y pulsa enter>> entonces<<carga él sistema y se muestra la página principal del sistema con el logo de la empresa>>
2.	<<La barra de navegación es necesaria en todo sistema>>	dado <<un administrador está en el sistema >> cuando <<ingresa y pulsa enter>> entonces<<carga la página y se muestra los controles >>
3.	<<La imagen y el título es necesario ser mostrado en todo el sistema web>>	dado <<un usuario está en el navegador de búsqueda>> cuando <<ingresa a la dirección del sistema web y pulsa enter>> entonces<<carga la imagen y el titulo lo cual se muestra en la página principal del sistema web>>

4.	<<La imagen y descripción de los servicios son necesarios ser mostrados en la página principal>>	dado <<un usuario está en el navegador de búsqueda>> cuando <<ingresa a la dirección del sistema web y pulsa enter>> entonces<<carga la sección de servicios con las imágenes de cada servicio lo cual se muestra en la página principal del sistema web>>
5.	<<La sección nosotros es necesario ser mostrado en la página principal>>	dado <<un usuario está en el navegador de búsqueda>> cuando <<ingresa a la dirección del sistema web y pulsa enter>> entonces<<carga la sección de nosotros con la información de la empresa la cual se muestra en la página principal del sistema web>>

Tabla 40 Planificación de logeo de sistema

HU02	Como <<administrador>> quiero <<ingresar un registro de información>>	
CRITERIOS DE ACEPTACIÓN		
1.	<<El administrador selecciona el botón registrar >>	<<un administrador selecciona registrar>> luego<<ingresa los parámetros necesarios para el registro>> entonces<<se ingresa el registro en el sistema>>
2.	<<El administrador cierra el proceso de registrar >>	Entonces << el proceso de registro >> no se guarda
3.	<<El administrador da registrar>>	Entonces << el registro de información queda grabado en la base de dato>>

Tabla 41 Planificación de un ingreso un registro de información

HU03	Como <<administrador>> quiero <<acceder a evaluar un registro ingresado>>	
CRITERIOS DE ACEPTACIÓN		
1.	<<administrador selecciona registro>>	Luego << de seleccionar el registro>> evaluamos los dominios, controles y objetivos
2.	<< evaluamos los dominios, controles y objetivos >>	evaluamos << cada dominio, control y objetivo según la iso 27001>>
3.	<<el administrador guarda los cambios>>	Dado<<un administrador en la ventana evaluación >> cuando <<guarda los cambios>> entonces <<se visualiza en la base de datos>>

Tabla 42 Planificación de evaluación de registro ingresado

HU04	Como <<administrador>> quiero <<actualizar los registros ya evaluados>> para <<tener un mejor control >>	
CRITERIOS DE ACEPTACIÓN		
1.	<< administrados ingresa al sistema>>	<< selecciona campos de evaluación registro>>
2.	<<administrador selección el registro evaluado >>	Luego << seleccionar el registro>> << podemos modificar los dominios, controles y objetivos necesarios
3.	<<administrador guarda las actualizaciones>>	Luego << de guardar los cambios necesarios>> el registro << guarda los cambios>> << muestra en la base de dato>>

Tabla 43 Planificación de actualización de registros evaluados

HU05	<<Ajustes>>	
CRITERIOS DE ACEPTACIÓN		
1	<<logeo de administrador>>	<<una vez loqueado el administrador>> muestra<< opción de actualizar y registro de usuario>>
2	<<registro de usuario>>	Debe << ingresar nombre y contraseña>>
3	<< una vez ingresado los datos>>	se << visualiza el usuario creado>>
4	<<Luego de seleccionar el usuario>>	Debe << modificar los campos nombre y contraseña>>
5	<<Administrador guarda los cambios>>	<< se actualiza los campos modificado>>

Tabla 44 Planificación de ajustes

Identificar Tareas

Lista de Tareas por cada proceso

HU01
Tar1.1- Elaborar la estructura del inicio del sistema.
Tar1.2- Diseñar la estructura del sistema

Tabla 45 Lista de tareas de inicio de sistema

HU02
Tar2.1- Ingresar un nuevo registro al sistema
Tar2.2- Ingresar los parámetros de necesarios para el registro
Tar2.3- Guardar el registro ingresado

Tabla 46 Lista de ingreso de nuevo registro

HU03
Tar3.1- Evaluar los registros ingresados
Tar3.2- Seleccionar el registro
Tar3.3- Evaluar los controles, objetivos y dominios de cada registro ingresado

Tabla 47 Lista de tareas evaluar registros ingresados

HU04
Tar4.1- actualizar registro ingresado
Tar4.2- Seleccionar el registro para actualizar
Tar4.3- Actualizar los controles, objetivos y dominios del registro evaluado

Tabla 48 Lista de tareas de actualización de registro

HU05
Tar5.1- Panel de administrador
Tar5.2- Crear y modificar usuarios para el sistema.

Tabla 49 Lista de tareas de ajustes

Anexo 5: Diseño

INTERFAZ DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Figura 15 Ingreso al sistema

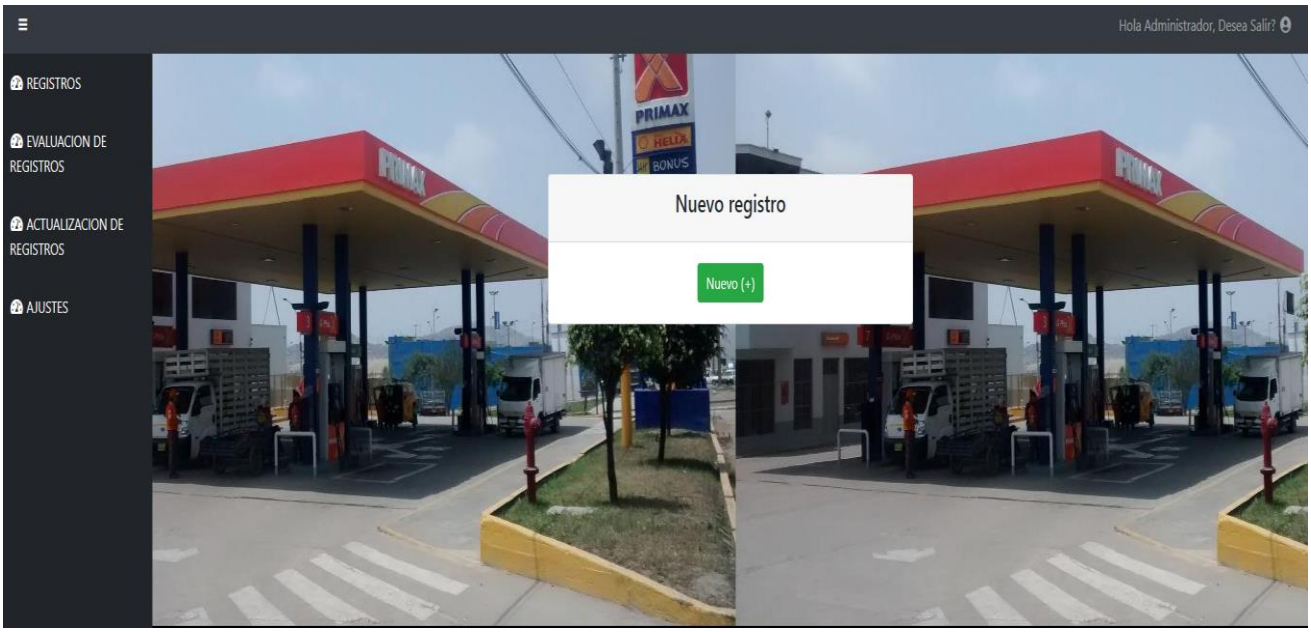


Figura 16 Página principal del sistema

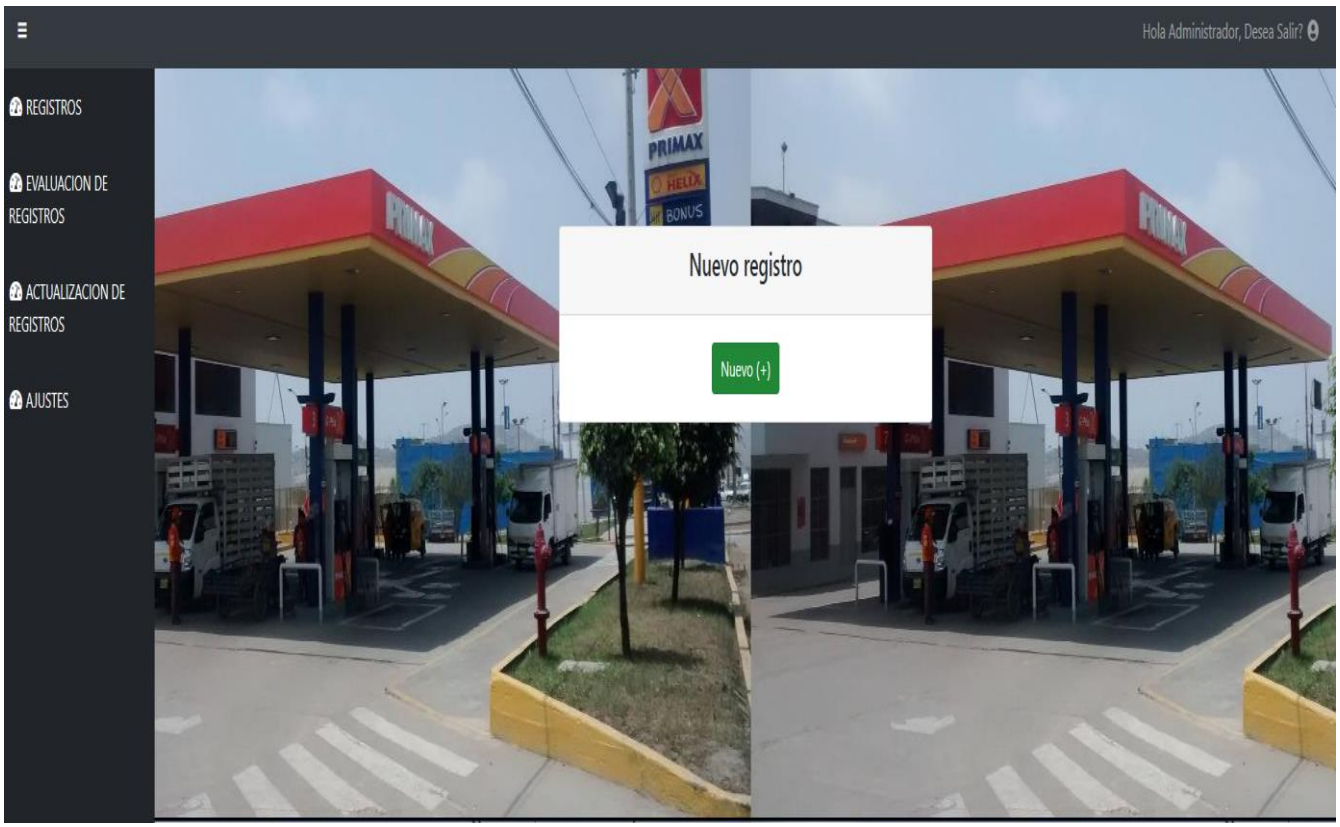


Figura 17 Ingreso de un nuevo registro

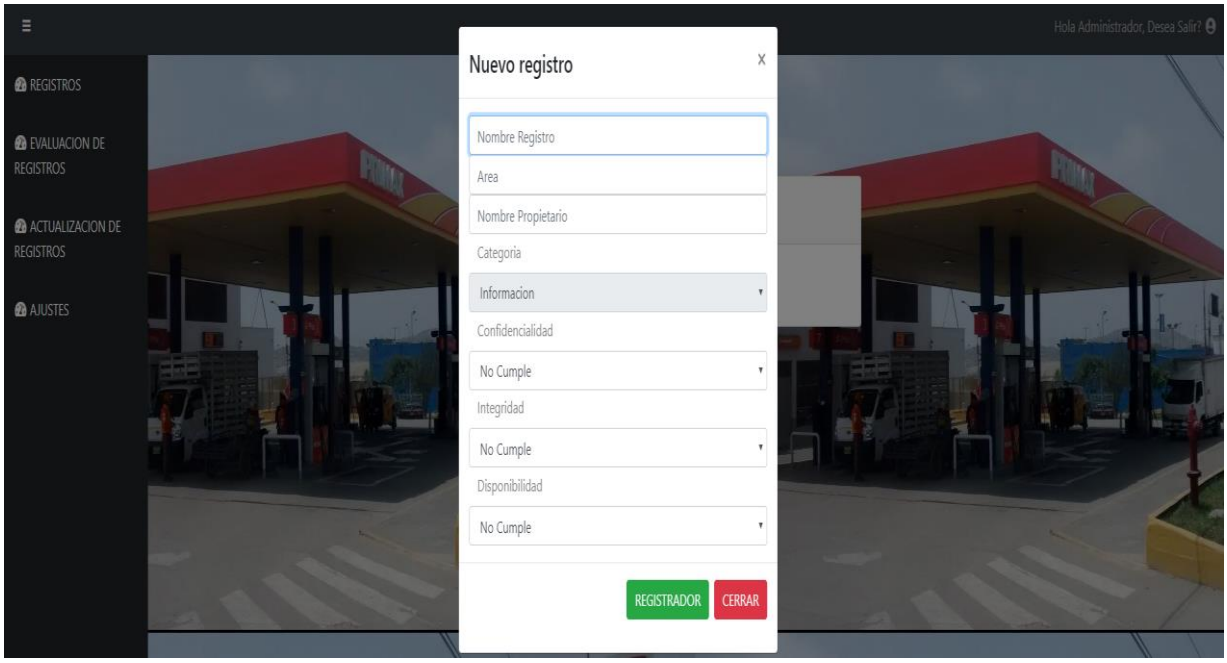


Figura 18 Ingreso de parámetros de nuevo registro

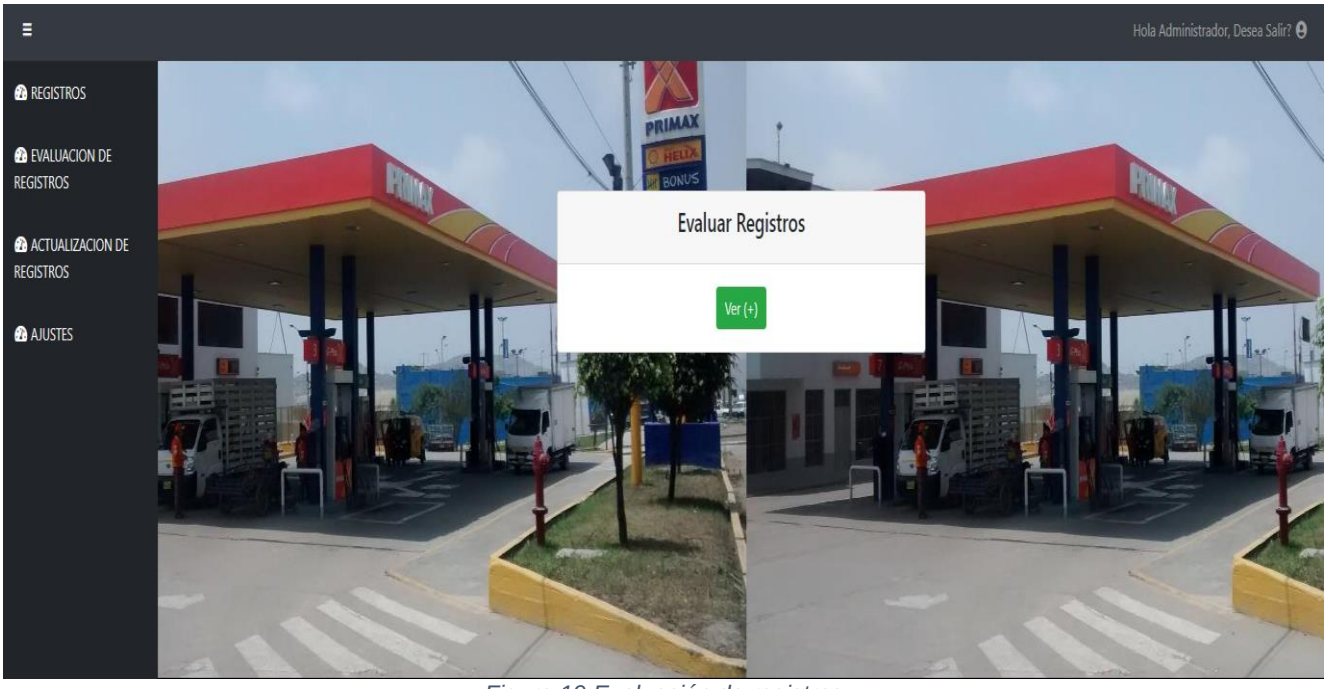


Figura 19 Evaluación de registros

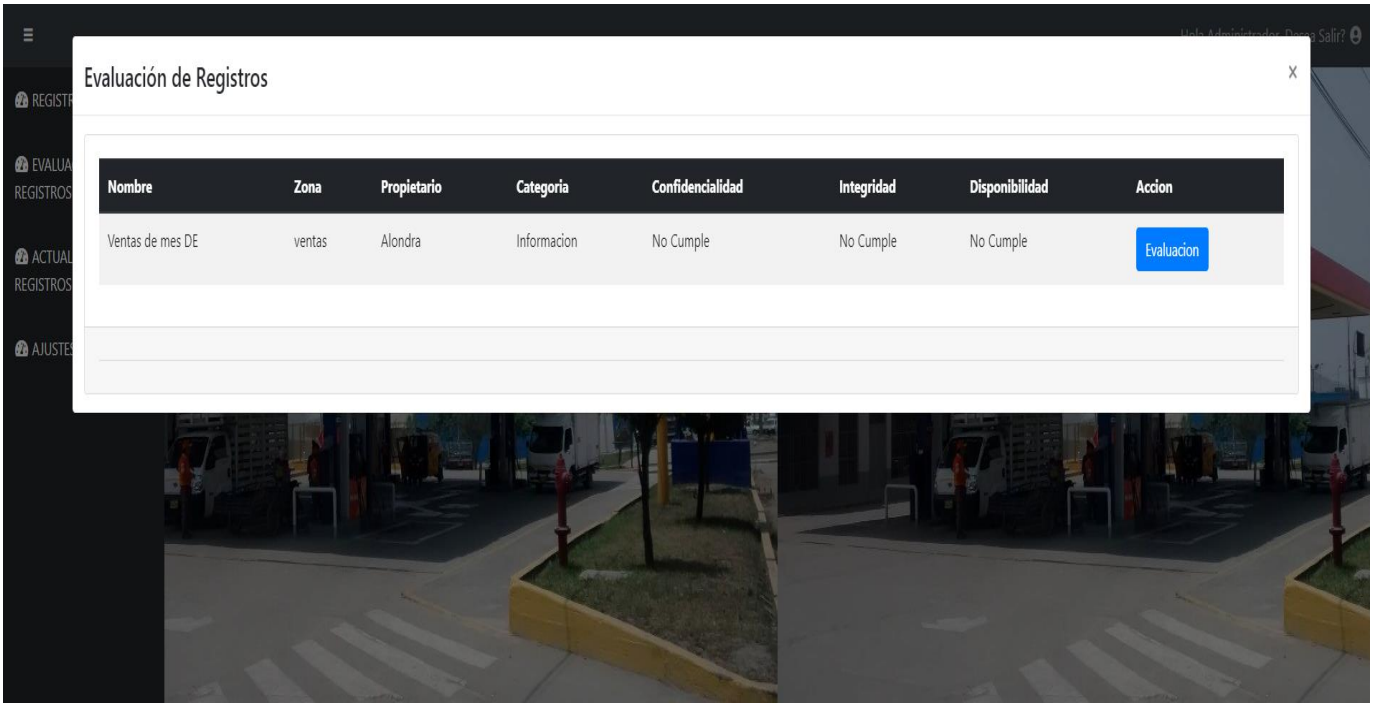


Figura 20 Selección de registro a evaluar

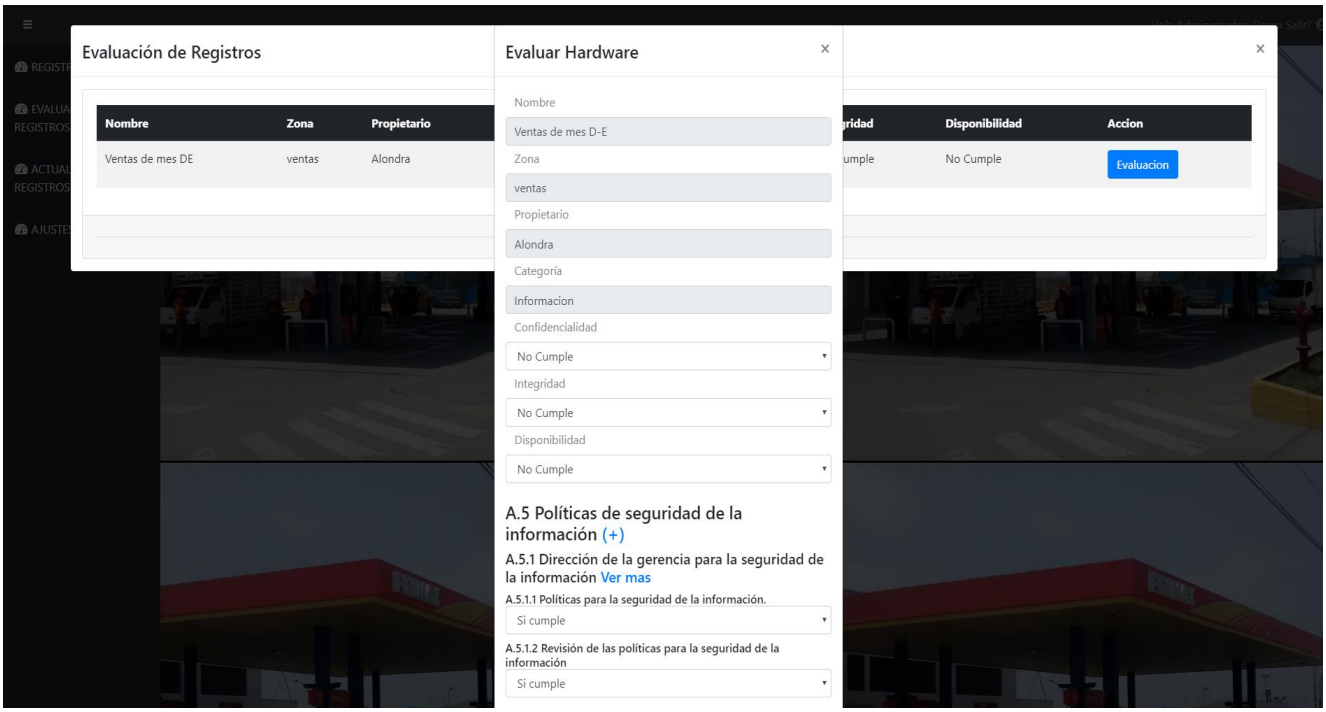


Figura 21 Selección de controles de evaluación

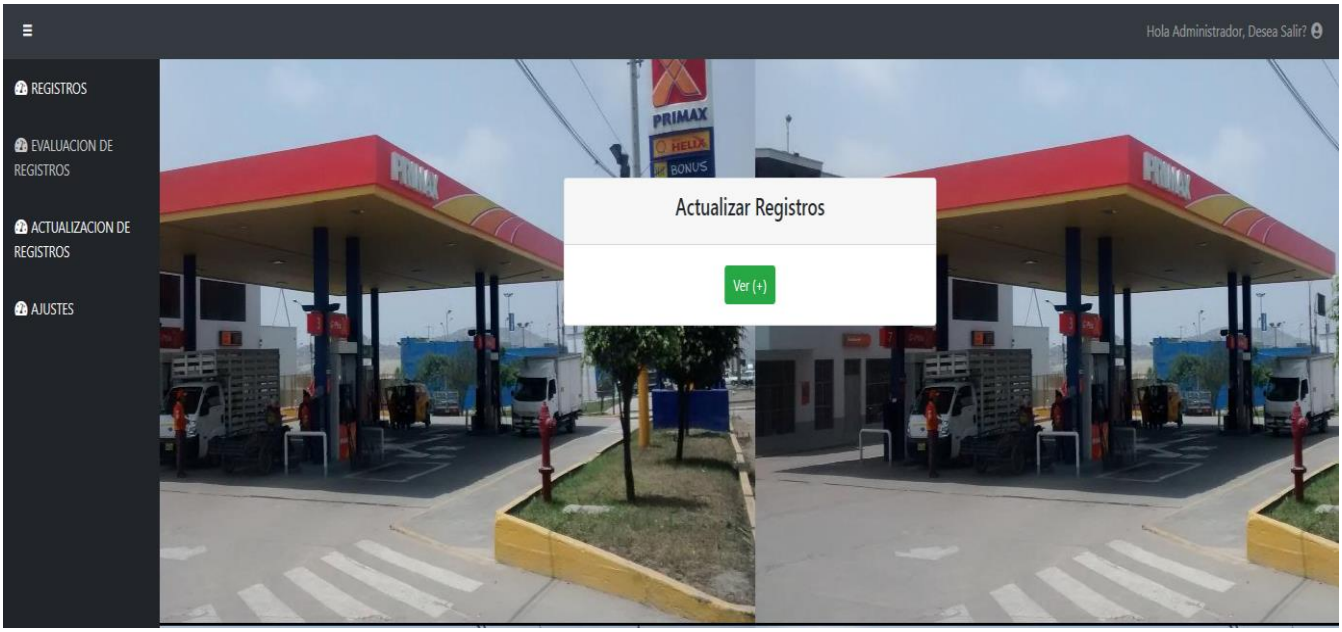


Figura 22 Actualización de registros

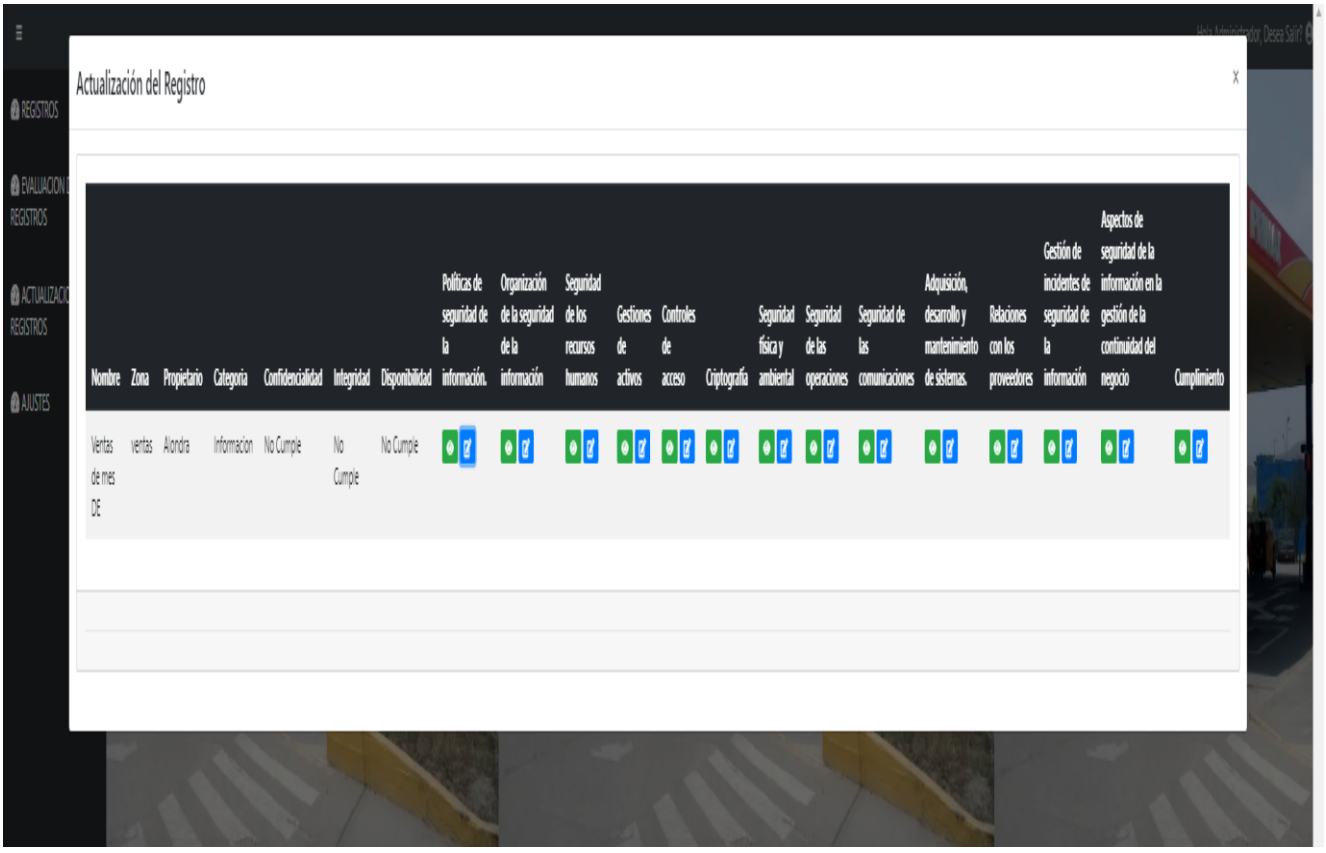


Figura 23 Visualización y actualización de los registros

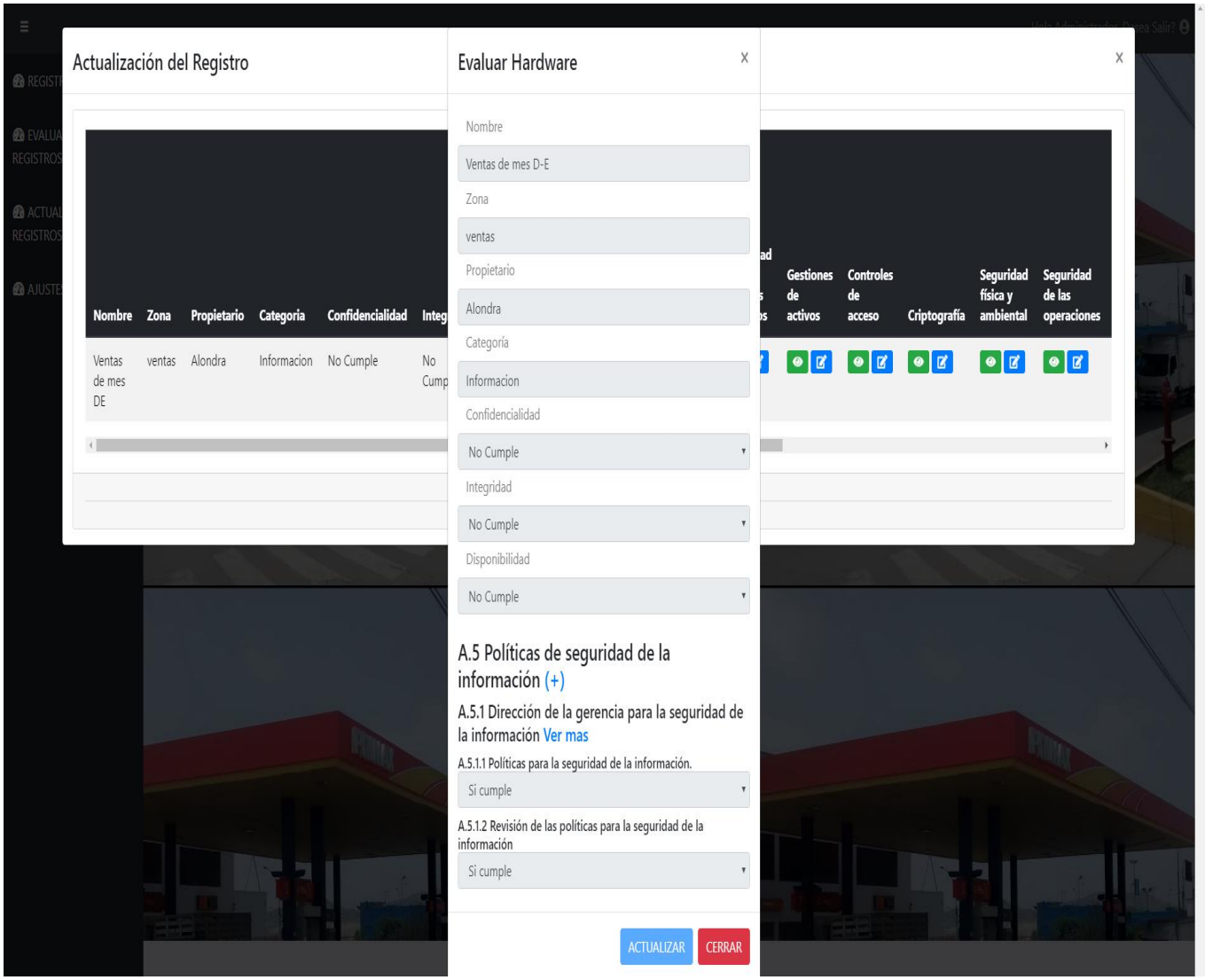


Figura 24 Visualización del estado del registro

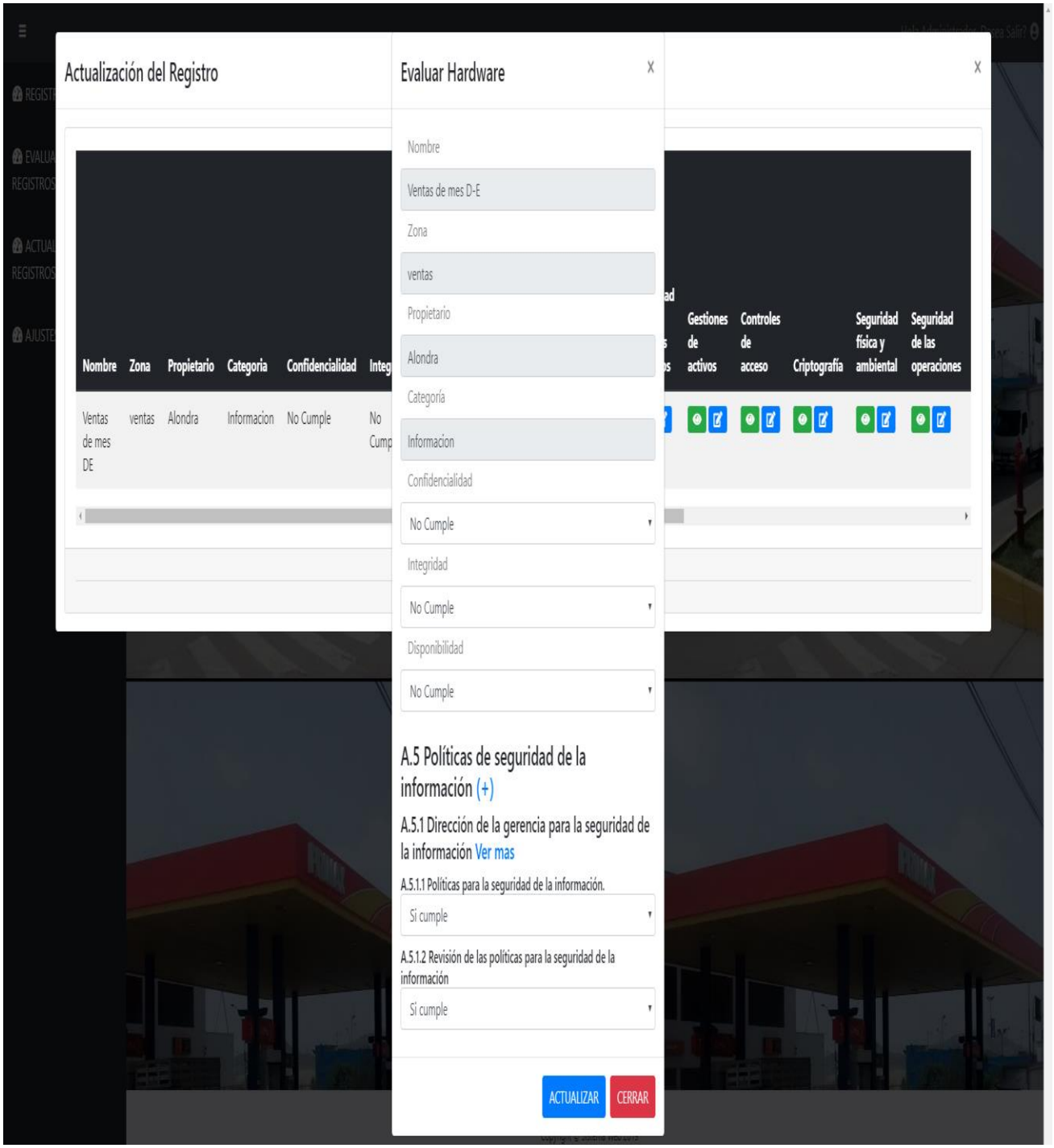


Figura 25 Actualización del estado del registro

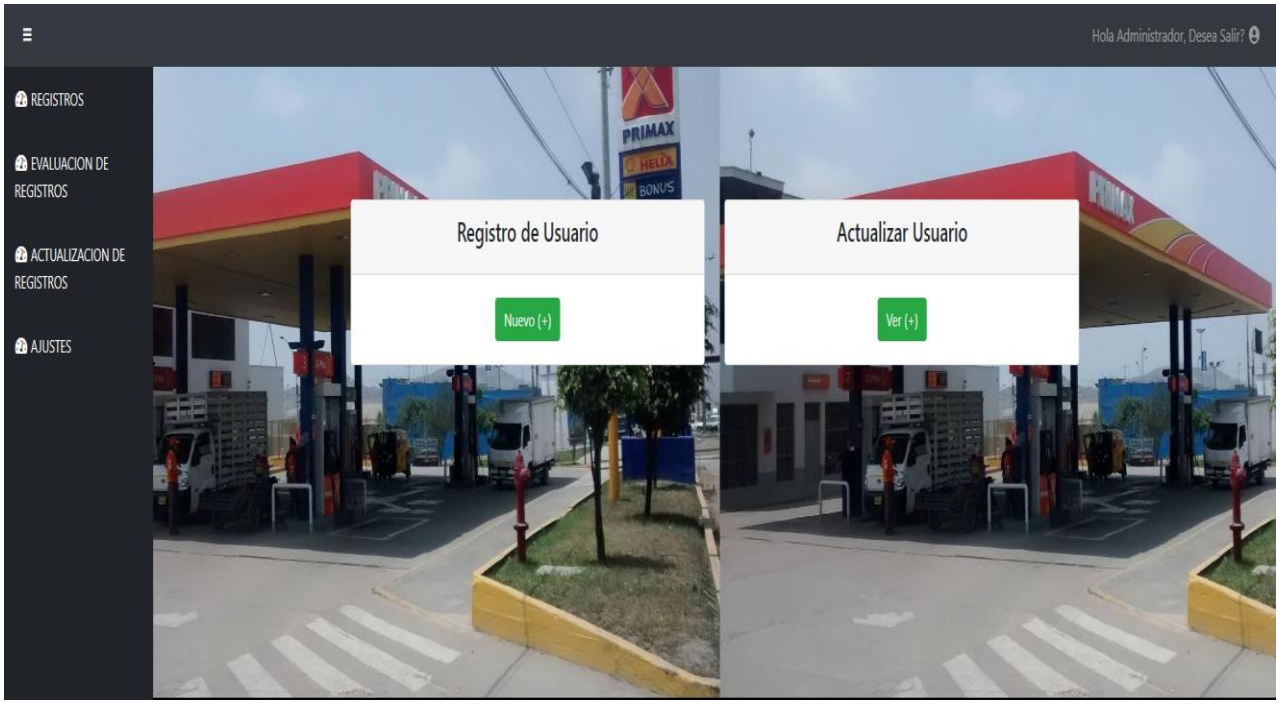


Figura 26 AJUSTES - Registrar y Actualizar usuarios

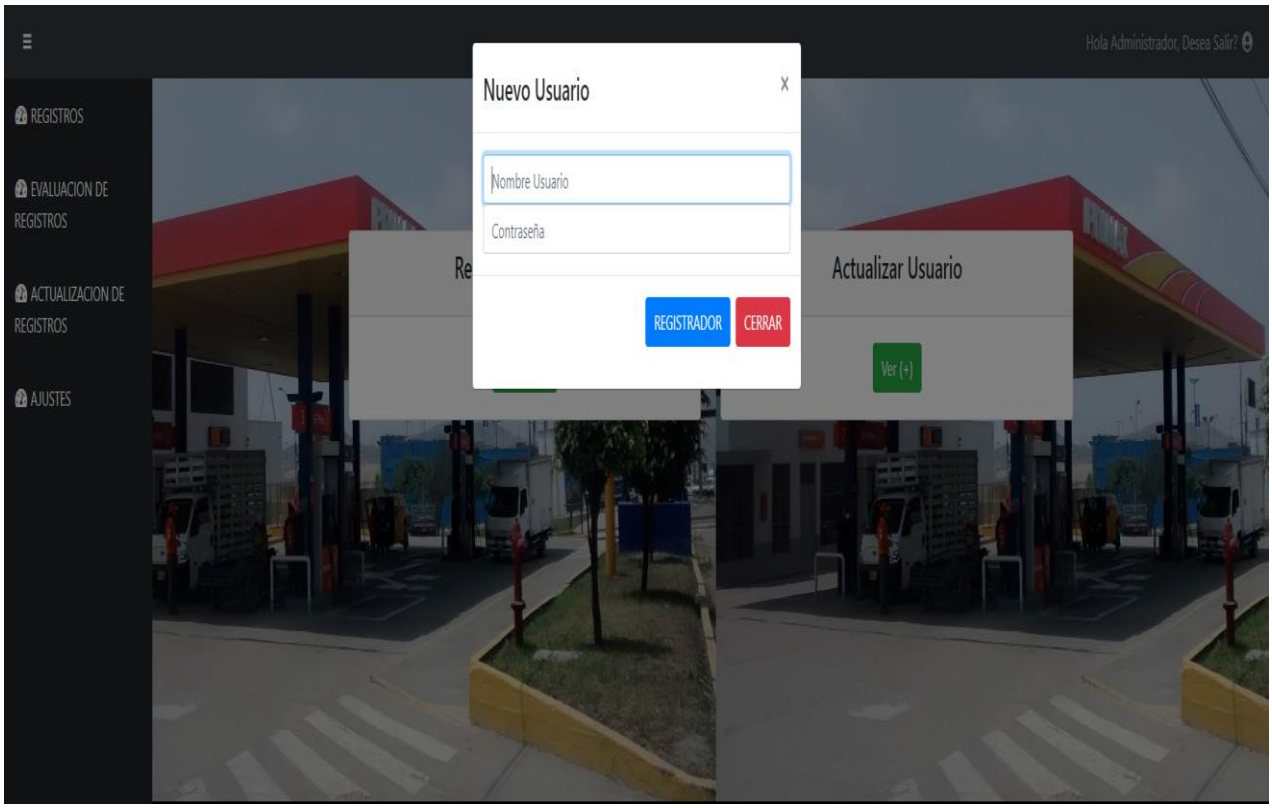


Figura 27 Registro de usuario

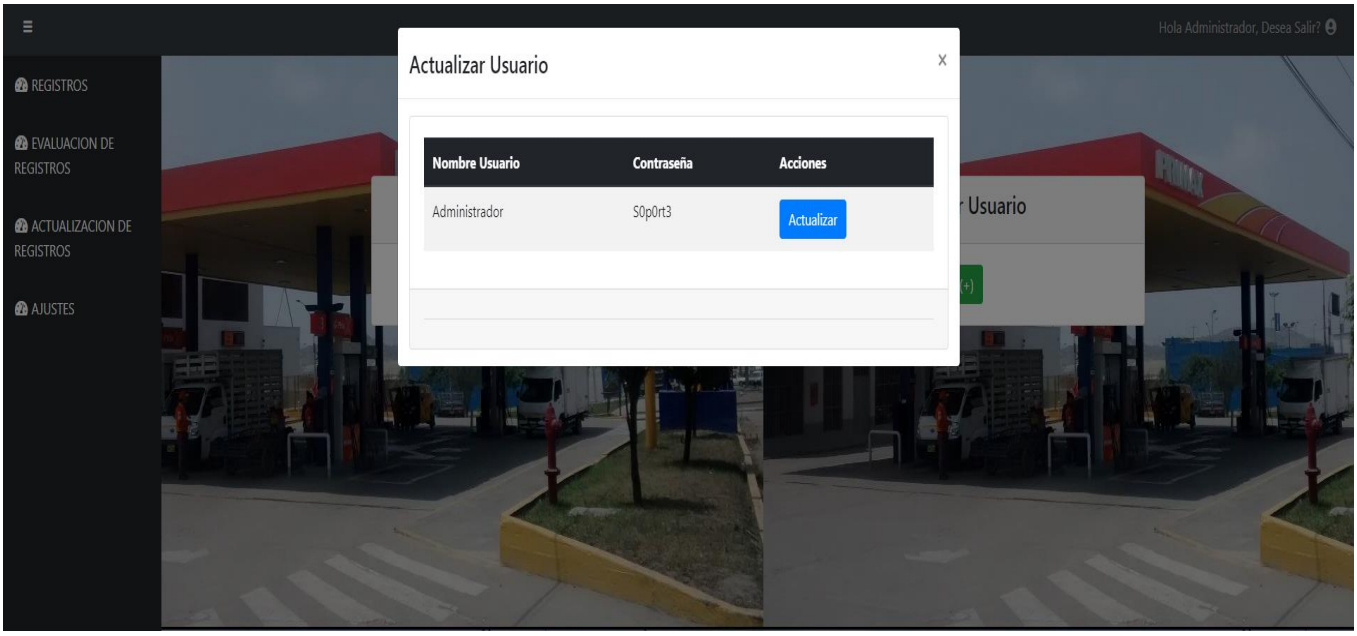


Figura 28 Actualizar usuario

Anexo 6: Carta de autorización

Lima, 20 de Julio del 2021

CARTA DE AUTORIZACION DE MANEJO DE DATOS

Yo LUIS CESAR ENRIQUEZ VENTURA con Nro. De DNI 10040852 en pleno uso de mis facultades legales e intelectuales, por este medio doy mi autorización a los estudiantes Luis Miguel Huamani Cahuana y Alexander Jesus Cruz Ruiz de la carrera de Ing. De Sistemas de la Universidad Cesar Vallejo – Lima Este, para el manejo de uso de los datos de la empresa para el desarrollo y publicación de su tesis.

ZEPPELIN
INVERSIONES GENERALES S.R.L.
Luis Cesar Enriquez Ventura
GERENTE GENERAL

LUIS CESAR ENRIQUEZ VENTURA
DNI: 10040852