UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de un plan de control y seguridad de los activos de información en la Estación de Servicios San José

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO DE SISTEMAS

AUTOR:

Chira Castillo, Gabriella Lucia (ORCID:0000-0003-4551-6839)

ASESOR:

Mg. Nizama Reyes, Mario Enrique (ORCID: 0000-0001-5598-0606)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

PIURA – PERÚ

2021

Dedicatoria

Dedico esta tesis a mi madre por haberme ayudado e incentivado en el día a día, a Dios por su amor eterno, a mi familia por su paciencia y apoyo incondicional y porque son el motivo de mi esfuerzo y superación.

Agradecimiento

Agradezco a Dios por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño anhelado y, de una manera muy especial a la gerencia y al personal de la Estación de Servicios San José – Piura quienes sin su apoyo no hubiera sido posible el desarrollo de esta investigación.

Índice de contenido

Índice de Tablas

Índice de Ilustraciones

Resumen

El presente estudio titulado “Implementación de un plan de control y seguridad de los activos de información en la Estación de Servicios San José” se planteó como objetivo general el Implementar un plan de control y seguridad basado en la metodología Cobit para la mejora de los activos de información en la Estación de Servicios San José
La investigación de tipo cuasi experimental con un solo grupo. Se trabajó con una muestra de 13 personas (gerente y personal de la estación de servicios) a quienes se les aplico dos cuestionarios sobre aceptación del plan de control y sobre eficiencia en toma de decisiones. Además se aplicaron guías de observación para identificar problemas en errores de digitación facturación y caídas del servidor; cuyos análisis e interpretación permitió diseñar e implementar un plan de control y seguridad, concluyéndose que la implementación del plan permitió en efecto reducir los errores en el proceso de facturación logrando una reducción considerable en el número de facturas rechazadas de 9.3% (15 facturas) a 4.1% (07 facturas) , asimismo se logró minimizar la cantidad de caídas del servidor que maneja el sistema de la organización, reduciendo el tiempo de interrupción que inicialmente ocurría entre 10 minutos - 4 horas a un promedio de 5 minutos en el día; también se permitió controlar la emisión de vales emitidos, pasando de 200 vales devueltos (de un total de 2000 vales visados) a 25 vales (de un total de 2025) devueltos tras la aplicación del plan. El personal demostró un buen nivel de aceptación del plan de control y seguridad y se logró que la gerencia tome decisiones basada en la eficiencia del plan de control y seguridad implementado.

Palabras claves: Plan de control y seguridad, metodología Cobit, activos de información, estación de servicios

Abstract

The present study entitled "Implementation of a control and security plan for information assets at the San José service station" had as its general objective the implementation of a control and security plan based on the Cobit methodology for the improvement of assets. information at the San José service station

Quasi-experimental research with a single group. We worked with a sample of 13 people (service station manager and staff) to whom two questionnaires were applied on acceptance of the control plan and on efficiency in decision making. In addition, observation guides were applied to identify problems in billing typing errors and server crashes; whose analysis and interpretation allowed the design and implementation of a control and security plan, concluding that the implementation of the plan allowed in effect to reduce errors in the billing process, achieving a considerable reduction in the number of rejected invoices from 9.3% (15 invoices) to 4.1% (07 invoices), it was also possible to minimize the number of server crashes handled by the organization's system, reducing the interruption time that initially occurred between 10 minutes - 4 hours to an average of 5 minutes a day; It was also possible to control the issuance of issued vouchers, going from 200 returned vouchers (of a total of 2,000 endorsed vouchers) to 25 vouchers (of a total of 2,025) returned after the application of the plan. The staff demonstrated a good level of acceptance of the control and security plan and management was able to make decisions based on the efficiency of the control and security plan implemented.

Keywords: Control and security plan, Cobit methodology, information assets, service station

I. INTRODUCCIÓN

Actualmente al hablar acerca de seguridad de la información debemos ser conscientes de lo que significa debido a que este término es común en todas las empresas y se verán a lo largo de esta tesis.

La presente tesis está basada en el conocimiento adquirido para implementar un plan de control y seguridad, tomando como base estándares internacionales., considerando la importancia de implementar lo que es un gobierno de las tecnologías de información.

El manejo de información abarca desde la documentación hasta el proceso de almacenaje, denominándose a ello gestión documental, estando involucrados tanto los sistemas internos de la organización como externos a ella, los cuales están en la obligación de brindar información considerando aspectos relevantes como la forma en la que se almacena dicha información, respaldo de la información y los planes de contingencia.

Una cantidad de organizaciones ignoran la dimensión de la problemática y consideran a la seguridad como algo secundario y en la gran mayoría no se da la oportunidad de inversión necesaria para la prevención de la pérdida de información que actualmente con el avance de la tecnología está expuesta.

La seguridad se caracteriza por la confidencialidad, integridad y disponibilidad cuyas amenazas pueden ser internas o externas, de origen accidental o premeditado pudiendo generar en la empresa u organización problemas, de paralización de sus actividades, conllevando ello a pérdidas en su producción y en su economía, ambos importantes para su desarrollo.

Por lo expuesto, la empresa Estación de Servicios San José en la actualidad no posee un plan de seguridad y control de la información con el propósito de mitigar las amenazas, riesgos y vulnerabilidades que con frecuencia está expuesta la información de le empresa; no se han propuesto planes considerando estándares que minimicen los delitos informáticos o amenazas a los que están expuestos la información comprometiendo su confidencialidad, la integridad y disponibilidad. La empresa posee muchas deficiencias en el manejo

de la información, pues en su continuo crecimiento, no se ha dado la importancia debida a salvaguardar la información que continúa manejándose.

Una de las principales amenazas, es el factor humano dentro de la organización cuya información está al alcance de los trabajadores del área de grifos, siendo el tipo de amenaza donde se invierte grandes recursos para su control .Se considera los actos malintencionados como en la variación de información, negligencia, falta de control, incurrir en incumplimiento de las medidas de seguridad, accesos no autorizados, bien de manera accidental, curiosidad, desafío personal u otras razones o motivaciones..

En lo que respecta a las amenazas por software, se consideran la posibilidad de fallas en el sistema operativo, software vulnerable por deficiencias en su diseño, asimismo la existencia de una gran cantidad de software mal intencionado lo que representa amenazas latentes en la organización. Asimismo, la red; los dos errores más comunes que se detectan son la interrupción de la red y la posible extracción de datos a través de esta.

La información de la organización está llamada a vulnerabilidades físicas, como por ejemplo, el lugar de la instalación de los equipos de sistemas (Computadoras, Servidores y otros) de no poseer ventilación adecuada o ambientación controlada, as como desastres naturales entre otros.

El problema presentado en la organización mencionada está relacionado con la forma de manejo de información ya sea en el área de los grifos y el área de Rent A Car, el acceso a internet de los empleados de la organización hace que la información de la empresa se vea reflejada en personas externas a la misma, así mismo el manejo de los equipos, servidores y problemas que presentan en su vida útil mientras se maneja datos y registros.

El tema de facturación de ambos establecimientos también es un problema constante por los errores ya sean de las mismas personas administrativas o error de los sistemas implementados que ocasionan desestabilidad en los procesos. En base al trabajo de investigación la empresa no podría continuar con sus funciones, más aún cuando hablamos de empresas cuyos procesos en

total son automáticos por lo cual la seguridad siempre es tema de discusión, varias organizaciones fracasan por este punto importante.

Debido a esto; hoy en día se necesita que todas las empresas se constituyan en base a la confidencialidad, integridad y disponibilidad y los empleados de las mismas tengan parámetros de seguridad establecidos en los procesos. Ante esto la seguridad se debe dar por ayuda entre las personas encargadas de la misma las cuales disponen de las medidas que se encuentran a su alcance y utilizar los recursos de la organización, ante la presencia de inconveniente que comprometan su seguridad. Según lo descrito esta responsabilidad recae en el personal encargado de mantener a salvo la seguridad de la información de la empresa, mediante la implementación de mecanismos o procedimientos de actuación que efectivicen las medidas técnicas informáticas adoptadas de acuerdo a estándares de normatividad en cuanto a seguridad.

Para todo esto, surge la necesidad de políticas reguladoras de buenas prácticas de los procesos de la organización y recursos relacionados con la información, teniendo en cuenta los activos que también están ligados de una u otra manera a este proceso. De no realizar dentro de sus sistemas estos procedimientos toda la información estará expuesta sin duda alguna a sufrir la sustracción de información, eliminación, modificación o denegación de servicios entre otros.

Ante ello se formula la interrogante de investigación ¿De qué manera influye la implementación de un plan de control y seguridad basado en la metodología Cobit en los activos de información en la Estación de Servicios San José? y como preguntas específicas se tiene ¿Cómo se reduce la cantidad de errores que se presentan a diario en el proceso de facturación?, ¿Cómo se minimiza la cantidad de caídas del servidor que maneja el sistema de la organización?, ¿Cómo se controla la emisión de vales emitidos visados por el área administrativa?, ¿Cómo se eleva el grado de aceptación del personal con la gestión de control implementada en Estación de Servicios San José?, ¿Cómo se incrementa la eficiencia en la toma de decisiones de los altos ejecutivos?

La justificación de la presente investigación dada en la empresa Estación De Servicios San José SAC, cuenta con negocios en crecimiento dedicándose al

rubro de combustibles y alquiler de vehículos cuyos procesos que se realizan están en constantes crecimiento de los cuales depende el buen funcionamiento administrativo. La información se encuentra en toda la empresa desde el personal administrativo, en correos electrónicos y en formato físico, se puede concluir que no se han establecido políticas de fiscalización que realicen un buen cuidado de este activo como es la información de la empresa. Por ello la empresa deben considerar en su plan de trabajo el aseguramiento de la información mediante políticas de control para poder garantizar la continuidad de la información de manera segura acorde con los estándares actuales y para ello se debe tener en cuenta el análisis de riesgos que deberá ser motivo de estudio de la información de la empresa.

Como objetivo general se plantea Implementar un plan de control y seguridad basado en la metodología Cobit para la mejora de los activos de información en la Estación de Servicios San José y como objetivos específicos Reducir la cantidad de errores que se presentan a diario en el proceso de facturación, Minimizar la cantidad de caídas del servidor que maneja el sistema de la organización, Controlar la emisión de vales emitidos visados por el área administrativa, Elevar el grado de aceptación del personal con la gestión de control implementada en Estación de Servicios San José, Incrementar la eficiencia en la toma de decisiones de los altos ejecutivos.

Finalmente se plantea la hipótesis: Mediante la metodología COBIT es viable la implementación del plan de control y seguridad de los activos de información en la Estación de Servicios San José.

II. MARCO TEÓRICO

En lo que respecta a los antecedentes que sustentan la presente investigación se consideró referentes internacionales, nacionales y locales.

En el contexto internacional Perafán Ruiz (2014) con su tesis “Análisis de riesgo de la seguridad de la información para la institución universitaria Colegio Mayor del Cauca, Universidad Nacional Abierta y a Distancia”, cuyo objetivo general fue realizar el análisis de riesgos para la generación de controles que minimicen la probabilidad de ocurrencia e impacto de los riesgos. La metodología de la investigación fue de tipo aplicada, ejecutando el análisis de riesgo mediante el ciclo de mejora PHVA, la población considerada fueron los activos de información. En cuanto a los resultados se determinó el incumplimiento con el mantenimiento preventivo del hardware, no existe procedimientos definidos para ello; en software no hay control de las instalaciones, ni procedimientos definidos de actualizaciones; en redes los sistemas de protección perimetral requieren de renovación anual, así como un inadecuado estado del cableado estructurado en la sede principal.

Con respecto a los antecedentes nacionales Aguirre Mollehuanca (2014) en la tesis “Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A”, el objetivo general fue el diseño un sistema de gestión para la seguridad de la información en la mencionada institución. La metodología de investigación, es tipo aplicada, nivel descriptivo; como metodología de desarrollo para el proyecto se utilizó la guía PMBOK de PMI y el ciclo de Deming PDCA. En los resultados, se identificaron los activos de información, procediendo a su valoración, identificación, evaluación y tratamiento de los riesgos. Asimismo, se elaboró una matriz de riesgos con su respectiva declaración de aplicabilidad. Se concluye la necesidad de difundir las normas de seguridad, así como la necesidad de contratar personal especializado para soporte de estos procesos.

Ramos Arca (2015) con la tesis “Propuesta de un plan de auditoria informática para el sistema de información en salud y el aplicativo para el registro de formatos SIS en los establecimientos de salud de la unidad ejecutora 400 en la

región Piura en el año 2015", cuyo objetivo general fue proponer un plan de auditoria informática en un establecimiento de salud. La metodología de investigación, fue tipo no aplicada, nivel descriptivo propositivo; como metodología se consideró como base el marco normativo peruano. En sus resultados propuso un plan de auditoría informática, mediante una aplicación sistematizada para el registro de Formatos SIS, con el propósito de que sea una guía para las auditorías a los sistemas informáticos del estado basado en la normatividad. Debido a que Contraloría General del estado peruano, no poseía una normatividad explicita, como guía de auditorías de sistemas informáticos, se consideró las buenas prácticas o estándares internacionales, relacionadas con la temática; con el fin de evaluar controles para utilizar en los procesos informáticos de las entidades públicas del estado, para lograr minimizar riesgos que afecten alcanzar los objetivos y propuestas por la institución. Asimismo, se determinó las documentaciones aplicables por un auditor a un plan de auditoría informática.

Miranda-Vásquez (2013), desarrolló la investigación "Guía metodológica para implementar un sistema de gestión de seguridad en instituciones", siendo el objetivo general el desarrollo de una guía metodológica para la implementación de un sistema de gestión de seguridad. La metodología de investigación, es de tipo no aplicada, nivel descriptivo propositivo; como metodología de desarrollo se consideró como base el marco normativo peruano. En sus resultados se midió el desempeño en la empresa 1, considerándose como métricas la cantidad de incidentes cerrados respecto a los reportados, porcentaje de colaboradores que aprobaron las charlas, porcentaje de controles implementados en una determinada fecha; en la empresa 2 se aplicó como estrategia mini charlas de 05 minutos de reforzamiento en temas de seguridad en el lugar, lo cual ayudo a fortalecer el tema de seguridad.

Por tanto, Villena Aguilar (2016) realizó la tesis "Sistema de gestión de seguridad de información para una Institución Financiera", cuyo objetivo general fue el establecimiento de lineamientos principales para la implementación exitosa en una institución financiera en el Perú de un sistema de gestión de seguridad de

información (SGSI). En los resultados se planteó un SGSI considerando 05 dominios, tales como administración de riesgos, gobierno de la seguridad de la información, administración de un programa de seguridad de la información, gestión de la seguridad de la información y administración de respuestas a incidentes. Se concluye que el proyecto logra la propuesta de controles para uniformizar y la mejora de los procesos de las instituciones, aplicando conceptualizaciones de seguridad de la información.

Como soporte teórico relacionado con la investigación, se desarrolla las definiciones de la variable en estudio.

En cuanto al control de los activos de información, según el artículo de Anastacio Cortez & Osorio Quijandría (2018), en las organizaciones se ha desbordado la gran cantidad de información digital debido a su crecimiento de manera exponencial, comprometiendo su capacidad de gestión. Asimismo, según Oscar Alcides (2018), los clientes, proveedores, socios y demás interesados se han vuelto cada vez más exigentes en cuanto a servicios rápidos, eficiencia en resultados. En las organizaciones los directivos no cuentan con información idónea para la toma de decisiones y con ello proponer estrategias de acorde al contexto del negocio, asimismo el personal enfrenta cada vez más problemas para poseer información oportuna, debido a la falta de evidencia digital en cada uno de los procesos en los que se involucra los activos de información, para presentar a los auditores, no consiguiendo toda la información acerca de los clientes, socios, proveedores y otros más involucrados en el negocio (Tejena-Macías, 2014). Son las organizaciones que no sean capaces de gestionar la información en un futuro, las que no serán competitivas perdiendo productividad en un mercado global (Castro Siguas, 2017).

Según Mesa Palacios y otros (Mesa Palacios, Serra Toledo, & Fleitas Triana, 2018), en una organización para gestionar en forma adecuada los activos de información, es menester su identificación en forma precisa y detallada, validando a detalle cada una de las características necesarias de su información.

Se definen las siguientes fases: Fase I: Identificación de activos, la misma que

busca identificar que no es un activo de información, considerando todos los recursos, verificar sus características y que los datos sean administrados, procesados y almacenados. Fase II: Clasificación de activos, consiste en analizar cada activo de información cuyas características a tener en cuenta, considerando como una métrica guía en función de la información más relevante para la empresa. De esta manera se obtiene la clasificación de los activos, la misma que debe incluir mecanismos para una constante actualización. Fase III: Análisis del riesgo en los activos de información, es importante que cada uno de los activos de información pase por la evaluación de dos importantes etapas las cuales son la identificación y medición. Fase IV: Gestión de activos, comprende la clasificación de los activos de información, con el que logra determinar del porcentaje de vulnerabilidad con respecto al riesgo, emitiendo así reportes tales como: informe de logros, informe de riesgo, informe de resultados, así como plan de mitigación integral. Fase V: Seguimiento del plan de mitigación integral, corresponde al cumplimiento de los planes de mitigación aprobados, esto lleva a determinar desviaciones en forma preventiva, presentándolos en la alta gerencia para la evaluación del impacto de las desviaciones en contraste con la sensibilidad de la información a proteger (Carolina Nieves, 2017).

Con el propósito de la determinación de las implicaciones de seguridad y los controles requeridos para la protección de los activos de información del acceso de terceros; estos podrían ser. Proceso para determinación si hay mayor vulnerabilidad de los activos y/o perdida de información, disponibilidad de servicio, detalle de obligaciones de las partes en los contratos, verificación en forma constante de hardware y software, controles acerca del acceso a terceros en la organización, acuerdos y definiciones de requerimientos y controles de seguridad en los contratos. Para esto deben estar contenidos que y de qué manera será garantizado los requerimientos de seguridad de la información (Guerrero Julio, 2010).

Cuando hablamos de seguridad, significa carencia de amenazas, esta situación actualmente es muy difícil de mantener ya que todas las organizaciones son organizaciones de riesgo. El componente riesgo es permanente en ellas es por

eso que no podemos decir que la seguridad no puede estar con ausencia de amenaza (Castellaro, Romaniz, Ramos, Feck, & Gaspoz, 2016).

El SGSI es un conjunto de procesos que permiten el establecimiento, implementación, mantenimiento y mejoramiento de forma continua de la seguridad de la información, considerando los riesgos latentes en la organización. Su implantación presume establecer procesos formales y una definición precisa de responsabilidades basado en políticas, planes y procedimientos cuya implementación debe documentarse de manera apropiada (Berrío, Montoya Pérez, Pérez Zapata, & Jiménez Builes, 2016). El objetivo principal del SGSI es el establecimiento de los alineamientos para gestionar los recursos tecnológicos logrando con ello controlar las vulnerabilidades y amenazas a los activos de información, controlar el manejo del esquema de control interno, disminución de riesgos en los activos de información y elaborar los planes de corrección a través de los esquemas de control (Mero García, 2016).

El plan de control y seguridad normalmente se ve obligado a proteger el derecho de acceso a la información mediante los procesos de control. Este proceso nos da lugar a entender que estos operadores tienen solo la exclusividad de accesos a áreas establecidas (Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018).

A medida que funcionan las organizaciones, se crea la necesidad de contar con un marco referencial concerniente a la seguridad y control de la información. Las organizaciones deben tener conocimiento de la importancia básica de los riesgos y limitaciones de las tecnologías de información en toda la organización identificando posibles riesgos, de acorde a lo señalado por COBIT, la cual es una herramienta que ha ayudado al gobierno de TI y modificando la manera en que trabajan los profesionales de TI. COBIT, se basa en las buenas prácticas para controlar riesgos del negocio dando así lugar al desarrollo de políticas de control de las tecnologías de toda la organización. Los principios de Cobit en referencia a su desarrollo es ofrecer un marco aplicable de referencia integral único cubriendo la empresa de extremo a extremo y la satisfacción de las

necesidades de las partes interesadas (Steuperaert, 2019).

Según De Haes, Van Grembergen, Joshi, & Huygh (2019) COBIT, al orientarse a todos los procesos de una organización, lo que busca es auditar los procesos y el control de todos los sistemas de información, funcionando, así como un modelo de monitoreo que abarcan la información del negocio y control de la seguridad especifica desde una perspectiva de negocio. Según León Acurio y otros (2018), entre los beneficios del Cobit se tiene: Alineación de acuerdo al negocio, mejora la visión de las TI para su administración, lineamiento especifico de responsabilidades, accesibilidad con propios y entes reguladores. Las tecnologías de la información son el enfoque principal de COBIT, COBIT está basado en 34 objetivos de control generales, cuyos procesos están agrupados en cuatro grandes dominios, toma en cuenta actuales tendencias de gobierno y administración, origina nuevos modelos de referencia en base a las nuevas TI.

La investigación se realizó en la empresa Estación de Servicios San José, tomando en cuenta los siguientes fundamentos: fundada en 1993 en Piura, con un sólido respaldo patrimonial y financiero cuenta con grifos a nivel nacional y alquiler de vehículos en la ciudad de Piura, Talara, Chiclayo, Tumbes, Trujillo y Lima. A mediados de los años 90, un grupo de piuranos, constituyeron una empresa de distribución de combustibles y alquiler de vehículos de capital 100% peruano que competiría con grandes multinacionales, llevando energía y servicios de calidad a más peruanos. En el mes de setiembre de 1994, el Ministerio de Energía y Minas, otorgó el permiso para el inicio de operaciones, en julio de 1997, logrando realizar el primer despacho en el mes de octubre del mismo año. El profundo conocimiento del territorio peruano, sus necesidades y costumbres fueron el valor diferenciado frente a empresas extranjeras, para lograr generar credibilidad, empatía y confianza.

Actualmente Servicios San José cuentan con 6 grifos y sedes de alquiler de vehículos en el territorio nacional; personal técnico altamente calificado y la infraestructura idónea ofreciendo servicio de calidad a precios muy competitivos cumpliendo con las exigencias de nuestros clientes con un profundo respeto por el medio ambiente.

Según la página web de Estación de Servicios San José SAC (2017) su misión es “satisfacer las necesidades de transportes de sus clientes asegurándoles un trato referencial y personalizado, con las tarifas más económicas del mercado y con vehículos modernos, con vehículos que garanticen su tranquilidad, comodidad y seguridad total, tanto en su viaje de trabajo y/o placer”.

En tanto en su visión indica “consolidarnos como la empresa líder en el rubro de alquiler de vehículos, ofreciendo un servicio seguro y confiable en el mercado regional y nacional.”

Así mismo el principal objetivo según la página web es buscar constantemente y aplicar nuevas ideas, servicios, prácticas con el fin de mejorar procedimientos y alcanzar los objetivos de mejorar día a día de la satisfacción de nuestros clientes

Entre sus políticas generales de la institución podemos afirmar políticas Generales de la institución: Reafirmar la posición de liderazgo de Estación de Servicios San José SAC en el sector; lograr los objetivos planificados disponiendo de los recursos necesarios, lograr la satisfacción plena de los clientes, conociendo sus necesidades, cumplir con los requisitos legales y reglamentarios de los clientes, constituir un equipo profesional compacto e integrado a la filosofía de la empresa; atención de reclamaciones y sugerencias de los clientes y colaboradores, cumplimiento de objetivos de calidad, mediante la mejora continua de nuestras actuaciones y procesos, internalizar la calidad como base irrenunciable de nuestro comportamiento y el cumplimiento de los requisitos, alineado al cuidado del medio ambiente y ahorro de recursos.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

3.1.1. Tipo de investigación

La investigación es aplicativa, pues se plantea una solución, mediante la implementación de un plan de control y seguridad de los activos de información. El nivel de investigación es descriptivo, dado que se conoce y describe las actividades inmersas en el proceso de implementación de un plan de control y seguridad de los activos de información (Hernández Sampieri, Mendez Valencia, & Mendoza Torres, 2017).

3.1.2. Diseño de investigación:

Según Hernández Escobar y otros (2018), los diseños cuasi-experimentales que más se utilizan, siguen la misma lógica, involucrando la comparación de los grupos de tratamiento y control. En otros diseños, el grupo de tratamiento sirve como su propio control, comparando el "antes" con el "después", utilizando métodos y técnicas para medir su impacto.

G_1	-	O_1
G_1	X	O_2

G1: Grupo 1

O1: Observación 1 (Pre test)

O2: Observación 2 (Post test)

X: Solución

3.2 Variables, operacionalización

Variable dependiente: Control de activos de información

Definición conceptual:

Consiste en gestionar en forma adecuada los activos de información,

logrando su identificación en forma precisa y detallada, validando a detalle cada una de las características necesarias de su información (Mesa Palacios, Serra Toledo, & Fleitas Triana, 2018).

Definición operacional:

Mediante la aplicación de instrumentos como guías de observación en las dimensiones de errores de facturación, emisión de facturas y facturas rechazadas, se valora cada uno de sus indicadores antes y después de la de la implementación de un Plan de Control y Seguridad de los Activos de Información.

Dimensiones:

Errores de facturación, los indicadores son cantidad de facturas emitidas, Cantidad de facturas rechazadas y cantidad de errores en facturaciones

Caídas del servidor, los indicadores son tiempo de trabajo del servidor, tiempo de interrupción del servidor y tiempo funcionamiento del servidor

Emisión de vales, los indicadores son cantidad de vales emitidos, cantidad de vales utilizados y vales de combustible no utilizados

Variable independiente: Plan de control y seguridad

Definición conceptual:

El plan de control y seguridad normalmente, corresponde a proteger el derecho de acceso a la información mediante los procesos de control, dando lugar a entender que operadores tienen exclusividad de accesos a áreas establecidas dentro de la organización (Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018).

Definición operacional:

Mediante la aplicación de instrumentos como guías de observación a la dimensión de satisfacción, se valora cada uno de sus indicadores como Grado de satisfacción del personal administrativo y Grado de satisfacción de gerencia.

Dimensiones:

Satisfacción, los indicadores fueron grado de satisfacción del personal administrativo y grado de satisfacción de gerencia.

3.3 Población, muestra y muestreo

3.3.1. Población

La población estuvo conformada por el área administrativa de la Estación de Servicios San José, la cual está en constante intercambio de información diaria en los procesos de ventas y facturaciones que se prestan como principales servicios al consumidor. La población descrita está conformada por las siguientes personas

ÁREA GRIFO (ZONA PIURA)

CARGO	No
Gerente General	1
Administradora	1
Gerente de operaciones	1
Gerente comercial	1
Tesorería	1
Área de facturación	2
Caja chica	2
Almacén	2
Recursos humanos	2
TOTAL	**13**

3.3.2. Muestra

La población del área administrativa será igual a la muestra por conformar un grupo menor a 30 personas. Por lo tanto, la muestra será igual a la población es decir de 13 personas.

3.4 Técnicas e instrumentos de recolección de datos La observación

3.4.1. Técnicas

Para medir el indicador de la cantidad de errores en facturación diaria, se

utilizó la técnica de observación, basándose en los resultados obtenidos de la guía de observación N° 1. Este instrumento consideró la cantidad de errores que se producen en la facturación de la estación aplicándolo a los usuarios del área administrativa que es donde se realiza esta función. Este instrumento fue evaluado en una semana obteniendo resultados y así llegar a la cantidad de errores que se realizan al momento de la facturación. Para esto se considera la cantidad de facturas emitidas al cierre diario de información y la cantidad de facturas que se reporten como rechazadas. La cantidad de personas evaluadas para esta tarea fueron dos, los cuales son encargadas de emitir estos comprobantes.

Para medir el indicador del tiempo de funcionamiento del servidor, se utilizó la técnica de observación, basándose en los resultados obtenidos de la guía de observación N° 2. En este instrumento se indica el tiempo de caída del servidor que si bien es cierto no es muy a menudo cuando esto ocurre en la estación es un peligro latente pues paraliza las ventas y cae el sistema. Este instrumento fue evaluado en 1 semana para esclarecer el tiempo que se emplea en dar la solución a la caída del servidor. Se tomó en consideración el tiempo de trabajo del servicio que es diario y no para durante las 24 horas de funcionamiento de la estación, el tiempo en el momento de la caída y levantamiento del mismo. Son tres personas las encargadas de esta área.

Para medir el indicador de la emisión de vales de combustibles, se utilizó la técnica de observación, basándose de la guía de observación N°3. Con este instrumento se evaluó a una persona las cuales están encargadas de la emisión de vales de combustibles y posterior entrega a los clientes; la evaluación duro 2 semanas para la verificación de lo entrega de vales de combustible. Es así como se consideró la cantidad de vales emitidos y la cantidad de vales que van siendo utilizados para los abastecimientos.

3.4.2. Instrumentos

La encuesta

Para medir el indicador de grado de satisfacción del personal administrativo, se utilizó el cuestionario como instrumento para determinar la satisfacción de la gestión de control y seguridad que se ha implementado tomando en consideración todas las áreas de la empresa (administración, contabilidad, informática, tesorería). Se empleó 1 día de duración para este cuestionario el cual estuvo compuesto por tres preguntas. Para medir el grado de satisfacción de la gerencia, se hará uso de la técnica de la encuesta, basándose en los resultados obtenidos del cuestionario N°2. Para este fin se tomó la opinión del gerente siendo este cuestionario dirigido hacia él para la búsqueda de satisfacción según el plan de control y seguridad implementado en la empresa formulándole dos preguntas.

3.4.3. Validez

De acuerdo a los instrumentos de la presente investigación serán avalados por tres expertos relacionados con el tema de estudio quienes orientaron a desarrollar la claridad de los instrumentos.

3.4.4. Confiabilidad

La confiabilidad es implícita por la misma naturaleza de los instrumentos por tanto no se utilizó esta técnica debido a que se cuenta con guías de observación, escala de medición, cuestionarios.

3.5 Procedimientos

Se entrevistó con los responsables del área de Rent A Car, para el desarrollo de la investigación y el uso de los datos respectivamente.

Se aplicó la técnica de observación para medir la cantidad de errores en facturación diaria, el tiempo de funcionamiento del servidor (tiempo en el momento de la caída y levantamiento del mismo) y la emisión de vales de combustibles, se consideró la cantidad de vales emitidos y la cantidad de vales que van siendo utilizados para los abastecimientos.

3.6 Método de análisis de datos

El proyecto expuesto es un análisis ligado a la hipótesis a partir de un

estudio estadístico descriptivo de las variables, en donde los indicadores proporcionan las variables para el estudio a través de un estadígrafo estadístico como el coeficiente de correlación de Spearman.

3.7 Aspectos éticos

La estructura de las citas y referencias de las fuentes consideradas para la investigación se basan en el estilo ISO 690:2010, lo expresado en el artículo N°43 del código de ética profesional del Colegio de Ingenieros del Perú y de la Universidad César Vallejo en lo que respecta a faltas de ética y sanciones; en cuanto que su investigación se desarrolló con de rigor científico, responsabilidad y honestidad en cuanto a la elaboración del informa basado estrictamente con el manejo de la información recopilada. Finalmente se considera el artículo N°15 con respecto al plagio y el artículo N°16 con respecto a la autoría del trabajo.

IV. RESULTADOS

4.1 Reducir la cantidad de errores que se presentan a diario en el proceso de facturación.

Tabla 1 Errores diarios en el proceso de facturación

N°	Cantidad de facturas emitidas		Cantidad facturas rechazadas		Cantidad de facturas declaradas	
	PreTest	PostTest	Pre Test	PostTest	Pre Test	Post test
1	56	60	5	2	51	58
2	105	110	10	5	95	105
TOTAL	**161**	**170**	**15**	**07**	**146**	**163**

Fuente: Guía de observación cantidad de facturas rechazadas

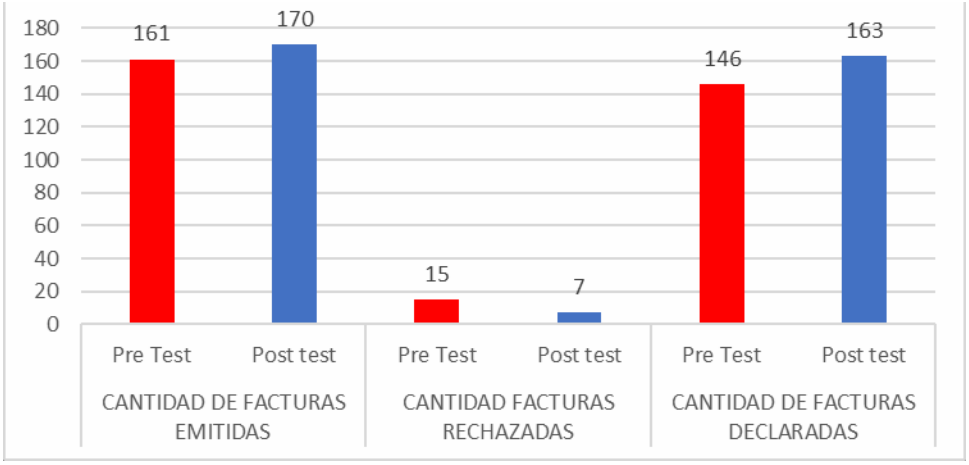

Ilustración 1 Proceso de facturación

Respecto a los errores que se presenta a diario en el proceso de facturación, la tabla 01 muestra los resultados en base a la cantidad de facturas emitidas, las facturas rechazadas y las facturas declaradas. Para el caso de las cantidad de facturas emitidas se observa que antes de la implementación del Plan de Control y Seguridad de los Activos de Información el pre test arrojó que se emitieron un total de 161 facturas, de las cuales fueron rechazadas 15 y solo se declararon 146 lo que evidencia que existe una problemática en la emisión que está relacionada con errores de digitación de información y/ facturas rechazadas por

la Sunat las fallas en el servidor y la ausencia de buenas prácticas en la facturación. Tras la implementación del plan de control la situación cambio notablemente en el post test pues se observa que aumentó la cantidad de facturas emitidas a 170, se redujo considerablemente el número de facturas rechazadas a 07 y el número de facturas declarada respecto al total fue de 163. Lo que sin lugar a dudas demuestra la ausencia y/o reducción significativa de errores lo que permite que en el área de facturación no esté condicionada al tiempo de verificación del servidor de Sunat.

4.2 Minimizar la cantidad de caídas del servidor que maneja el sistema de la organización.

Tabla 2 Pre y post test de la cantidad de caídas del servidor

N°	**Tiempo de trabajo del servidor**		**Tiempo de interrupción del servidor**		**Tiempo funcionamiento del servidor**	
	Pre test	**Post test**	**Pre test**	**Post test**	**Pre test**	**Post test**
1	24:00	24:00	00:10	00:05	23:50	23:55
2	24:00	24:00	00:08	00:03	23:52	23:57
3	24:00	24:00	04:00	00:05	20:00	23:55

Fuente: Guía de observación para tiempo de funcionamiento del servidor

Respecto al funcionamiento del servidor, la tabla 02 muestra los resultados obtenidos en relación al tiempo de trabajo, de interrupción y funcionamiento del servido de la estación de servicios San José antes y después de la implementación del plan de control y seguridad de los activos de información.

Los resultados evidencian que el servidor de la estación de servicios trabaja y este funcionamiento las 24 horas del día y mediante el pre test se observó que su funcionamiento se vio interrumpido en lapsos que van de 10 minutos a 4 horas en el caso más extremo. Estas interrupciones o “caídas” inciden directamente en el servicio de facturación y venta de combustible logrado con

ello que se paralice el servicio y la consiguiente pérdida de información. Este último hecho denota a la ausencia de un soporte o backup. La implementación del plan de control y seguridad de los activos de información diseñado bajo la metodología Cobit permitió mejorar esta situación, pues en el post test se observó una notable reducción de interrupciones del servidor a un promedio de 5 minutos en el día. Ello se logró a través de actividades de mantenimientos preventivos en los equipos y cableados, así como el ordenamiento de los sistemas de información. Con esto se logra que los servicios brindados en las diversas áreas de la empresa trabajen de manera óptima.

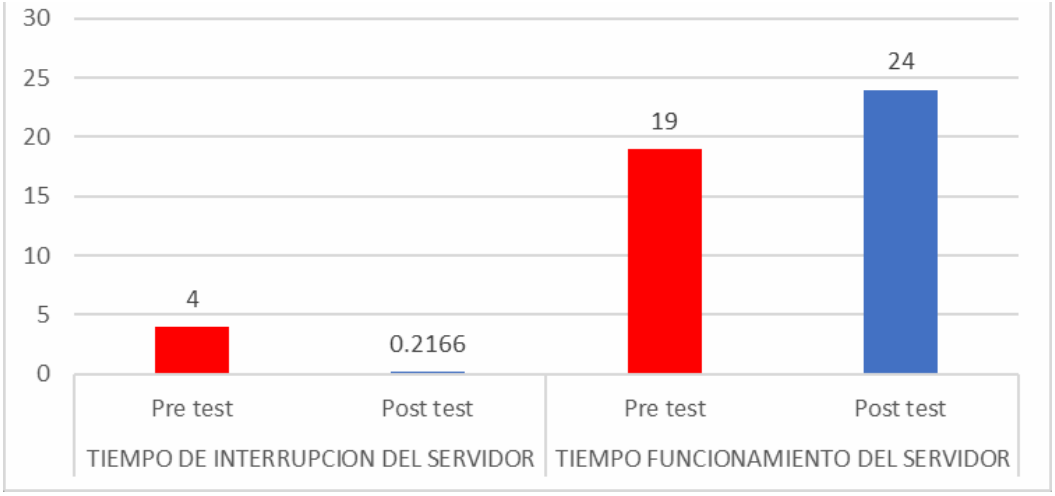

Ilustración 2 Caídas del servidor

4.3 Controlar la emisión de vales emitidos visados por el área administrativa

Indicador N.º 03.- Controlar la emisión de vales emitidos visados por el área administrativa.

Tabla 3 Pre y post test de emisión de vales de combustible

No	**Cantidad de Vales emitidos**		**Cantidad de vales utilizados**		**Vales de combustible no utilizados**	
	Pre test	**Post test**	**Pre test**	**Post test**	**Pre test**	**Post test**
1	2000	2050	1800	2025	200	25

Fuente: Guía de observación para la emisión de vales de combustible

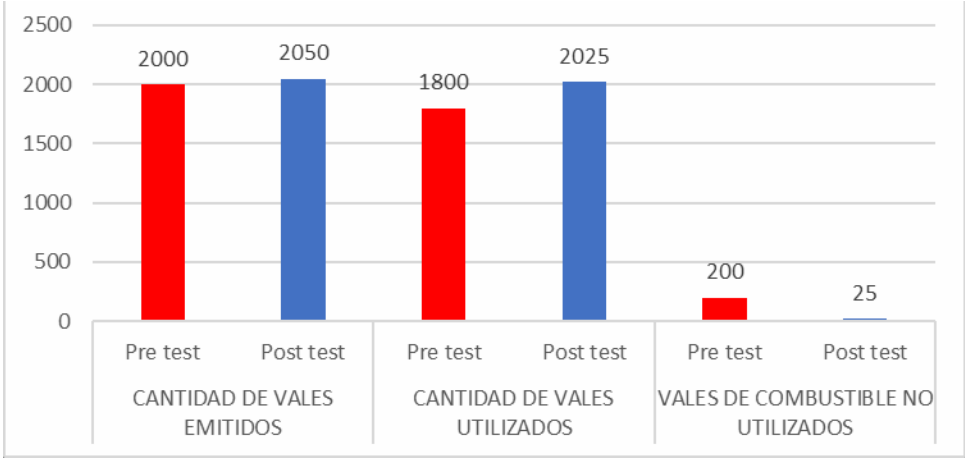

Ilustración 3 Emisión de vales de combustible

Respecto a la emisión de vales de combustible, en la tabla 3, los resultados del pre test evidenciaron que en lapso de la investigación (2 semanas) se emitieron un total de 2000 vales, de los cuales se utilizaron 1800 con un saldo de 200 vales que fueron devueltos para el para registro e identificación del área encargada, y así llevar un registro de los vales que se han utilizado con abastecimiento de combustible y los no utilizados. Ello implica una recarga en el trabajo y denota a su vez la ausencia de una política de control adecuada. Tras la implementación del plan de control y seguridad de los activos de Información se logró corregir esta situación ya que los resultados del post test arrojaron un incremento de vales de combustible emitidos a 2025 y en contraste una disminución de vales devueltos a la cantidad de 25. Este aumento de emisión de los vales se debe al incremento de los clientes que realizan convenio de crédito con el grifo debiendo tener en cuenta aún más los vales en el abastecimiento de combustible.

4.4 Elevar el grado de aceptación del personal con la gestión de control implementada en Estación de Servicios San José, Incrementar la eficiencia en la toma de decisiones de los altos ejecutivos.

Tabla 4 Grado de aceptación del personal con la gestión de control implementada en Estación de Servicios San José

PREGUNTAS	RESPUESTAS	FRECUENCIAS			
		Pre test		Post test	
¿Cómo calificaría usted la implementación de un plan de control y seguridad en los activos de la empresa?	Muy Buena	0	0	4	0.31
	Buena	0	0	7	0.54
	Regular	9	0.69	2	0.15
	Mala	1	0.08	0	0.00
	Muy Mala	3	0.23	0	0.00
¿Cree usted que al implementarse este control los activos de información que a diario incrementan estarán más seguros?	Siempre	0	0.00	7	0.54
	Casi Siempre	2	0.15	6	0.46
	A veces	7	0.54	0	0.00
	Nunca	4	0.31	0	0.00
	Casi Nunca	0	0.00	0	0.00
¿Cómo calificaría el plan de control de los activos de información que circula en la administración de la empresa?	Segura	0	0.00	13	1.00
	Insegura	5	0.38	0	0.00
	Nada confiable	8	0.62	0	0.00

Fuente: Cuestionario sobre grado de aceptación

Respecto al Grado de aceptación del personal con la gestión de control implementada en Estación de Servicios San José, en la tabla 4, los resultados del cuestionario aplicado antes de la implementación del plan de control (pre test) evidencio que 69% del personal valoro como regular la la auditoria de seguridad para la implementación de un plan de control en los activos de la empresa, asimismo considero el 54% manifiesto que a veces podría brindar seguridad la implementación de un control los activos de información que a diario incrementan estarán más seguros y calificó como nada confiable (62%) el

plan de control de los activos de información que circula en la administración de la empresa. Tras el diseño e implementación del plan de control y seguridad basado en la metodología Cobit el personal cambio su percepción y valoración, así el post test arrojo que el 54% del personal valoró como buena la implantación el plan de control implementado, considero en un 54% que el plan de control implementado si ofrece seguridad a los activos de información y en el 100% están seguros de la utilidad del plan de control nuevo.

Tabla 5 Eficiencia en la toma de decisiones de los altos ejecutivos

Preguntas	**Respuestas**	**Frecuencias**			
		Pre test		**Post test**	
¿Ha notado cambios considerables en el control de seguridad que se ha implementado para los activos de información de la empresa?	Si	0	0.00	1	100
	No	1	1.00	0	0.00
¿Se ha logrado controlar el uso irregular y salida de información en cuanto a los vales de combustible de la estación?	Siempre	0	0.00	1	100
	Casi Siempre	0	0.00	0	0.00
	No	1	1.00	0	0.00
	Poco	0	0.00	0	0.00
¿Suele interrumpirse la conexión del servidor e interrumpir las tareas de facturación?	Si	1	1.00	0	0.00
	No	0	0.00	1	100

Respecto a la eficiencia en la toma de decisiones de los altos ejecutivos antes y después de la implementación del plan de control la tabla 05 evidencia que antes de la aplicación del plan de control los ejecutivos (la gerencia) no había notado cambios en el control de seguridad, consideraba que no se había logrado controlar el uso de los vales de combustible y que el servidor solía interrumpirse ocasionando los procesos de venta y facturación. Tras el conocimiento del plan de control y seguridad, las aplicaciones de post test cambio la percepción de los

objetivos evidenciado que al 100% habían notados cambios tras la aplicación del plan de control además en su totalidad comprenden que se ha logrado controlar el uso regular de información sobre todo los vales y 100% cree que ahora no puede interrumpirse la conexión y ello favorece el servicio de venta y facturación.

Prueba De Hipótesis

Hi: Mediante la metodología COBIT es viable implementar el plan de Control y seguridad de los Activos de información en la Estación de Servicios San José

Ho: Mediante la metodología COBIT no es viable implementar el plan de Control y seguridad de los Activos de información en la Estación de Servicios San José

Tabla 6 Prueba de hipótesis

Nivel de significación: Para todo valor de probabilidad igual o menor que 0.05, se acepta Hi y se rechaza Ho.		**Plan de control y seguridad**	**Control de activos de información**
Plan de control y seguridad	Correlation Coeficient	1	0,412**
	Sig. (2-tailed)		0,000
	N	13	13
Control de activos de información	Correlation Coeficient	0,412**	1
	Sig. (2-tailed)	0,000	
	N	13	13

Tras la aplicación del coeficiente de correlación de Spearman se obtuvo un coeficiente de correlación de 0,462** y como el valor equivale a una probabilidad menor que 0.01 (por lo tanto, también menor que 0.05, el cual es el nivel de significancia), se acepta Hi y se rechaza Ho: por lo tanto se prueba la presencia de una relación alta y estadísticamente significativa entre las variables, es decir, que Mediante la metodología COBIT si es viable implementar el plan de Control y seguridad de los Activos de información en la Estación de Servicios San José.

V. DISCUSIÓN

Hoy en día toda empresa o negocio que ofrezca servicio o se dedique a la producción cuenta con sistemas de información computarizadas y/o sistemas informáticos a través de los cuales se procesan diversas actividades, mayormente referidas a procesos de control de actividades, de personal y de control financiero. No obstante, la sistematización a través de estos sistemas de información, no siempre resulta positivo su mantenimiento ocasionando, debido a ello fallas en el servicio, interrupciones o caídas de servidores que afectan el normal proceso de las empresas o negocios

Ante problemas de este tipo surgen los llamados planes de control y seguridad que son documentos en los que establece los lineamientos de respuesta para atender en forma oportuna, eficiente y eficaz, daños en equipos de cómputo o desastres producto de eventos naturales u otros, a causa de algún incidente tanto interno como externo a tecnologías de información. Para el caso que nos ocupa en esta investigación el plan de control y seguridad incorpora elementos tendientes a reducir la cantidad de errores, la caída del servidor, los problemas de facturación y la confianza y aceptación del personal en el nuevo plan implementado.

El error siempre se ha considerado como un elemento que retrasa una actividad o perjudica un sistema organizado, para el caso de las tecnologías de la información, el error (humano o mecánico, individual o grupal, etc.) puede causar no solo la interrupción o calidad en un sistema informático sino también la paralización productiva o de los servicios que una empresa puede ofrecer.

Para el caso de la estación de Servicios San José el desarrollo de la investigación permitió que en relación al Objetivo N.º 01. Reducir la cantidad de errores que se presentan a diario en el proceso de facturación, los resultados obtenidos permitan establecer que el error en el proceso de facturación tiene predominancia humana más que informática, y ello es probable en el número de facturas emitidas (161) relacionadas con aquellas que han sido rechazadas (15) y con aquellas que fueron declaradas (146). Este hecho reflejaba que no se ha empoderado al personal encargado, que no existe una política de control

y verificación de los procesos de facturación pues la mayoría de los errores observados se relacionaba con la inadecuada digitación de las mismas. Ante esta problemática, la decisión de diseñar e implementar un plan de control y seguridad de los activos de información buscaba determinar cómo incorporar procesos de la metodología Cobit en el afán de mejorar la situación problemática descrita. Así se decidió incorporar el dominio Planeación y organización a fin de que el proceso DS- 4 Asegurar la continuidad del servicio; a través de este se evalúo el riesgo que este error conllevaba a la empresa, así como también verificar hasta qué punto se lograba reducir el error en la digitación. La implementación del plan permitió en efecto reducir los errores en el proceso de saturación logrando que se aumente el número de facturas emitidas (170) y se redujera el número de facturas rechazadas

La caída del servidor de cualquier sistema informático (down time) es usado para definir cuando el sistema no está disponible (solo para servidores). Los casos pueden ser planeados o no planeados. Los casos de tiempos de inactividad planeadas pueden ser por cambio del sistema, cambios de datos, reconfiguración del sistemas o reinicio de servicios. Los casos de tiempos de inactividad no planeadas pueden ser provocados por fallas del sistema, daño en los servidores, fallas de la red de datos, fallas en el fluido eléctrico. Este último momento formo parte del objetivo Nº 02 que buscaba minimizar la cantidad de caídas del servidor que maneja el sistema de la estación de servicio San José. Los datos obtenidos tras la aplicación de los instrumentos permitió conocer que el servicio de la estación de servicios antes de la implementación del plan de control y seguridad estaba propenso a quedar inactivo o “caerse” por demasiado tiempo (entre 0 a 4 horas) y la razón de ello es que al parecer no existía política de mantenimiento preventivo, no se había adecuado la infraestructura para que el servidor tenga condiciones de humedad y limpieza que contribuyera a que el servicio del servidor se vea, si bien no interrumpido, al menos que las instrucciones que se den de manera fortuita (por corte de fluido eléctrico por ejemplo) sean mínimas, Por ello dentro del plan de control y seguridad se estableció y rigió el dominio entrega y soporte de dominio en el proceso DS5

Garantizar seguridad de sistemas, lo cual contribuyó a mejorar la situación, pues en el post test se observó una notable reducción de interrupciones del servidor a un promedio de 5 minutos en el día. Ello se logró a través de actividades de mantenimientos preventivos en los equipos y cableados, así como el ordenamiento de los sistemas de información. Con esto se logra que los servicios brindados en las diversas áreas de la empresa trabajen de manera óptima.

La emisión de vales en la Estación de Servicios San José no solo busca incrementar la venta sino también incorporar nuevos clientes a través de una cartera de créditos. No obstante, esta política comercial requiere control tal como se buscaba en el Objetivo N.º 03.- Controlar la emisión de vales emitidos visados por el área administrativa. Los vales que se emiten por clientes que están autorizados por la misma estación para hacer uso de estos vales, sin embargo, existe, al momento de abastecimiento el uso irregular de estos vales, como adulteración en el momento de abastecer y la compra o intercambio irregular de los mismos ocasionando que las personas responsables de esa actividad sean despedidas o amonestadas por este uso no permitido. Según con los estándares que se han aplicado se ha buscado minorar la anulación por error o pérdida de los mismos y así realizar una correcta facturación por cliente de acuerdo al reporte de abastecimiento aplicando el proceso M-1 Monitorear los procesos. Ello se pudo notar en los resultados obtenidos antes de la implementación y aplicación el plan de control y seguridad donde se emitieron 2000 vales y solo se utilizaron 1800 con un saldo de 200 vales que fueron devueltos a la gerencia. Ello implica una recarga en el trabajo y denota a su vez la ausencia de una política de control adecuada. Tras la implementación del Plan de Control y Seguridad de los Activos de Información se logró corregir esta situación ya que los resultados del post test arrojaron un incremento de vales de combustible emitidos a 2025 y en contraste una disminución de vales devueltos a la cantidad de 25. Este aumento de emisión de los vales se debe al incremento de los clientes que realizan convenio de crédito con el grifo debiendo tener en cuenta aún más los vales en el abastecimiento de combustible.

El grado de aceptación es definido como la satisfacción de un individuo ante un objeto, una acción, etc. que la incorpora a su mundo natural y cultural provocando cambios de conductas y aptitud. Para el caso del presente estudio en el Objetivo N.º 04 se buscaba elevar el grado de aceptación del personal con la gestión de control implementada en Estación de Servicios San José. Para ello se aplicó un cuestionario a fin de conocer la percepción y aceptación del personal respecto al control y seguridad que existía en la estación de servicios San José antes y después de la implementación del pan de control y seguridad basado en la metodología Cobit. Los resultados evidenciaron que antes de implementar el plan no existía una aceptación positiva acerca del control y seguridad imperante y la confianza en ella era muy reducida. Po ello en el diseño del plan de control y seguridad basado en Cobit se seleccionó el componente DS-5 – Garantizar la seguridad de sistemas con sus sub componentes DS5-C7 – Concientización respecto a la seguridad IT; DS5-C8; ello permitió que tras la aplicación el personal cambie su percepción y valoración, al punto que el 54% del personal valoro como buena la implantación el plan de control implementado, se dieron cuenta que el plan de control implementado si ofrece seguridad a los activos de información y están seguros de la utilidad del plan de control nuevo.

La eficiencia es definida usualmente como “el óptimo empleo de los recursos para obtener mejores resultados” (Schmelkes, 2001) en el caso de la presente investigación a través del, Objetivo Nº 05 se buscó incrementar la eficiencia en la toma de decisiones de los altos ejecutivos. Para ello se entrevistó al gerente de la estación de servicios antes del diseño e implementación el plan de control y seguridad. Los resultados permitieren conocer que antes de conocer e implementar el plan, el gerente se encontraba preocupado por no alcanzar eficiencia en el desenvolvimiento de su personal, particularmente por los constantes errores en la facturación y la ausencia de una política de control y seguridad que permitieran evitar interrupción del soporte informático. Cuando se le hizo conocer el plan y su implementación su percepción de mejora cambio notablemente

VI. CONCLUSIONES

1. La implementación del plan permitió en efecto reducir los errores en el proceso de facturación logrando una reducción considerablemente el número de facturas rechazadas de 9.3% (15 facturas) a 4.1% (07 facturas) y en contrapartida se aumentó el número de facturas emitidas (de 161 a 170) y aumento también la cantidad de facturas declaradas (de 146 a 163)

2. La implementación del plan de control y seguridad basado en la metodología Cobit permitió minimizar la cantidad de caídas del servidor que maneja el sistema de la organización, reduciendo el tiempo de interrupción que inicialmente ocurría entre 10 minutos – 4 horas a un promedio de 5 minutos en el día

3. La implementación del plan de control y seguridad permitió controlar la emisión de vales emitidos, pasando de 200 vales devueltos (de un total de 2000 vales visados) a 25 vales de un total de 2025) devueltos tras la aplicación del plan

4. El grado de aceptación del personal con la gestión de control implementada en Estación de Servicios San José se elevó demostrado en el que más de la mitad (54%) del personal valoro como buena la implementación del plan de control implementado, se dieron reconocieron que el plan de control implementado si ofrece seguridad a los activos de información y están seguros de la utilidad del plan de control nuevo

5. La implementación del plan de control y seguridad basado en la metodología Cobit permitió a los ejecutivos de la gerencia de la estación de servicios San José incrementar la eficiencia en la toma de decisiones de los altos ejecutivos puesto que tras la aplicación reconocieron que la estructura y organización de las actividades propuestas si permite reducir los errores de facturación y reducir las interrupciones y/o caídas del soporte informático de la empresa

VII. RECOMENDACIONES

1. Procurar desarrollar talleres de capacitación en control y seguridad al personal de cualquier negocio u organización, tal como se contempla en el plan de control y seguridad diseñada a fin de reducir los errores en los procesos.

2. A través del marco de referencia COBIT, monitorear al personal de las organizaciones en cuanto el uso del soporte informático a fin de detectar a tiempo los errores que se puedan cometer al momento de realizar cualquier proceso para así contribuir al logro de los objetivos del negocio.

3. Generar una política de mantenimiento preventivo tal como lo señala el plan de control y seguridad implementado de manera tal que el software y el servidor se encuentren en condiciones óptimas de funcionamiento.

4. Fomentar entre el personal un sentimiento de valoración para con sus labores, de manera tal que se pueda incorporarle una cultura organizacional que redunda en un mejor servicio.

5. Procurar empoderar a toda la organización capacitándolos en el uso y aplicación el plan de control y seguridad diseñado, de manera tal que se pueda dotar de un documento de control, monitoreo y evaluación de toda la organización.

REFERENCIAS

- Aguirre Mollehuanca, D. A. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A",.* Lima, Perú. Obtenido de https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/5677/AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf?sequence=1&isAllowed=y
- Anastacio Cortez, C. J., & Osorio Quijandría, C. A. (2018). *Incidencia del control contable de activos fijos en la información financiera de Impulsa365 SAC – San Isidro, año 2018.* Lima, Perú. Obtenido de http://hdl.handle.net/11537/22469
- Ángel, P. I. (2012). *Cobit 5.* México .
- Berrío, J. P., Montoya Pérez, Y., Pérez Zapata, G. A., & Jiménez Builes, J. (2016). *Modelo para la evaluación de desempeño de los controles de un SGSI basado en el estándar ISO/IEC 27001.* Medellín, Colombia. Obtenido de http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/618/COMTEL%202016%20-%20Paper13.pdf?sequence=1&isAllowed=y
- Carolina Nieves, A. (2017). *Diseño de un sistema de gestión de la aseguridad de la (SGSI) basado en la norma SO/IEC 27001:2013.* Colombia. Obtenido de https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y
- Castellaro, M., Romaniz, S., Ramos, J. C., Feck, C., & Gaspoz, I. (2016). *Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas.* Obtenido de http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(2).pdf
- Castro Siguas, J. J. (2017). *Implementación de la NTP ISO/IEC 27001:2014 para mejorar la gestión de la seguridad en los sistemas de información de la Autoridad Portuaria Nacional, Callao - 2017.* Lima, Perú. Obtenido de https://repositorio.autonoma.edu.pe/bitstream/handle/20.500.13067/587/Castro%20Siguas%20Joshimar.pdf?sequence=1&isAllowed=y
- De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2019). COBIT as a Framework for Enterprise Governance of IT. *Enterprise Governance of Information Technology*, 125–162. Obtenido de https://link.springer.com/chapter/10.1007/978-3-030-25918-1_5

- Del Toro, J. (2005). *Control Interno.* La Habana, Cuba: Centro de Estudios Contables Financieros y de Seguros (CECOFIS).
- Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). *La seguridad informática y la seguridad de la información.* Manta, Ecuador. Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/420
- Gómez Fernández Luis, F. R. (2015). *Como implantar un SGSI.* España : AENOR (Asociación Española de Normalización y Certificación).
- Guerrero Julio, M. L. (2010). *Gestión de riesgos y controles en sistemas de información.* Bucaramanga, Colombia. Obtenido de http://tangara.uis.edu.co/biblioweb/tesis/2010/136503.pdf
- Hernández Escobar, A. A. (2018). *Metodología de la Investigación Científica.*
- Hernández Sampieri, R., Mendez Valencia, S., & Mendoza Torres, C. P. (2017). *Metodología de la investigación.*
- León-Acurio, J. V., Mora-Aristega, J. E., Huilcapi-Masacon, M. R., Tamayo-Herrera, A. d., & Armijos-Maya, C. A. (2018). COBIT como modelo para auditorías y control de los sistemas de información. *Casedelpo*. Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/439
- Mero García, A. F. (2016). *Implantación de un sistema de gestión de seguridad de información (SGSI) en el distrito de salud 13d04 24 de mayo – Santa Ana – Olmedo – salud de la provincia de Manabí.* Manabi, Ecuador. Obtenido de http://repositorio.puce.edu.ec/handle/22000/11322
- Mesa Palacios, G., Serra Toledo, R., & Fleitas Triana, S. (2018). *Metodología para la gestión de los activos fijos intangibles visibles en una universidad.* La Habana, Cuba: Universidad Tecnológica de la Habana José Antonio Echeverría. Cuba. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202018000400154
- Miranda-Vásquez, K. (2013). *Guía metodológica para implementar un sistema de gestión de seguridad en las instituciones.* Obtenido de https://pirhua.udep.edu.pe/bitstream/handle/11042/2787/MAS_DET_012.pdf?sequence=1&isAllowed=y
- Oscar Alcides, D. C. (2018). *Gestión de riesgos de activos de información.* Colombia: Universidad Piloto de Colombia. Obtenido de

http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8586/Gestion%20de%20riesgo%20de%20activos%20de%20informacion.pdf?sequence=1&isAllowed=y

- Perafán Ruiz, J. J., & Caicedo Cuchimba, M. (2014). *Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca.* Popayán, Colombia: Universidad Nacional Abierta y a Distancia. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf?sequence=3&isAllowed=y
- Ramos Arca, C. C. (2015). *Propuesta de un plan de auditoria informática para el sistema de información en salud y el aplicativo para el registro de formatos SIS en los establecimientos de salud de la unidad ejecutora 400 en la región Piura en el año 2015.* Piura, Perú. Obtenido de https://repositorio.unp.edu.pe/handle/UNP/683
- Sandoval Morales, H. (2012). *Introducción a la auditoria.* Mexico.
- Santillana Gonzales, J. R. (2013). *Auditoría Interna.* México: PEARSON EDUCACIÓN.
- Steuperaert, D. (2019). *COBIT 2019: A Significant Update.* ISACA. Obtenido de https://www.tandfonline.com/doi/abs/10.1080/07366981.2019.1578474
- Tejena-Macías, M. A. (2014). *Análisis de riesgos en seguridad de la información.* Manta, Ecuador. Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/809
- Villena Aguilar, M. A. (2016). *https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/362/VILLENA_MOIS%c3%89S_SISTEMA_DE%20GESTI%c3%93N_DE_SEGURIDAD_DE_INFORMACI%c3%93N_PARA_UNA_INSTITUCI%c3%93N_FINANCIERA.pdf?sequence=1&isAllowed=y.* Lima, Perú: Universidad Católica del Perú. Obtenido de https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/362/VILLENA_MOIS%c3%89S_SISTEMA_DE%20GESTI%c3%93N_DE_SEGURIDAD_DE_INFORMACI%c3%93N_PARA_UNA_INSTITUCI%c3%93N_FINANCIERA.pdf?sequence=1&isAllowed=y

PROPUESTA

Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José

Fundamentación

Hoy en día, la información es un activo importante para las empresas, es fundamental para el negocio: facturas, informes, bases de datos de clientes, pedidos, etc. Podemos decir que las empresas basan su actividad en sistemas de información con soporte tecnológico. La estación de servicios San José no está exenta de poseer un sistema de información basado en servidores que constituyen la forma de controlar no solo la cantidad de combustibles que venden en sus diversas variedades sino también les permite tener el control y seguimiento de los procesos de facturación.

Este proceso de automatización conlleva no solo a diseñar procesos de control sino también a formular planes de seguridad de los activos de información, ya que proteger los sistemas de información es proteger el negocio. Para garantizar la seguridad de la información del negocio se necesita llevar a cabo una gestión planificada de actuaciones en materia de Ciberseguridad, tal y como se realiza en cualquier otro proceso productivo de la organización, de ahí la necesidad de diseñar el presente plan de control y seguridad de los activos de información en la estación de servicios san José

El plan consiste en la definición y priorización de un conjunto de acciones y/o buenas prácticas en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial, que permite incorporar las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización, así como terceros que colaboren con ésta

Finalmente, el plan pretende también que la estación de servicios “San José” –Piura siga siendo competitiva dentro de un mercado exigente basando su éxito en la seguridad de sus activos de información, así como también que mejore en su producción, su organización, y que obtenga de esta manera un reconocimiento en el mercado nacional. El propósito de este trabajo es alcanzar dicha meta, para que la empresa no solo sea conocida en Piura, sino también dentro de todo el Perú, para más adelante apuntar a los mercados que están fuera del país. Con el fin de obtener una marca que pueda competir con otras ya reconocidas mundialmente en el mismo rubro.

Objetivos del plan

Objetivo general:

Aplicar el plan de control y seguridad de los activos de información para incrementar la eficiencia en el servicio a los clientes y mejorar las condiciones de operatividad en las instalaciones bajo el fundamento de protección del sistema informático que posea la estación de servicios

Objetivos específicos

1. Asegurar la capacidad de supervivencia de la estación de servicios ante eventos que pongan en peligro su existencia.
2. Proteger y conservar los activos de la empresa, de riesgos, desastres naturales o actos mal intencionados.
3. Reducir la probabilidad de las perdidas, a un mínimo de nivel aceptable, a un costo razonable y asegurar la adecuada recuperación.
4. Asegurar controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento

Análisis de cumplimento del plan

Para llevar a cabo el análisis de cumplimiento y situación se realizaron las siguientes actividades:

1. Se realizaron observación in situ de las instalaciones a fin de determinar la infraestructura y la ubicación del servidor principal de la estación de servicios
2. Registro de todos los problemas y evidencias detectadas en relación a los requisitos de seguridad de aplicación y que están prefijados de acuerdo con el modelo metodológico Cobit (que supone 34 procesos en esta etapa) que luego se contrastaron.
3. Reuniones con la gerencia a fin de poder exponer el interés de diseñar e implementar el plan de control
4. Reuniones con el gerente y el personal de la estación para evaluar el cumplimiento de los controles de seguridad implantados. Aunque la mayor parte de los controles corresponden al área de activos de información, específicamente al sistema informático fue también necesario analizar procesos de otras áreas (administración, la infraestructura, la seguridad, etc.) Para poder desempeñar adecuadamente las tareas de recopilación de información, fue vital que la gerencia traslade mediante comunicación personal y documentada a cada una de las áreas y sus responsables la importancia del plan, los beneficios derivados de su implantación, así como la implicación que se espera de ellos en todas las fases del proyecto.
5. Una vez que se ha dispuesto de toda la información, se analizaron los resultados y situamos el cumplimiento de cada control en una escala, por ejemplo, entre el 0 al 5, según el modelo de madurez, donde 0 es la ausencia total del control, y el 5 la aplicación optimizada del control

Administración de riesgos

Basándonos en la metodología COBIT, en donde se identifican 34 procesos que rigen la administración y control de tecnología de la información y cómo estos son impactados principalmente por las características de seguridad de la información (confidencialidad, integridad y disponibilidad) se seleccionó los procesos que a continuación se detallan:

			Confidencialidad	Integridad	Disponibilidad
Dominio	**Proceso**		**Criterios de información**		
Planeación y organización	PO9	Evaluar riesgos	x	x	x
	PO11	Administrar calidad		x	
Adquisición e instalación	A16	Administrar cambios		x	x
Entrega y soporte de servicios	DS4	Asegurar continuidad del servicio			x
	DS5	Garantizar seguridad de sistemas	x	x	
	DS11	Administra la información		x	
	DS12	Administrar las instalaciones		x	x

PLAN DE ACCIÓN

MODELO DE MEJORES PRÁCTICAS COBIT **ESTACIÓN DE SERVICIOS SAN JOSÉ**		
Empresa: Estación de Servicios San José	Fecha de diagnóstico	
Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José		Pág.
PLAN DE ACCIÓN		
Dominio: Planificación y organización	**Proceso: PO9 – Evaluar riesgo**	
Que satisface los requerimientos de Negocio	Soportar las decisiones a través del logro de objetivos de la TI y responder a las amenazas reduciendo su complejidad incrementando su objetividad e identificando factores de decisión importantes	
Se hace posible a través de	La participación de la propia organización en la identificación de riesgos de TI en el análisis de impacto, involucrando funciones multidisciplinarias y tomando medidas económicas para mitigar los riesgos	
Y toma en consideración	Propiedad y registro de la identificación del riesgo Diferentes tipos de riesgo por TI Definir y comunicar el perfil de tolerancia del riesgo Medición cualitativa y cuantitativa del riesgo Metodología de evaluación de riesgos Plan de acción de riesgos Reevaluaciones oportunas	
CONTROLES		
Control a implementar **PO9**	**POLÍTICAS Y PROCEDIMIENTOS DE EVALUACIÓN DE RIESGOS**	

MODELO DE MEJORES PRÁCTICAS COBIT ESTACIÓN DE SERVICIOS SAN JOSÉ		
Empresa: Estación de Servicios San José	Fecha de diagnóstico	
Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José		Pág.
PLAN DE ACCIÓN		
Dominio: Planificación y organización	**Proceso: PO9 – Evaluar riesgo**	
CONTROLES		
Control a implementar PO9	**DEFINICIÓN DE UN MARCO REFERENCIAL DE RIESGOS**	
La gerencia debe establecer una evaluación sistemática de riesgos incorporando: **1.** Los riesgos de información relevantes para el logro de los objetivos de la organización **2.** Base de datos para determinar la forma en que los riesgos deben ser manejables a un nivel aceptables **3.** El alcance y los límites de la evaluación de riesgos		
Responsable de la implementación	Gerente general	**Plazo de ejecución**: dos meses
Control a implementar PO9	**PROCEDIMIENTOS DE EVALUACIÓN DE RIESGOS**	
La gerencia deberá **1.** Determinar que los riesgos identificados incluyen factores tanto externos como internos **2.** Asesores expertos en riesgos deben asegurar las evaluaciones de riesgo		

3. Revisar los informes de resultados de las auditorias **4.** Revisiones de inspecciones e incidentes identificados **5.** Definir un enfoque cuantitativo y cualitativo formal para la identificación y medición de riesgos, amenazas y exposiciones		
Responsable de la implementación	Gerente general	**Plazo de ejecución**: tres meses

MODELO DE MEJORES PRÁCTICAS COBIT **ESTACIÓN DE SERVICIOS SAN JOSÉ**		
Empresa: Estación de Servicios San José	Fecha de diagnóstico	
Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José		Pág.
PLAN DE ACCIÓN		
Dominio: Planificación y organización	**Proceso: PO11– administración de la calidad**	
Que satisface los requerimientos de Negocio	Satisfacer los requerimientos del cliente de TI	
Se hace posible a través de	La planeación, implementación y mantenimiento de estándares y sistemas de administración provistos para las distintas fases de desarrollo, con entregables claros y responsabilidades explicitas.	
Y toma en consideración	Establecimiento de una cultura de calidad **1.** Planes de calidad **2.** Responsables del aseguramiento de la calidad	

	3. Prácticas de control de calidad **4.** Metodología del ciclo de vida del sistema **5.** Pruebas y documentación de programas y sistemas **6.** Revisiones y reporte de aseguramiento de calidad **7.** Entrenamiento e involucramiento del personal **8.** Desarrollo de una base de conocimientos de aseguramiento de calidad **9.** Benchmarking contra normas de la industria		
Control a implementar **PO11**	**POLÍTICAS Y PROCEDIMIENTOS RELACIONADOS CON EL ASEGURAMIENTO DE LA CALIDAD**		
La organización deberá desarrollar, diseminar y periódicamente revisar/actualizar	**1.** Procedimientos documentados para facilitar la implantación de lapolítica del plan general de calidad y los controles asociados		
Responsable de la implementación	Gerente general y gerente de sistemas	**Plazo de ejecución**: Un mes	
MODELO DE MEJORES PRÁCTICAS COBIT **ESTACIÓN DE SERVICIOS SAN JOSÉ**			
	Empresa: Estación de Servicios San José		
	Implementación de un Plan de Control y Seguridad de los **Activos de Información en la Estación de Servicios San José**		Pág.
	PLAN DE ACCIÓN		

Dominio ADQUISICIÓN E IMPLEMENTACIÓN	**Proceso: A16 – Administrar Cambios**
Que satisface los requerimientos de Negocio	Minimizar la probabilidad e interrupciones del sistema, alteraciones no autorizadas, caída de servidores y errores
Se hace posible a través de	Un sistema de administración que permita el análisis implementación y seguimiento de todos los cambios requeridos y llevados a cabo en la infraestructura de la TI
Y toma en consideración	**1.** Identificación de cambios **2.** Procedimientos de categorización, priorización y emergencia **3.** Evaluación del impacto **4.** Administración de liberación **5.** Distribución de software **6.** Uso de herramientas automatizadas **7.** Administración de la configuración **8.** Rediseño de los procesos del negocio

CONTROLES		
Control a implementar A16	**CONTROL DE CAMBIOS**	
1. La gerencia de Ti deberá asegurar que la administración de cambios, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de configuración **2.** El sistema de monitoreo debe ser periódico para evitar caídas del servidor y problemas en la facturación.		
Responsable de la implementación	Gerente general y gerente de sistemas	**Plazo de ejecución**: tres meses

MODELO DE MEJORES PRÁCTICAS COBIT ESTACIÓN DE SERVICIOS SAN JOSÉ		
Empresa: Estación de Servicios San José	Fecha de diagnóstico	
Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José		Pág.
PLAN DE ACCIÓN		
Dominio: ADQUISICIÓN E IMPLEMENTACIÓN	**Proceso: A16 – Administrador de cambios**	
CONTROLES		
Control a implementar A16	**DOCUMENTACIÓN DE LOS SISTEMAS DE INFORMACIÓN**	
La Organización deberá asegurar que esté disponible la adecuada documentación para el sistema de información y sus componentes constitutivos protegida cuando es requerida y distribuida al personal autorizado		
Responsable de la implementación	Gerente general, responsable del sistema y personal de seguridad	**Plazo de ejecución**: Un mes

MODELO DE MEJORES PRÁCTICAS COBIT ESTACIÓN DE SERVICIOS SAN JOSÉ		
Empresa: Estación de Servicios San José	Fecha de diagnostico	
Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José		Pág.
PLAN DE ACCIÓN		
Dominio: ENTREGA Y SOPORTE	**Proceso: DS-4 – Asegurar continuidad del servicio**	
Que satisface los requerimientos de Negocio de	Asegurar que los servicios de TI estén disponibles de acuerdo con los requerimientos y asegurar un impacto mínimo en el negocio en el evento que ocurra una interrupción mayor (caída del servidor principalmente)	
Se hace posible a través de	Teniendo un plan de continuidad probado y funcional que este alineado con los objetivos y metas del negocio y sus requerimientos técnicos a nivel del sistema informático	
Y toma en consideración	**1.** Clasificación con base a la criticidad **2.** Procedimientos alternativos **3.** Respaldo y recuperación **4.** Planes de reactivación **5.** Actividades de administración de riesgos **6.** Análisis de punto único de falla **7.** Administración de problemas	
CONTROLES		
Control a implementar DS4	**POLÍTICAS Y PROCEDIMIENTOS DEL PLAN DE CONTINGENCIA**	
La administración deberá diseminar, desarrollar y periódicamente revisar/actualizar		

1. Una política del plan de contingencia con el propósito de identificar roles y responsabilidades **2.** Procedimientos documentados para facilitar a la implantación de políticas del plan de continuidad del negocio y controles asociados		
Responsable de la implementación	Gerente general y gerente de sistemas	**Plazo de ejecución**: tres meses
Control a implementar DS4	**PLAN DE CONTINGENCIA**	
La organización debe desarrollar e implementar un plan de contingencia para los sistemas de información. Designar un trabajador para que revise y apruebe el plan de contingencia y distribuya copias al personal clave de la contingencia		
Responsable de la implementación	Gerente general y gerente de sistemas	**Plazo de ejecución**: Un mes
Control a implementar DS4	**ENTRENAMIENTO PARA LA CONTINGENCIA**	
La organización debe entrenar al personal involucrado en la contingencia con sus roles, responsabilidades con respecto a los sistemas de información y proveeré constante entrenamiento. Se deben incorporar acciones de simulacro dentro del entrenamiento para una respuesta efectiva del personal en situaciones de crisis.		
Responsable de la implementación	Gerente general y gerente de sistemas	**Plazo de ejecución**: dos semanas

MODELO DE MEJORES PRÁCTICAS COBIT ESTACIÓN DE SERVICIOS SAN JOSÉ		
Empresa: Estación de Servicios San José	Fecha de diagnóstico	
Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José		Pág.
PLAN DE ACCIÓN		
Dominio: ENTREGA Y SOPORTE	**Proceso**: **DS-4 – Asegurar continuidad del servicio**	
CONTROLES		
Control a implementar DS4	**PROBAR EL PLAN DE CONTINGENCIA**	
La organización debe probar el plan de contingencias para los sistemas de información y determinar si el plan es efectivo y la organización está lista para ejecutar el plan		
Responsable de la implementación	Gerente general y gerente de sistemas	**Plazo de ejecución**: un mes
Control a implementar DS4	**ACTUALIZACIÓN DEL PLAN DE CONTINGENCIA**	
La organización debe revisar el plan de contingencia los cambios o problemas encontrados durante la implementación, ejecución o prueba del pan.		
Responsable de la implementación	Gerente general y gerente de sistemas	**Plazo de ejecución**: Un mes

MODELO DE MEJORES PRÁCTICAS COBIT ESTACIÓN DE SERVICIOS SAN JOSÉ		
Empresa: Estación de Servicios San José	Fecha de diagnóstico	
Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José		Pág.
PLAN DE ACCION		
Dominio: ENTREGA Y SOPORTE	**Proceso: DS-5 – GARANTIZAR LA SEGURIDAD DE SISTEMAS**	
Que satisface los requerimientos de Negocio	Salvaguardar la información contra uso no autorizado, divulgación, modificación, daño o pérdida.	
Se hace posible a través de	Controles de acceso lógico que asegura que el acceso a sistemas, datos, y `programas está restringido a usuarios autorizados	
Y toma en consideración	**3.** Requerimiento de confidencialidad y privacidad **4.** Autorización, autenticación y control de acceso **5.** Identificación de usuarios y perfiles de autorización **6.** Manejo, reporte y seguimiento de incidentes **7.** Prevención y detección de virus **8.** Firewalls **9.** Entrenamiento a usuarios **10.** Pruebas y reportes de intrusión	

<table>
<tr><td colspan="4">MODELO DE MEJORES PRÁCTICAS COBIT
ESTACIÓN DE SERVICIOS SAN JOSÉ</td></tr>
<tr><td colspan="2">Empresa: Estación de Servicios San José</td><td colspan="2">Fecha de diagnostico</td></tr>
<tr><td colspan="3">Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José</td><td>Pág.</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td colspan="2">Dominio: ENTREGA Y SOPORTE</td><td colspan="2">Proceso: DS12 – ADMINISTRAR LAS INSTALACIONES</td></tr>
<tr><td>Que satisface los requerimientos de Negocio</td><td colspan="3">Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de la TI contra peligros naturales o fallas humanas.</td></tr>
<tr><td>Se hace posible a través de</td><td colspan="3">La instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado.</td></tr>
<tr><td>Y toma en consideración</td><td colspan="3">11. Acceso a instalaciones
12. Identificación del sitio
13. Seguridad física
14. Políticas de inspección
15. Planeación de continuidad y administración de crisis
16. salud y seguridad personal
17. Políticas de mantenimiento preventivo
18. Protección contra amenazas ambientales
19. Monitoreo automatizado</td></tr>
<tr><td colspan="2">Responsable de la implementación</td><td>Gerente de sistemas y personal de seguridad</td><td>Plazo de ejecución: Un mes</td></tr>
<tr><td colspan="2">Control a implementar</td><td colspan="2">MONITOREAR EL ACCESO FÍSICO</td></tr>
</table>

DS12		
La organización deberá monitorear el acceso físico a los sistemas de información para detectar y responder a incidentes		
Responsable de la implementación	Gerente de sistemas y personal de seguridad	**Plazo de ejecución**: dos meses

Cronograma tentativo de implementación

Las actividades anteriormente diseñadas deberán ser lideradas por la gerencia general y el responsable del sistema informático de la estación quienes asumirán su responsabilidad. A continuación, se presenta un cronograma sugerido para la realización de las actividades correspondientes diseñadas.

Dominios y procesos del plan Control y Seguridad de los Activos de Información en la Estación de Servicios San José		**Mes 1**				**Mes 2**				**Mes 3**			
		1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Planeación y organización	PO9- Evaluar riesgos												
	PO11- Administrar calidad												
Adquisición e instalación	A16- Administrar cambios												
Entrega y soporte de servicios	DS4 - Asegurar continuidad del servicio												
	DS5- Garantizar seguridad de sistemas												
	DS11- Administra la información												
	DS12- Administrar las instalaciones												

ANEXOS

Anexo N° 1. Guía de observación N°1

Número de errores de facturación

Diariamente en el área de facturación de la estación de servicios se presentan errores en la facturación del sistema de gestión instalado, errores que dan a lugar a la exposición de información en cuanto al abastecimiento, cantidad, digitación

Procedimiento

Se tomará a 13 personas del área administrativa evaluándolas mediante una guía de observación, tomando la cantidad de facturas emitidas menos la cantidad de facturas rechazadas arrojándonos como resultado de esa diferencia la cantidad de errores q se producen en la facturación.

N°	CANTIDAD DE FACTURAS EMITIDAS	CANTIDAD FACTURAS RECHAZADAS	CANTIDAD DE ERRORES FACTURACIÓN
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

CEF = CFE-CFR

1. C+EF= cantidad de errores de facturación
2. CFE = cantidad de facturas emitidas
3. CFR = cantidad de facturas rechazadas

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICIÓN
Control de activos de información	Consiste en gestionar en forma adecuada los activos de información, logrando su identificación en forma precisa y detallada, validando a detalle cada una de las características necesarias de su información (Mesa Palacios, Serra Toledo, & Fleitas Triana, 2018).	Mediante la aplicación de instrumentos como guías de observación en las dimensiones de errores de facturación, emisión de facturas y facturas rechazadas, se valora cada uno de sus indicadores antes y después de la de la implementación de un Plan de Control y Seguridad de los Activos de Información.	Errores en facturaciones.	Cantidad de facturas emitidas	Nominal
				Cantidad de facturas rechazadas	Nominal
				Cantidad de errores en facturaciones.	Nominal
			Caídas del servidor	Tiempo de trabajo del servidor	Nominal
				Tiempo de interrupción del servidor	Nominal
				Tiempo funcionamiento del servidor	Nominal
			Emisión de vales	Cantidad de Vales emitidos	Nominal
				Cantidad de vales utilizados	Nominal
				Vales de combustible no utilizados	Nominal

Plan de control y seguridad	El plan de control y seguridad normalmente, corresponde a proteger el derecho de acceso a la información mediante los procesos de control, dando lugar a entender que operadores tienen exclusividad de accesos a áreas establecidas dentro de la organización (Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018).	Mediante la aplicación de instrumentos como guías de observación a la dimensión de satisfacción, se valora cada uno de sus indicadores como Grado de satisfacción del personal administrativo y Grado de satisfacción de gerencia.	Satisfacción	Grado de satisfacción del personal administrativo.	Porcentual
				Grado de satisfacción De gerencia.	Porcentual

Anexo N° 2. Guía de observación N°2

Tiempo de funcionamiento del servidor

El servidor de la estación de servicios realiza un trabajo de 24 horas al día el cual por ocasiones presenta caídas que suele interrumpir el trabajo del personal administrativo debido a los distintos sistemas de gestión que se manejan en la empresa.

Procedimiento

Se tomará en consideración 2 horarios para medir el tiempo de funcionamiento del servidor sea en horario diurno o nocturno; considerando el tiempo de trabajo del servidor menos el tiempo de interrupción del servidor.

N°	TIEMPO DE TRABAJO DEL SERVIDOR	TIEMPO DE INTERRUPCIÓN DEL SERVIDOR	TIEMPO FUNCIONAMIENTO DEL SERVIDOR
1			
2			

TFS= TTS-TIS

1. TFS = Tiempo funcionamiento del servidor.
2. TTS = Tiempo de trabajo del servidor
3. TIS = Tiempo interrupción del servidor

Anexo N° 3. Guía de observación N°3

Emisión de vales de combustible

La estación de servicios emite vales de combustibles para las empresas que abastecen en el local, siendo así que a cada cliente se le asigna cierta cantidad de vales de combustibles para su utilización. Se presentan situaciones como datos inexactos en la entrega de vales al momento de facturación, vales consumidos irregularmente a manera de canje fuera de la estación.

Procedimiento

Los vales de combustible cuya entrega se realiza a los clientes de la estación de servicios están diferenciados por colores que se asignan por empresa en donde la cantidad de vales emitidos menos la cantidad de vales utilizados nos indicara la emisión total de los vales de combustible.

N°	CANTIDAD DE VALES EMITIDOS	CANTIDAD DE VALES UTILIZADOS	EMISIÓN DE VALES DE COMBUSTIBLE
1			
2			

EVC = CVE-CVU

1. ECV = Emisión de vales de combustibles
2. CVE = Cantidad de vales emitidos
3. CVU = Cantidad de vales utilizados

CUESTIONARIO N° 1

GRADO DE SATISFACCIÓN DEL PERSONAL ADMINISTRATIVO

Estimado usuario, en la encuesta presentada se está buscando conocer su satisfacción en la gestión de control implementada en la empresa para lo cual le agradecería responder a las preguntas establecidas con total transparencia.

¿Cómo calificaría usted la auditoria de seguridad para la implementación de un plan de control en los activos de la empresa?

a) Muy buena b) Buena c) Regular d) Mala e) Muy mala

¿Cree usted que al implementarse este control los activos de información que a diario incrementan estarán más seguros?

a) Siempre b) Casi siempre c) A veces d) Nunca e) Casi nunca

¿Cómo calificaría el plan de control de los activos de información que circula en la administración de la empresa?

a) Segura b) Insegura c) Nada confiable

CUESTIONARIO N° 2

GRADO DE SATISFACCIÓN DE GERENCIA

Estimado gerente, en la encuesta presentada se está buscando conocer su satisfacción en la gestión de control implementada en la empresa para lo cual le agradecería responder a las preguntas establecidas con total transparencia.

¿Ha notado cambios considerables en el control de seguridad que se ha implementado para los activos de información de la empresa?

a) Si b) No

¿Se ha logrado controlar el uso irregular y salida de información en cuanto a los vales de combustible de la estación?

a) Siempre b) Casi siempre c) No d) Poco

¿Suele caerse el servidor e interrumpir las tareas de facturación?

a) Si b) No

MATRIZ DE CONSISTENCIA

PROBLEMA	¿De qué manera influye la implementación de un plan de control y seguridad basado en la metodología Cobit en los activos de información en la Estación de Servicios San José?
HIPÓTESIS	Mediante la metodología COBIT es viable implementar el plan de Control y seguridad de los Activos de información en la Estación Servicios San José.
VARIABLES	**Variable dependiente** Control de activos de información **Variable independiente** Plan de control y seguridad
OBJETIVOS	**General** Implementar un plan de control y seguridad basado en la metodología Cobit para la mejora de los activos de información en la Estación de Servicios San José
	Específicos • Reducir la cantidad de errores que se presentan a diario en el proceso de facturación. • Minimizar la cantidad de caídas del servidor que maneja el sistema de la organización. • Controlar la emisión de vales emitidos visados por el área administrativa. • Elevar el grado de aceptación del personal con la gestión de control implementada en Estación de Servicios San José. • Incrementar la eficiencia en la toma de decisiones de los altos ejecutivos.

Estación de Servicios
San José S.A.C. N° 1

CARTA DE AUTORIZACIÓN

Yo, Gunter Martin Castillo Gallo, identificado con DNI N º 02833580, en calidad de representante legal de ESTACION DE SERVICIOS SAN JOSE S.A.C. con RUC Nº 20175642341 y domicilio legal Av. Grau 1602 Piura - Piura, le saluda cordialmente expresa lo siguiente:

Que la Srta. Gabriella Lucia Chira Castillo, identificado con DNI 47100561 trabajadora de nuestra empresa y quien fuera estudiante de la UNIVERISDAD CESAR VALLEJO -PIURA en el programa de experiencia laboral SUBE Carrera de Ingeniería de Sistemas, se le autorizó el acceso a la información de nuestra empresa para la realización de investigación de tesis denominada “Implementación de un Plan de Control y Seguridad de los Activos de Información en la Estación de Servicios San José”

Se extiende el presente documento para los fines convenientes

Piura, 09 de Junio del 2022

ESTACIÓN DE SERVICIOS SAN JOSÉ S.A.C.
Gunter Martin Castillo Gallo
GERENTE