UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Presentado por:

MILCIADES WILLY HUAMALÍ ALHUAY

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BAJO EL ENFOQUE DE LA ISO/IEC 27001 PARA LA EMPRESA ITS BUSINESS SAC - LIMA

Asesor:

DRA. NORMA LORENA CATACORA FLORES

Co-Asesor:

ING. ENRIQUE EDGARDO CONDOR TINOCO

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

ANDAHUAYLAS – APURIMAC – PERÚ

2021

Aprobación del Asesor

ANEXO 21

APROBACIÓN DEL ASESOR

Quién suscribe:

Dra. Norma Lorena Catacora Flores, por la presente:

CERTIFICA,

Que, el bachiller en: ***Ingeniería de Sistemas***, ***Milciades Willy Huamalí Alhuay,*** ha iniciado el proceso de asesoramiento y firmamos el compromiso hasta la culminación satisfactoria del Informe Final del Tesis intitulado:

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO EL ENFOQUE DE LA ISO/IEC 27001 PARA LA EMPRESA ITS BUSINESS SAC – LIMA"; para optar el Título Profesional de Ingeniero de Sistemas.

Andahuaylas, 28 de Septiembre de 2021

Dra. Norma Lorena Catacora Flores
Asesora

Bach. Milciades Willy Huamalí Alhuay

Acta de Sustentación

Universidad Nacional José María Arguedas

Identidad y Excelencia para el Trabajo Productivo y el Desarrollo

FACULTAD DE INGENIERIA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

ACTA DE SUSTENTACION DE TESIS

En la Universidad Nacional José María Arguedas ubicado en el distrito de San Jerónimo de la Provincia de Andahuaylas, siendo las 8:30 horas del día 03 de noviembre del 2021, se reunieron los docentes: Dr. Yalma Ponce Atencio, M.Sc. Herwin Huillcen Baca, Ing. Roberto Quispe Quispe, en condición de integrantes del Jurado Evaluador del Informe Final de Tesis intitulado: "DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BAJO EL ENFOQUE DE LA ISO/IEC 27001 PARA LA EMPRESA ITS BUSINESS SAC - LIMA", autor es el Bachiller en Ingeniería de Sistemas **Milciades Willy Huamalí Alhuay**, y su asesora la Dra. Norma Lorena Catacora Flores y Co-Asesor el Ing. Enrique Edgardo Condor Tinoco, con el propósito de proceder a la sustentación y defensa de dicha tesis.

Luego de la sustentación y defensa de la tesis, el Jurado Evaluador **ACORDÓ**: **Aprobar por Unanimidad** al Bachiller en Ingeniería de Sistemas **Milciades Willy Huamalí Alhuay,** obteniendo la siguiente calificación y mención:

Nota escala vigesimal		Mención
Números	Letras	
16	Dieciseis	Muy Bueno

En señal de conformidad, se procedió a la firma de la presente acta.

D.Sc. Yalmar Ponce Atencio
Presidente de Jurado

M.Sc. Herwin Huillcen Baca
Primer Miembro Jurado Evaluador

Ing. Roberto Quispe Quispe
Segundo Miembro Jurado Evaluador

Aprobación del Jurado Evaluador

ANEXO 31

APROBACIÓN DEL JURADO DICTAMINADOR

LA TESIS "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO EL ENFOQUE DE LA ISO/IEC 27001 PARA LA EMPRESA ITS BUSINESS SAC – LIMA"; para optar el Título Profesional de Ingeniero de Sistemas.

PRESIDENTE: DR. YALMAR TEMÍSTOCLES PONCE ATENCIO
PRIMER MIEMBRO: MSC. HERWIN HUILLCEN BACA
SEGUNDO MIEMBRO: ING. ROBERTO QUISPE QUISPE

Habiendo sido aprobado por UNANIMIDAD, en la ciudad de Andahuaylas el día 03 del mes de noviembre de 2021

Andahuaylas, 03 de noviembre de 2021

DR. YALMAR TEMÍSTOCLES PONCE ATENCIO
PRESIDENTE DEL JURADO DICTAMINADOR

MSC. HERWIN HUILLCEN BACA
PRIMER MIEMBRO del Jurado Dictaminador

ING. ROBERTO QUISPE QUISPE
SEGUNDO MIEMBRO del Jurado Dictaminador

Resultado de Informe de Similitud de la Tesis

Universidad Nacional José María Arguedas

Identidad y Excelencia para el Trabajo Productivo y el Desarrollo

Unidad de Investigación de la Facultad Ingeniería
C 003-2023

Andahuaylas, 07 de agosto de 2023

La unidad de investigación de la Facultad de Ingeniería, expide la:

Constancia

De porcentaje de similitud (27%) según el software Turnitin, al informe final de investigación: Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la ISO/IEC 27001 para la empresa ITS Business SAC - Lima. Presentado por el Bach. Milciades Willy Huamali Alhuay cuyo Asesor es la Dra. Norma Lorena Catacora Flores.

Ing. Juan José Oré Cerrón
Presidente de la Unidad de Investigación de la
Facultad de Ingeniería

C.c
Archivo.

08 AGO 2023

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS - FACULTAD DE INGENIERÍA - ANDAHUAYLAS

1

Reporte de similitud

NOMBRE DEL TRABAJO

TESIS WILLY HUAMALI CORRGIDO ULTIMO ok.pdf

AUTOR

Willy Huamali

RECUENTO DE PALABRAS

32076 Words

RECUENTO DE CARACTERES

182079 Characters

RECUENTO DE PÁGINAS

137 Pages

TAMAÑO DEL ARCHIVO

2.2MB

FECHA DE ENTREGA

Jun 12, 2023 10:53 PM GMT-5

FECHA DEL INFORME

Jun 12, 2023 10:55 PM GMT-5

27% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base c

- 27% Base de datos de Internet
- 5% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 10 palabras)

Resumen

27% de similitud general

Principales fuentes encontradas en las siguientes bases de datos:

- 27% Base de datos de Internet
- Base de datos de Crossref
- 5% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

FUENTES PRINCIPALES

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	repositorio.unsch.edu.pe Internet	14%
2	repositorio.unajma.edu.pe Internet	9%
3	hdl.handle.net Internet	2%
4	repository.poligran.edu.co Internet	1%
5	docplayer.es Internet	<1%
6	repositorio.uss.edu.pe Internet	<1%
7	repositorio.unal.edu.co Internet	<1%
8	repositorioacademico.upc.edu.pe Internet	<1%
9	repository.unad.edu.co Internet	<1%

Descripción general de fuentes

10	repositorio.unab.cl Internet	<1%
11	repositorio.uns.edu.pe Internet	<1%
12	Campos del Razo Dulce. "Administración de la seguridad en tecnología... Publication	<1%
13	"Arsénico en el campo geotérmico de El Tatio : especiación en sínteres... Crossref posted content	<1%
14	Aragon Cordova, John | Fernandez Luque, Renato | Quintero Diaz, Erika... Publication	<1%
15	qdoc.tips Internet	<1%
16	Carpio Ramirez, Alfredo. "Sistema de control de tiro para torpedos a bo... Publication	<1%
17	Hernández Rodríguez Jacob Benjamín. "Tutorial de seguridad informát... Publication	<1%
18	Campos Valdovinos Yesenia. "Administración de riesgos en las tecnol... Publication	<1%
19	Gaínza Sánchez Sabino Isao. "Propuesta de aplicación de una metodol... Publication	<1%
20	Padilla Espinosa Miriam Josefina. "La gestión de riesgos de seguridad ... Publication	<1%
21	Reyes Granados Magdalena. "Propuestas para impulsar la seguridad in... Publication	<1%

Descripción general de fuentes

22	Saavedra Flores Daniel. "Análisis de riesgos en la seguridad informátic... Publication	<1%
23	repository.udistrital.edu.co Internet	<1%

Descripción general de fuentes

Dedicatoria

A Dios y a la virgen de Cocharcas, por darme la vida y protegerme en cada momento, les debo todo lo que tengo y todo lo que soy.

A mi familia, especialmente a mis padres Aurelia y Marcelo, que con su amor y comprensión estuvieron ahí para guiarme y aconsejarme cada vez que los necesite, siendo ellos mi motivación y ejemplo para ser un hombre de bien.

A mis hermanos Elsa, Edwin, Liliana y Janeth, por su aliento y la confianza que han puesto en mí.

Agradecimientos

A Dios porque sin el nada de esto hubiera sido posible.

A mis padres y familiares, por confiar mí y en mis anhelos, por sus palabras de motivación, sus consejos, sus buenas vibras que fueron el motor para lograr este sueño, por enseñarme a persistir y luchar día a día para cumplir mis metas.

A la Dra. Norma Lorena Catacora Flores por su asesoría, sus consejos, motivaciones y por brindarme sus conocimientos para lograr desarrollar y culminar este proyecto.

A mis amigos y compañeros de trabajo de la empresa ITS Business SAC por haberme brindado su tiempo y apoyo para la realización de esta tesis y especialmente a la gerencia y los trabajadores de la entidad.

A mis profesores de la universidad que marcaron con sus enseñanzas mi futuro, gracias por prepáranos para un futuro competitivo profesionalmente y sobre todo para ser mejores personas.

A todos ellos con cariño.

INDICE

Índice de Tablas

Índice de Figuras

Resumen

En la actualidad las empresas y organizaciones consideran a la “información” como el mayor activo más valioso que poseen, por lo tanto, ponen más énfasis en su mejor y mayor y adecuada protección.

La norma ISO/IEC 27001, es un estándar internacional que realiza la certificación a los procesos de una compañía u organización en la gestión (uso) correcta de la seguridad de la información. Empresa que logre certificarse, está en la capacidad de demostrar a sus clientes actuales y potenciales tener la capacidad de proteger la información, así como también mejorar y disminuir los riesgos de fraude, perdida o filtración de información. Por consiguiente, el gobierno peruano aprobó la aplicación de la Norma Técnica Peruana (NTP) ISO/IEC 27001:2014, Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información.

La presente tesis se enfoca en el caso de estudio a la empresa ITS Business SAC para la cual se desarrolló el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo la norma NTP ISO/IEC 27001:2014, el proyecto se dividió en tres fases principales**: Diagnóstico inicial y aceptación:** se realizó un análisis inicial de la entidad y se evaluó su disposición para implementar el SGSI. **Estudio de la organización y su contexto:** se estudió la organización en detalle, se identificó el proceso crítico, se definió la política de seguridad y se estableció el alcance del sistema. Además, se creó un comité de seguridad de la información. **Análisis y gestión de riesgos:** se siguió una metodología de análisis y gestión de riesgos. Se identificaron y evaluaron los activos de información, se identificaron las amenazas y se calculó el impacto de los riesgos. Con base en estos resultados, se determinaron las medidas de control necesarias para mitigar los riesgos a un nivel aceptable. finalmente, se elaboró un documento llamado “Declaración de Aplicabilidad” que justifica que los controles del Anexo A de la NTP ISO/IEC 27001:2014 pueden ser implementadas en la organización. Esta declaración proporciona una guía clara sobre las medidas de seguridad necesarias y su justificación para proteger la información de la empresa, de acuerdo con (Escalante Coronel, 2019)

Palabras clave: Sistema de gestión de seguridad de la información, NTP ISO/IEC 27001:2014, riesgo, impacto, control de seguridad

Abstract

Nowadays, companies and organizations consider "information" as the greatest most valuable asset they possess, therefore, they place more emphasis on its best and adequate protection.

ISO/IEC 27001 is an international standard that certifies the organization's processes in the correct management of information security. The company that achieves certification, is able to demonstrate to its current and potential customers to have the ability to protect information, as well as improve and reduce the risks of fraud, loss or leakage of information. Consequently, the Peruvian government approved the use of the Peruvian Technical Standard ISO/IEC 27001:2014, Security Techniques. Information Security Management System.

This thesis focuses on the case study of the company ITS Business SAC, for which the design of an Information Security Management System (ISMS) was developed following the NTP ISO/IEC 27001:2014 standard, the project It was divided into three main phases. Initial diagnosis and acceptance: an initial analysis of the entity was carried out and its willingness to implement the ISMS was evaluated. Study of the organization and its context: the organization was studied in detail, the critical process was identified, the security policy was defined and the scope of the system was established. In addition to creating an information security committee. Risk analysis and management: a risk analysis and management methodology was followed. Information assets were identified and evaluated, threats were identified, and the impact of risks was calculated. Based on these results, the necessary control measures were determined to mitigate the risks to an acceptable level. Finally, a document called "Statement of Applicability" was prepared that justifies that the controls of annex A of the NT ISO/IEC 27001:2014 standard can be implemented in the organization. This statement provides clear guidance on the necessary security measures and their justification to protect company information. According to (Escalante Coronel, 2019)

Keywords: Information security management system, NTP ISO/IEC 27001:2014, risk, impact, security control.

Chumasqa

Khunanqa, chay simi chaskiykunapas qhawarisqan kan chay huñunakuy ukhupi, allin huntayninkunapas, chayraykun munakun huq allin q`imiqta.

Kamachina ISO/IEC 27001, huq unanchaymi tiqsi muyuntinpi akllan llapan ruwayninkunata hinaspa unanchan chay huñunakuy ukhupi chay willakuymanta allinkaq ruwaykunata akllarinku. Mayqin ruruchiqchus llallipan unanchayta paymi yuyaykusqa riqsirichispa llapan khunan rantiqrunankunata kallpanchaspa willakuyta khuyarinanpaq, hinallataqmi wiñarichinqa huch`uyachinqataq mana allin waqllichisqa q`iwisqa willakuykunata, hina qhipampi umalliq kamachikuq peru suyomanta nimun kamachisqa ruwaykunata yachanapaq khuyanakuyta ima allin qhalillata willanakuspa ruwanata ISO/IEC 27001:2014.

Khunankaq yachay qelqasqamanqa akllirikamunmi imaymana yachaqaykuna wiñarichik hatun ITS Business SAC nisqaukhumanta, hinaspa wakichikullarantaq chay huñukuy NTP ISO/IEC 27001:2014 ukhupi willakukuyna kinsa t`aqaman p`akikunampaq: ñaupaqkaq t`aqasqapin qallarikun chiy qawariy y chaninchariy y munasqa kayninpan, iskaykaq t`aqapin yacharikun chay huñunakuykunata y yanapaqkunantapas chay uhupin taririkun imaymana huñuchikkunamanta, ahinapin tukukapun chay yanapay huñunakuy, hinaspapas yachakulllantaqmi pin chay uhupi kamachikuqtapas, q`imiqninkunatapas sispallapi kanankupaq. kinsakaq t`aqapitaqmi qatikuran chaninchaykunata hinaspa qhawarikuran allinta, mana allintawan.chay uhupin tarikuran allinta chay willakuykunata mat`irispa aparinapaq, hinaspa tarikullantaq mana allin manchariykunapas, khutuyariykunapiwan, chay hinapi qallarisqa huk qillqa mayt`u rikcharichin, paykunan atinku rikcharichiyta Anexo A nisqa chay NTP ISO/IEC 27001:2014 qhawariykunapan huñunasqa ukhupi.

**Huntap`ay Rimaykuna:** huñunasqa qallarichiqkuna chay willanakuymanta NTP ISO/IEC 27001:2014, kanman sasachakuypas, hark`anakuspa allinyanapaq.

INTRODUCCIÓN

La seguridad de la información se ha convertido en una preocupación que va en aumento en las compañías en todo el mundo en los últimos años, debido a los avances tecnológicos y a los cambios en la modalidad de trabajo (homework) a los cuales fueron adaptándose las empresas, ante ello se incrementó de forma masiva las amenazas y vulnerabilidades representando un riesgo al materializarse ya que generara un costo económico, sanciones legales, afectación de su imagen y reputación.

En cualquier empresa u organización la información se reconoce como uno de los recursos más preciados, por lo que es esencial proporcionarle una protección adecuada y garantizar su confidencialidad, integridad y disponibilidad.

En consecuencia, la empresa ITS Business SAC consciente de los posibles riesgos y de estar expuesta a las diversas amenazas que pueden atentar contra la seguridad y confiabilidad de la información propia y la de sus clientes, así como el peligro de pérdida o filtración en cualquier momento, reconoce la importancia de tener una plan de continuidad de negocio, este plan tiene como objetivo hacer frente a cualquier situación improvista de manera ágil y oportuna, permitiendo la pronta reanudación de las operaciones en el menor tiempo posible

En la presente tesis tiene como objetivo principal diseñar un SGSI para la empresa ITS Business SAC, utilizando la perspectiva de la norma peruana NTP ISO/IEC 27001:2014, para lograr esto se recopilo la información necesaria y se realizó un diagnóstico del estado actual de la empresa, conforme a la seguridad de la información. Una vez obtenido el diagnostico, se llevó a cabo un análisis de riesgo para identificar las posibles amenazas y vulnerabilidades que enfrenta la empresa en relación con la seguridad de la información. Con base a este análisis, se propusieron y diseñaron políticas de seguridad adecuada para mitigar los riesgos identificados.

Finalmente, la tesis presenta conclusiones que abordan cada uno de los objetivos planteados inicialmente. Además, se proporcionan recomendaciones que pueden ayudar a mejor el trabajo realizado y su posible implementación en la organización a futuro.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Realidad problemática

Vivimos en un mundo globalizado y competitivo en el que las compañías se encuentran diariamente con nuevos desafíos.

En el mundo actual, la información se ha vuelto extremadamente valiosa para muchas empresas. Los datos son ahora un componente fundamental para lograr ventajas competitivas y los altos niveles de rentabilidad en los negocios de hoy en día.

Seguridad de la Información es la preservación de la confidencialidad, la integridad y la disponibilidad de la información (NTP ISO/IEC-17799, 2015), es decir, buscar prevenir y proteger de ataques físicos como robos, incendios, así como también de ataques cibernéticos vulnerando la fragilidad de la seguridad de los sistemas.

Para Álvaro Gómez, Master en Seguridad Informática por la UNIR la seguridad de la información es “cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema” (Gomez Vieites, 2011)

Según el último reporte de seguridad en Latinoamérica elaborado por Eset, la tecnología no lo es todo en el campo de la seguridad de la información y es preciso complementarlas con una adecuada gestión. En ese sentido la implementación de políticas de seguridad es una de las prácticas más utilizadas en este campo, pero los niveles de implementación son demasiados bajos. Esto indica que las empresas de países como Ecuador (35%) y Perú (42%) son los que menos tienen implementadas. Costa Rica

(70%) lidera la lista dentro de 13 países latinoamericanos encuestados. (Harán , 2019)

Las empresas, independientemente de su tamaño, están realizando grandes esfuerzos en custodiar la información desde su origen hasta su aprovechamiento para las operaciones y para la toma de decisiones. Lo cual es una función entendible, dada la cantidad de datos que se generan a diario y desde diferentes fuentes. Las redes sociales, los dispositivos móviles, el comercio electrónico, la era de Big Data, etc. (Quero, 2019).

ITS BUSINESS S.A.C es una compañía establecida y confiable, con una trayectoria de más de 15 años en el Perú, nuestro enfoque principal es ayudar a las empresas a mejorar su eficiencia y productividad a través de la automatización, organización y la gestión efectiva. Brinda servicio de softwares para todo tipo de empresas. Dentro de sus productos se encuentran los siguientes:

- ✓ Sistema VisualCont software recomendado para la Gestión contable
- ✓ Sistema VisualPlan software recomendado para la Gestión de Planillas
- ✓ Sistema VisualFact software para la Gestión de Stock y Ventas
- ✓ Facturador Electrónico software recomendado para la Gestión estados de ventas electrónicas.

Esta empresa cuenta con más de mil clientes a quienes brinda asesoramiento, soporte técnico, capacitaciones entre otros, generando una enorme afluencia de información, para ello cuenta con el área de sistema, quienes velan por mantener los Software actualizados acorde a la necesidad de sus clientes. Pero como en muchas de las empresas peruanas se da poco valor e importancia a la seguridad de la información. En base a la información proporcionada, se identificaron las siguientes deficiencias en la empresa ITS Business SAC:

- Falta de una política de seguridad de la información
- Ausencias de un plan de gestión de riesgos de información
- Carencia de un plan de seguridad de la información.
- Control insuficiente de los accesos de los usuarios a la información
- Gestión Inadecuada de incidentes de seguridad de la información

1.2 Formulación del problema

1.2.1 Problema General

¿Cuáles son las características que debe tener un sistema de gestión de seguridad de la información adecuado para la empresa ITS BUSINESS SAC? (Escalante Coronel, 2019)

1.2.2 Problemas Específicos

- ¿Cuál es el alcance que se debe considerar en el diseño del SGSI para la empresa ITS BUSINESS SAC?

- ¿Cuáles son los resultados obtenidos al realizar el análisis de riesgo del (SGSI) en la empresa ITS BUSINESS SAC?

- ¿Qué controles de seguridad son aplicables para el diseño del SGSI para la empresa ITS BUSINESS SAC?

1.3 Objetivos

1.3.1 Objetivos General

El objetivo principal es diseñar un Sistema de Gestión de Seguridad de la Información para la empresa ITS BUSINESS SAC, siguiendo las pautas establecidas en la norma NTP ISO/IEC 27001.

1.3.2 Objetivo general

- Definir el alcance del diseño del Sistema Gestión de Seguridad de la Información (SGSI) para la Empresa ITS Business SAC

- Realizar una evaluación exhaustiva de los riesgos de seguridad de información para la empresa ITS Business SAC

- Crear una lista de medidas de seguridad que ayuden a reducir los riesgos identificados en el diseño del SGSI para la Empresa ITS Business SAC

- Obtener la certificación ISO/IEC 27001 para la empresa ITS Business SAC

1.4 Justificación

El presente trabajo de investigación, el sistema de gestión diseñado se basa en los principios establecidos en la norma NTP ISO/IEC 27001:2014, que proporciono un marco sólido para la Gestión de Seguridad de la Información para la empresa ITS Business SAC, este sistema permitió identificar procesos críticos, evaluar riesgos y establecer controles para proteger la información de la empresa luego de un análisis exhaustivo de sus procesos.

La importancia de contar con una empresa que tenga definida un SGSI con capacidad de respuesta ante una eventualidad de tal forma pueda tomar acciones preventivas y correctivas para evitar comprometer a datos confidenciales o en el peor de los casos ser víctima de pérdida de información valiosa.

La investigación tiene un impacto organizacional en seguridad de la información en la empresa ITS Business, en el ámbito laboral se generará un ambiente de confianza en el manejo de la información y mejorará con el buen desempeño del personal en la empresa.

En el aspecto social la empresa ITS Business transmitirá a sus clientes una imagen de confianza y seguridad con respecto a la gestión de la información.

En lo económico el impacto que generara el SGSI en la entidad quede ser positivo, ya que ayuda a evitar costosos incidentes de seguridad, mejorar la eficiencia operativa, reduce inversiones innecesarias en seguridad y tecnología. Al proteger la información de manera efectiva, la empresa mantendrá una buena reputación, minimizar los riesgos y aprovechar las oportunidades en un entorno empresarial cada vez más digital.

La empresa generara una imagen de liderazgo ante sus pares en la región. Al implementar el SGSI la empresa identificara, clasificará, lo valorara y tratar de manera adecuada los riegos de seguridad identificados.
De esta manera la investigación beneficiara a la empresa ITS Business SAC.

1.5 Delimitación

La presente investigación es realizada en la empresa ITS BUSINESS S.A.C, sin embargo, los resultados de la presente investigación pueden replicarse en las demás empresas que estén en el mismo rubro.

Debido al tipo de proyecto y al tiempo establecido solo se procederá a la fase del análisis y diseño de SGSI, pero no abarca la fase implementación por tiempo que requeriría.

Se iniciará el 01 de julio del 2020 y se concluirá en septiembre del 2021

Los Ejes temáticos; donde se circunscribe el problema de investigación serán: seguridad de la información, ISO/IEC 27001, riesgo, políticas de seguridad y mejora continua.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de investigación

- (Aguirre Mollehuanca, 2014) en su investigación “Diseño De Un Sistema De Gestión De Seguridad De Información Para Servicios Postales Del Perú S.A.” tesis para optar el título de ingeniero informático en la Pontificia Universidad Católica Del Perú, se planteó como objetivo general Diseñar un sistema de gestión de seguridad de información para SERPOST según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de seguridad de información, llegando a la conclusión que el apoyo de la alta gerencia para el diseño de este sistema de gestión fue imprescindible, debido a que fue necesaria su intervención para ayudar a concientizar a los jefes de área y dueños de los procesos a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga. Esta tesis se tomó como referencia la estructura del desarrollo para el diseño del SGSI para la empresa ITS Business SAC.

- (Guzman Silva, 2015) en su investigación “Diseño De Un Sistema De Gestión De Seguridad De La Información Para Una Entidad Financiera De Segundo Piso ”Trabajo de Grado en la Institución Universitaria Politécnico Grancolombiano, Colombia, se planteó como objetivo general “ Diseñar un Sistema de Gestión de Seguridad de la Información para la empresa IGM S.A., tomando como referencia la norma NTC-ISO-IEC 27001:2013”, llegando en una de sus conclusiones de que el nivel de cumplimiento de la entidad frente de los requerimientos de la norma ISO/IEC 27001:2013, es del 46%, lo que significa que la implementación del SGSI implicará a la entidad un refuerzo considerable debido a la ausencia de controles o al bajo grado de cumplimiento de muchos de ellos. Se hace imprescindible que los altos directivos aprueben y establezcan políticas de seguridad con el objetivo asegurar que estas sean implementadas, actualizadas y

cumplidas adecuadamente para su funcionamiento continuo. En consecuencia, la empresa financiera que fue objeto de estudio en esta tesis tiene un proceso de gestión de activos y recursos similares a la que tiene la empresa ITS Business SAC, por lo tanto, ayudo en el diseño del SGSI.

- (Ccesa Quincho, 2016) en su investigación "Diseño De Un Sistema De Gestión De Seguridad De La Información Bajo La NTP ISO/IEC 27001:2014 Para La Municipalidad Provincial De Huamanga, 2016" tesis para optar el título profesional de Ingeniero informático en la Universidad Nacional De San Cristóbal De Huamanga, se planteó como objetivo principal Determinar las características del diseño de un Sistema de Gestión de Seguridad de la Información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, llegando a la conclusión de determinar cómo características esenciales del diseño del SGSI para la Municipalidad Provincial de Huamanga, el compromiso y apoyo de la alta dirección, el conocimiento de la organización, la adecuada identificación del alcance del SGSI, la evaluación de riesgos y la mejora continua. Así determino que, el análisis y gestión de riesgos es el eje principal para evaluar y elaborar los posibles riesgos a los que está expuesta la información, al analizar el riesgo se identifican las amenazas potenciales y evaluar su probabilidad de ocurrencia, esta información cuantitativa ayuda a tomar mejores decisiones informadas. Por lo tanto, esta tesis se tomó como referencia para desarrollar el diagnóstico de la situación actual de la empresa ITS Business S.A.C con relación a la norma ISO 27001 y para el análisis de riesgo ya que uso la metodología Magerit versión 3.

- (Escalante Coronel, 2019) en su investigación “Diseño de un Sistema de Gestión de Seguridad de la Información Bajo El Enfoque De La NTP ISO/IEC 27001 Para La Dirección De Salud Virgen De Cocharcas – Chincheros” tesis para optar el título profesional de ingeniero de sistemas en la Universidad Nacional José María Arguedas – Andahuaylas, se planteó como objetivo general Implementar un Diseño de un Sistema de

Gestión de Seguridad de la Información bajo el enfoque de la NTP - ISO/IEC 27001:2014 para la Dirección de Salud Virgen de Cocharcas - Chincheros. Para el análisis de riesgo utilizo el método octave llegando a una de sus conclusiones el desarrollo de los controles de seguridad para reducir a lo más mínimo los riesgos a los que está expuesto los recursos (activos) y la información de la DSVC – Chincheros. En tanto, esta tesis se tomó como referencia para adecuar la norma ISO 27001:2014 en el proceso de gestión de seguridad de la información para la empresa ITS Business SAC y para realizar los controles para el tratamiento de riesgo.

2.2 Bases teóricas

2.2.1 Información

La información “comprende los datos y conocimientos que se usan en la toma de decisiones” (Hirt & Ferrell, 2004)

“Es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones” (Chiavenato, 2006)

2.2.2 Sistema de información

Un sistema de información (SI) es un conjunto de elementos diseñados recopila, administrar y procesar datos e información de manera organizada, con el propósito de satisfacer una necesidad o alcanzar un objetivo determinado. Estos elementos están listos para ser usados posteriormente por la entidad.

2.2.3 Seguridad de la Información

La seguridad de la información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información según (INDECOPI, 2014)

De acuerdo a la Asociación Española para la Calidad, la Seguridad de la Información tiene como propósito la protección de la información y de los sistemas de la información contra las amenazas y eventos que atenten con el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada.

La confidencialidad, garantiza que solo los individuos, entidades o procesos autorizados tengan permiso a acceder a la información y que esta no se divulgue o se ponga a disposición de personas no autorizadas (ISO27000.ES, 2005)

La disponibilidad, acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo necesiten (ISO27000.ES, 2005)

La integridad, mantener la exactitud y completitud de la información y los métodos de procesos asociados (ISO27000.ES, 2005)

La autenticidad, Propiedad que una entidad es lo que dice ser. Es la seguridad de que un mensaje, una transacción u otro intercambio de información proviene de la fuente de la que afirma ser (UNE-ISO/IEC 27000:2014)

2.2.4 Sistema de Gestión de Seguridad de la Información

El sistema de gestión para la Seguridad de la información se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan a la seguridad de la información en una empresa u organización (ISO/IEC 27001, 2013)

Además, la Gestión de la Seguridad de la Información se encarga de implementar y mantener programas, controles y políticas de

seguridad para proteger la información de la empresa es sus tres aspectos fundamentales que son: la confidencialidad, integridad y disponibilidad.

(Goméz Fernández & Fernández Rivero , 2015) Definen al sistema de gestión de seguridad de la información como un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización. Así mismo mencionan que la implementación de un SGSI supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada. Fundamentalmente se distinguen dos tipos de procesos (2019)

1. Procesos de gestión. Controlan el funcionamiento del propio sistema de gestión y su mejora continua.

2. Procesos de seguridad. Se centran en los aspectos relativos a la propia seguridad de información.

2.2.5 Riesgo

El riesgo es la posibilidad de enfrentar situaciones adversar que pueden resultar en daños o perdidas.

También podemos referirnos al riesgo a la probabilidad de que ocurra un evento no deseado y las consecuencias negativas que puede acarrear. Este riesgo se compone de dos elementos principales: la amenaza, que es la probabilidad de que ocurra el evento y la vulnerabilidad es la debilidad ante dicho evento.

(MAGERIT, 2012) “refiere el riesgo a la probabilidad de que ocurra un evento y que cause un impacto negativo en un activo o en un dominio especifico de la organización. Esto implica que existe la posibilidad de

que algo malo suceda y cause un daño, perdida o interrupción en el lugar donde se encuentra el activo o dominio. El riesgo está relacionado en evaluar y estimar cuan problemas que se ocurra dicho evento y cuales podrían ser las consecuencias".

Análisis de riesgo

"El objetivo de realizar el análisis de riesgos es fundamental para identificar y evaluar los factores de riesgo que pueden afectar a la organización. Este plan conlleva a determinar los activos y el impacto provocado por los riesgos, calificándolos y evaluándolos con el objetivo de obtener información importante para luego implementar medidas de seguridad y la respuesta a incidentes de esta forma reducir la probabilidad de que ocurran los riesgos identificados y minimizar su impacto en caso se materialicen" (Guanoluisa Huertas & Maldonado Soliz , 2015).

MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas (Gutiérrez Amaya, 2013)

2.2.6 ISO 27001

La ISO 27001 es una norma internacional que establece los requisitos mínimos para un sistema de gestión de seguridad de la información (SGSI). El objetivo de esta norma es proporcionar un marco de buenas prácticas para identificar, analizar e implementar los controles necesarios para gestionar y mitigar los riegos relacionados con la seguridad (LRQA Entidad ceriticadora ISO 27001, s.f.)

La norma ISO 27001 es certificable en cualquier organización independientemente de su tamaño, previo a un proceso de evaluación por una entidad independiente, quien verifica si cumple con los requisitos que exige esta norma. Esta certificación trae

condigo muchos beneficios en la entidad que lo obtenga, genera confianza entre sus socios y clientes ya que cumplirá con normas reguladoras y mostrara un compromiso con la seguridad de la información.

La norma ISO 27001 es un estándar internacional que establece los requisitos mínimos para implementar de SGSI, su objetivo es garantizar la conservación de datos y sistema de información contra el acceso, uso, divulgación o destrucción no autorizada.

La Seguridad de la información, según la norma ISO 27001, en un conjunto de medidas y controles que se implementan para salvaguardar la confidencialidad, disponibilidad e integridad de la información relevante de una organización. Esta información encontrase en diversos formatos ya sea en digital o físico.

2.2.7 Norma Técnica Peruana (NTP) ISO/IEC 27001:2014

(INDECOPI, 2014) “la norma NTP - ISO/IEC 27001:2014 es una adaptación de la ISO/IEC 27001. La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico, dispone el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014, tecnología de la información, técnicas de seguridad, Sistema de Gestión de Seguridad de Información”

Esta NTP fue creado con el propósito de establecer los requerimientos elementales para desarrollar, implementar, mantener y mejorar de manera constante un SGSI. La implementación de este sistema está influenciada por la necesidad y metas específicas de la organización, así como por los requisitos de seguridad, el tamaño y la estructura de la misma por ello elección de adoptar un sistema de gestión de seguridad de la información es una decisión estratégica que debe tomar una organización. (Escalante Coronel, 2019)

2.2.8 Estructura de la NTP - ISO/IEC 27001:2014

(Excellence-ISOTools, 2015) “la norma ISO 27001:2013 (en el Perú NTP - ISO/IEC 27001:2014) no sólo establece cambios en el contenido (respecto a la ISO 27001:2005) sino también en la estructura, lo que verá reflejado en otros documentos que forman parte de la familia ISO 2700. La norma ISO 27001, en la que se proporciona un formato y un conjunto de alineamiento que siguen el desarrollo documental de un sistema de gestión sin que le importe el enfoque empresarial, se alinean bajo la misma estructura todos los documentos que se relacionan con el sistema de gestión de seguridad de la información y así se evitan problemas de integración con otros marcos de referencia”.

La organización (estructura) de esta norma se establece de la siguiente manera:

1. Introducción
2. Objeto y campo de aplicación
3. Referencias normativas
4. Términos y definiciones
5. Contexto de la organización
6. Liderazgo
7. Planificación
8. Soporte
9. Operación
10. Evaluación de desempeño
11. Mejora
12. Anexo A -lista de controles

(Excellence-ISOTools, 2015)

2.2.9 Ciclo de mejora continúa

La ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming”: PDCA – acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), siendo éste un enfoque de mejora continua:

- **Plan (Planificar):** En esta fase se planifica la implantación de SGSI. Se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos.
- **Do (Hacer)**: Se implementa y pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas.
- **Check (Verificar):** En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente.
- **Act (Actuar):** En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase**”** (Goméz Fernández & Fernández Rivero , 2015)

Figura 1: Ciclo PDCA en ISO/IEC

Fuente: *https://images.app.goo.gl/aodQ6RX5rwRMS4oAA*

2.2.10 Magerit

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de

España, que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno, esta metodología es de carácter público y puede ser usada libremente sin ninguna restricción (Portal de Administración Electrónica, 2016).

Objetivos de Magerit

Directos:

1. Crear conciencia entre los líderes de las organizaciones sobre los riesgos y la importancia de manejarlos adecuadamente
2. Proporcionar un enfoque estructurado para evaluar los riesgos asociados al uso de tecnologías de la información y comunicaciones
3. Contribuir con la identificación y planificación de medidas necesarias para mantener los riesgos controlados de manera oportuna

Indirectos:

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso (MAGERIT, 2012).

La gestión de riesgos, MARGERIT divide el proceso en dos subprocesos principales:

Análisis de Riesgos:

En este subproceso implica a identificar y tener conocimiento de los posibles riesgos que podrían afectar a un proyecto, proceso o una organización.

a. Identificar los activos más importantes para la entidad, entender su relación entre sí y determinar su valor. También se evaluar el costo o daño que produciría si de degradan estos activos.

b. Identificar las amenazas a las que están expuestos esos activos. Esto implica identificar las posibles fuentes o eventos que podrían causar daño o perdida a los activos.
c. Evaluar las salvaguardas existentes, es decir, las medidas de protección implementados para mitigar los riesgos. Se analiza la efectividad y se determina si son adecuadas para hacer frente a las amenazas antes identificadas.
d. Estimar el impacto que podría tener la materialización de una amenaza en los activos. Esto conlleva a evaluar la pérdida o daño que podría ocurrir si se hace realizar una amenaza.
e. Estimar el riesgo, que se define como el impacto potencial multiplicativo por la probabilidad de que ocurra la amenaza, es decir, se evalúa la magnitud del riesgo con el impacto como probabilidad de que la amenaza ocurra.

2.2.11 Octave

La Metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Es una metodología que estudia los riesgos en base a tres principios confidencialidad, integridad y disponibilidad, además esta metodología está desarrollada para MPYMES.

La metodología OCTAVE consta de tres fases principales:

- **Fase 1 Visión de organización**: se centra y enfoca en los siguientes elementos: activos, amenazas, vulnerabilidades de organización, requerimientos de seguridad y normas existentes.

- **Fase 2 Visión tecnológica:** está clasificado en dos eleméntenos principales que son: componentes claves y vulnerabilidades técnicas.

- **Fase 3 Elaboración de estrategias y reducción de los riesgos:** se divide en tres elementos que son: evaluación de los riesgos, estrategia de protección, estrategias de reducción de los riesgos (López Jaramillo & Vásquez Mejía, 2016).

Beneficios del método OCTAVE:

- Esta metodología ayuda a identificar los riesgos de seguridad que podrían afectar en la organización en el proceso de lograr sus objetivos. Atreves de este análisis las organizaciones pueden tener un panorama más claro sobre los riesgos a los que se enfrentan.

- Esta metodología proporciona un marco estructurado para evaluar los riesgos de seguridad de la información y con ello ayudar a las organizaciones a analizar y comprender sobre la probabilidad de que algún riesgo se materialice y el impacto que podría ocasionar.

- Estrategia de protección: después de haber identificado y evaluado los riesgos esta metodología ayuda a las organizaciones a desarrollar una estrategia de protección. En ello se establecen acciones y regulaciones importantes con el objetivo de disminuir los peligros asociados a la seguridad de la información.

- Así mismo ayuda con el cumplimiento normativo, debido a la evaluación integral de los riesgos y desarrollar una estrategia de adecuada protección, esta metodología ayuda a las organizaciones a satisfacer las regulaciones y estándares de seguridad de la información. Al hacerlo, muestra que esta cumpliendo con las normas establecidas en el ámbito de SI.

2.2.12 Política de seguridad

Las políticas de seguridad son un conjunto de reglas y pautas establecidas para garantizar la protección de la información y los sistemas de una empresa contra amenazas informáticas.

Para (R. Peltier, Peltier, & Blackley, 2005) la política de seguridad de información es considerada como una arquitectura fundamental que

establece los lineamentos y objetivo generales para proteger la información dentro de la organización. A partir de esta política se derivan otros documentos importantes como directivas, estándares, procedimientos y guías.

Por otro lado, la política de seguridad de la información cumple dos roles importantes, tanto internos como externo que a continuación se detalla:

- **En Su Rol Interno:** En este rol se define las responsabilidades de cada uno de los miembros que integran la organización en los que respecta a la protección y seguridad de la información. Se establece lo que se espera de cada uno de los colaboradores y como se realizara la evaluación, de esta forma sepan como contribuir en la seguridad de la información en su trabajo diario.

- **En Su Rol Externo:** La política de seguridad de la información tiene la función de mostrar a los demás como se trabaja dentro de la organización en términos de protección de la información, esto muestra públicamente que la organización es consciente de la importancia de proteger la información propia y la de sus clientes. De esta manera muestra al mundo exterior su compromiso y esfuerzo para lograr un entorno confiable y seguro para sus activos de información (Ccesa Quincho, 2016).

2.2.13 Oficial de seguridad de la información

El oficial de seguridad informática (OSI), es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización.

El Oficial de seguridad informática tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la organización (M. Farias-Elinos, 2004).

2.3 Marco Conceptual

SGSI: Sistema de Gestión de Seguridad de la Información.

Alta dirección: Persona o grupo de persona que dirige y controla una organización y tiene el poder de delegar autoridad y proporcionar recurso dentro de la organización (ISO/IEC 27001, 2013).

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO 27000, 2018)

Causa: factor que origina incidentes o produce un efecto o resultado específico.

Activo de información: cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para la organización (ISO 27000, 2018) .

Ciclo de Deming: Ciclo PDCA (Plan, Do, Check, Act) es un enfoque de gestión y mejora continua para la implementación de un sistema de mejora continua.

Colaborador: En una persona que trabaja en conjunto con otros para lograr un objetivo común aportando conocimientos, habilidades y esfuerzos para alcanzar resultados y metas.

Controles: Son contramedidas que incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo (ISO 27000, 2018).

Impacto: Consecuencias que sobre un activo tiene la materialización de una amenaza (MAGERIT, 2012)

Oficial de seguridad: Es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización.

Probabilidad de Ocurrencia: es una medida de posibilidad de que ocurra una situación o evento específico.

Riesgo: Es la posibilidad de que las amenaza exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a una organización (ISO/IEC 27001, 2013).

Aceptación del Riesgo: Decisión informada de tomar un riesgo particular, aceptación del riesgo puede ocurrir sin tratamiento de riesgo o durante el proceso de tratamiento de riesgo (UNE-ISO/IEC 27000:2014).

Confidencialidad: Propiedad que indica que la información no esté disponible o a disposición o se divulgue a personas, entidades no autorizados (UNE-ISO/IEC 27000:2014)

Disponibilidad: Propiedad de indica que la información sea accesible y utilizable por aquellas personas o entidad debidamente autorizadas (UNE-ISO/IEC 27000:2014, 2014).

Integridad: Propiedad que determina el salvaguardar la exactitud y estado completo de los datos (UNE-ISO/IEC 27000:2014).

Vulnerabilidad: Debilidad de un activo de información que puede ser aprovechada y/o explotada por una o más amenazas por falta o ausencia de controles de seguridad (UNE-ISO/IEC 27000:2014).

CAPITULO III

DEFINICIÓN DE VARIABLE

3.1 Operacionalización de la variable

- **X. diseño de un sistema de gestión de seguridad de la información (SGSI)**

  Es un marco de trabajo estructurado, se refiere al proceso de planificar y establecer un sistema que permita proteger la información y garantizar su seguridad dentro de la organización, estableciendo un conjunto de políticas, procedimientos y controles para gestionar y minimizar los riesgos.

  Indicadores

  - **X1 - Alcance:** “Aclara los límites del SGSI en función del contexto y/o importancia y ubicación de los activos críticos de información de la organización. Es el ámbito de la organización que queda sometido al SGSI” (ISO 27000, 2018).

  - **X2 - Análisis de riesgo:** Es el proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. La cual proporciona la base para la estimación de riesgos y su tratamiento (ISO 27000.ES, 2018).

  - **X3 - Controles de seguridad:** “los controles son medidas establecidas, como políticas, procedimientos y estructuras organizativas, que se implementan para mantener los riesgos de seguridad de la información en un nivel aceptable. Los controles también se consideran salvaguardas. En términos más simples, un control es una medida que se adopta para modificar o mitigar el riesgo” (ISO 27000, 2018).

3.2 Definición operacional de la variable

en ese estudio de investigación se emplea el enfoque de descomposición para definir operacionalmente la variable de investigación. Esto implica analizar los distintos componentes o elementos que conforman la variable diseño de un sistema de gestión de seguridad de la información, ya que se pretende estudiar cada uno de ellos de manera individual.

Tabla 1. *Operacionalización de la Variable de un SGSI*

VARIABLE	INDICADORES	INDICE	ITEMS
X. DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**1. Alance**	1.1. Aspectos externos e internos relevantes para el SGSI 1.2. Requisitos de las partes intercedas relevantes al SGSI	1. ¿Cuál es la razón para la implementas un diseño de SGSI? 2. ¿A qué grupo o partes interesa que se establezca y se implemente el SGSI? 3. ¿En qué ámbito o proceso se requiere la cobertura por parte del SGSI?
	2. Análisis de riesgo	2.1. Inventario de activos 2.2. Identificar los riesgos 2.3. Probabilidad e impacto del riesgo 2.4. Propiedades del riesgo	1. ¿Qué recursos de datos/información de esenciales para que la dependencia logre sus objetivos y estén alineados con los objetivos de la organización? 2. ¿Qué recursos de tipo servicio, software y hardware son fundamentales para que la dependencia logre sus objetivos de la organización? 3. ¿Qué dispositivos físicos utiliza la dependencia para almacenar información de forma permanente o por largos periodos de tiempo? 4. ¿Qué recursos respaldan los sistemas de información? 5. ¿Cuáles son las amenazas a las que enfrentan y que impacto podrían tener en los recursos? 6. ¿Cuál es la probabilidad de que ocurra o se materialice alguna de estas amenazas? 7. ¿Qué consecuencias tendría para los recursos si se materializa una amenaza? 8. ¿Cuál es nivel de riesgo al que se exponen los recursos?
	3. Controles de seguridad	3.1. Criterios de aceptación de riesgo 3.2. Políticas de seguridad 3.3. Roles y responsabilidades	1. ¿Cuál es el nivel de riesgo que la ITS BUSINESS SAC está dispuesto a asumir? 2. ¿Qué estrategias de gestión de riesgos se van a elegir? 3. ¿Qué acciones de protección se van a implementar?

Fuente: Adaptada de (Escalante Coronel, 2019)

CAPITULO IV

METODOLOGÍA DE INVESTIGACIÓN

La metodología utilizada en esta investigación considera como punto de partida la norma NTP - ISO/IEC 27001:2014. Esta norma describe los pasos y acciones necesarias para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Al adoptar esta metodología se garantiza que se están teniendo en cuanta los estándares y mejores prácticas establecidas en dicha norma.

4.1 Nivel de investigación

El nivel de investigación de la presente tesis llevar una investigación de nivel descriptivo que se centran en identificar y describir las características fundamentales del diseño de un “Sistema de Gestión de Seguridad de la Información” (SGSI). El enfoque esta investigación se basa en la Norma Técnica Peruana (NTP) ISO/IEC 27001:2014 para la ITS BUSINESS SAC como caso de estudio.

4.2 Diseño de la investigación

El diseño de investigación de esta tesis se caracteriza por no ser experimental - Transaccional descriptivo.

4.3 Población

La población estuvo conformada por los empleados y/o colaboradores de la empresa ITS Business SAC.

4.4 Muestra

Se utiliza un método de muestreo no probabilístico basado en el juicio de experto y criterio de Saturación, la cual consistió en seleccionar a seis trabajadores del área de sistemas de la Empresa ITS Business SAC para formar parte de la muestra.

4.5 Procedimiento de la Investigación

1. Fase I. Diagnóstico de SGSI

- **a.** Evaluación inicial del estado de la empresa ITS Business SAC con relación con los requisitos de la Norma Técnica Peruana (NTP) ISO/IEC 27001:2014
- **b.** Estudio de la posibilidad de aceptar un sistema de Gestión de Seguridad de la Información (SGSI) y el diagnóstico del estado inicial de la seguridad de la información.

2. Fase II

- **a.** Análisis del contexto (examinar tanto el entorno externo e interno) de la Empresa ITS Business SAC e identificación de las partes interesadas por el SGSI.
- **b.** Establecimiento de los límites y la extensión del alcance del SGSI.
- **c.** Desarrollo de una política y objetivos de seguridad de la información.
- **d.** Identificar los requisitos legales y normativos aplicables.
- **e.** Creación del comité de seguridad.

3. Fase III. Planificación del SGSI

- **a.** Para la evaluación de riesgos; en esta investigación se utilizó la metodología MAGERIT V.3 para realizar el análisis y gestión de riesgos. A continuación de describen las tareas realizadas:
  - ✓ Identificación de los activos; se determinaron los activos que respaldan a los procesos del negocio definiendo el alcance del estudio, esto permitió crear un inventario de activos.
  - ✓ Valoración de los activos; se cuantifico el valor de los activos determinados en su disponibilidad, confidencialidad e integridad para comprender su importación y dar prioridad en la gestión de riesgo.
  - ✓ Identificación y valoración de las amenazas que podrían afectar a los activos.
  - ✓ Calculó del impacto; se determinó el impacto que tendría de materialización de las amenazas identificadas en los activos.

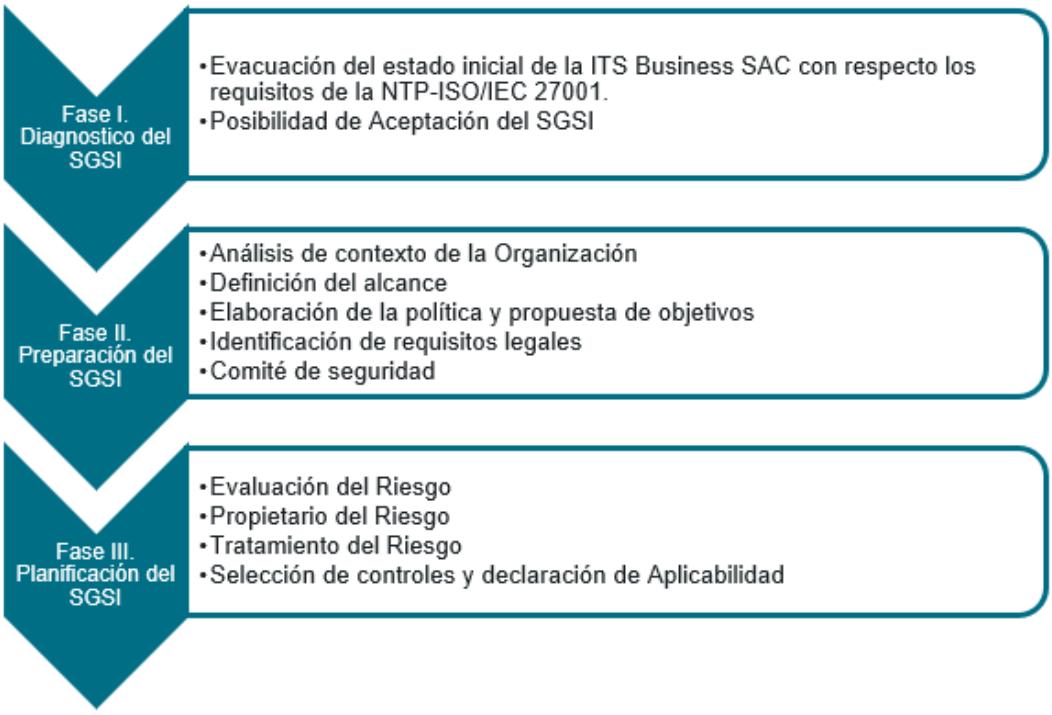
- ✓ Calculó el riesgo; se calculó el riesgo para cada activo, teniendo en consideración la probabilidad de ocurrencia de las amenazas y el impacto.

b. Identificación de los propietarios del riesgo.

c. Tratamiento de los riesgos.

d. Selección de controles y declaración de aplicabilidad.

Figura 2: Fases para el diseño del SGSI



Fuente: adaptado de "Cómo implementar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad", (Gomez, 2015)(p. 48)

4.6 Técnicas e Instrumentos de Recolección de Datos

Se emplearon los siguientes métodos y/o técnicas para la recopilación de información.

Tabla 2. *Técnica e instrumentos para la recolección de información*

TECNICA	INSTRUMENTO	INSTRUMENTO DE REGISTRO	DETALLE
Análisis Documental	Fichas bibliográfica y referencias	Formato de citas y referencias bibliográfica de investigación	Se utilizo una técnica para analizar tanto material impreso y digital relacionado al tema de investigación. Se recurrió a diversas fuentes de información que incluyeron libros, tesis, normas de seguridad y otras fuentes relevantes.
Observación	Escala de Likert (ver tabla 4)	Formato: Anexo A	Esta técnica fue fundamental para recopilar información sobre la situación inicial de la empresa ITS Business SAC en relación con la norma NTP ISO/IEC 27001:2014
Entrevista	Guía de revista (cuestionario)	Formato: Anexo G	Se llevaron a cabo entrevistas con los trabajadores del área de sistemas de la empresa ITS Business SAC, con el objetivo de obtener su opinión sobre el SGSI diseñar, además se buscó conocer el impacto que esta investigación tendría en el área de sistemas, identificar las amenazas y evaluar la probabilidad de que estas se materialicen
Encuesta	Cuestionamiento autoadministrado y autoadministrado grupal	Formato: Anexo **B,E,F** (Tablas 11, 13 y 18)	Se empleo esta técnica y herramienta para obtener datos acerca de nivel de seguridad de la información y la viabilidad de implementar un SGSI, el objetivo era identificar y evaluar los activos de información de la empresa ITS Business SAC
Internet	Tecnologías de información y comunicación	Referencia bibliográfica de esta investigación	Se utilizo esta técnica para la búsqueda de información en libros, revistar, etc ya que el internet es uno de las medias más utilizados para la búsqueda de información en la actualidad.

Fuente: adaptada de (Ccesa Quincho, 2016)

4.7 Plan de tratamiento de datos

Las Herramientas y/o instrumentos que se utilizaron para el análisis y el tratamiento de la información (datos) fueron las que se describen a continuación:

Tabla 3. *Herramientas para el tratamiento de datos*

HERRAMIENTA Y/O INSTRUMENTO	DESCRIPCION
Análisis PEST	El análisis PEST (Políticos, Económicos, Social y Tecnológico) es una herramienta utilizada para el análisis empresarial y estratégico para evaluar el entorno externo de una empresa.
Microsoft Excel	Esta herramienta permite organizar, analizar y manipular datos numéricos y alfanuméricos de manera eficiente para la toma de decisiones.
Matriz DAFO	Es una herramienta de análisis estratégico que se utiliza en las empresas para evaluar las fortalezas, debilidades, oportunidades y amenazas en un proyecto u organización

Fuente: *Elaboración propia*

CAPITULO V

RESULTADOS

5.1 FASE I: Diagnostico del SGSI

Durante esta etapa inicial se realizaron diversas actividades para evaluar la situación inicial de la empresa ITS Business SAC con respecto a la seguridad de la información y al diseño del Sistema de Gestión de Seguridad de la Información (SGSI).

5.1.1 Evaluación inicial del estado de la empresa ITS Business SAC con relación con las disposiciones de la NTP ISO/IEC 27001.

La evaluación del estado inicial de la empresa ITS Business SAC en relación con las disposiciones de la norma ISO/IEC 27001, se desarrolló de dos formas diferentes, una descriptiva y otra cuantificable **(tabla 4)**. Esta técnica consiste en calificar el estado de los requisitos utilizando una escala de Likert que incluye cinco opciones, desde le menor hasta el mayor.

Tabla 4. *Criterio para evaluar el estado inicial de la ITS BUSINESS*

CRITERIO DE CALIFICACION (VALORACION)	VALORACION
No diseñado: Las actividades/métodos demuestran que no se tiene el requisito y/o no se ha bosquejado su implementación	0%
Parcialmente diseñado: Las actividades/métodos demuestran que se tiene el requisito definido, pero este no es del todo conforme con el requisito de la NTP ISO/IEC 27001	25%
Diseñado: Los métodos son conformes con el requisito de la NTP ISO/IEC 27001, pero sin evidencias de aplicación.	50%
Parcialmente implementado: Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001, pero con pocas evidencias de aplicación.	75%
Completamente implementado: Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001, y se cuenta con evidencias de aplicaciones permanentes.	100%

Fuente: adaptado de (Escalante Coronel, 2019)

A continuación, se presenta una sección de la evolución del estado inicial de la empresa ITS Business SAC respecto a los requisitos de la NTP ISO/IEC 27001 que se muestra en la siguiente tabla **(ver tabla 5)**. Aquí un extracto de evaluación realizada.

La evaluación completa se encuentra en el Anexo "A" de esta investigación en donde se proporciona un análisis detallado de cada un requisito y su estado correspondiente, así como cualquier observación relevante para cada uno de los puntos tratados en esta evaluación.

Tabla 5. *Estado inicial de la ITS Business respecto a la norma ISO/IEC 27001*

SECCIÓN	REQUERIMIENTOS DE LA ISO/IEC 27001	ESTADO	EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? / ¿QUÉ SE TENDRIA QUE HACER?	VALORACIÓN
4	**CONTEXTO DE LA ORGANIZACIÓN**	**No diseñado**	Se recomienda realizar un análisis exhaustivo del entorno de la empresa ITS Business SAC. Esto implica comprender tanto los factores internos y externos que puedan influir en su SGSI, así como identificar las partes interesadas, y los requisitos y la documentación del alcance del SGSI.	**10%**
4.1	**Comprender la Organización y contexto.** La organización **debe** determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI	**Parcialmente diseñado**	La empresa ITS Business SAC tiene documentos que describen su Misión, Visión, matriz FODA y estrategias, pero no aborda de manera clara los aspectos de seguridad, se recomienda realizar objetivos de seguridad que estén en línea con los objetivos estratégicos de la empresa.	**25%**
4.2	**Comprende las necesidades y expectativas de las artes interesadas.** La organización **debe** determinar las partes interesadas y los requisitos de las mismas.	**No diseñado**	**Sugerencia: I**dentificar a las partes interesadas y comprender las necesidades y expectativas de estas partes con relación a la seguridad de la información	**5%**
4.3	**Determinar el alcance del SGSI.**	**No diseñado**	**Sugerencia:** Definir y establecer el alcance del SGSI, teniendo en cuanta los aspectos la referencia 4.1 y 4.2, una vez definido el alcance documentarlo de forma clara para que las partes interesadas pueden entenderlo.	**0%**

4.4	**Sistema de gestión de seguridad de la información. la organización debe establece, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de la NTP**	**No diseñado**	**Sugerencia:** implementar una estrategia que el SGSI tena una mejora continua según manifiesta la NTP actual. **Establecer el alcance de los límites del SGSI.**	**15%**
5	**LIDERAZGO**	**Parcialmente diseñado**	El Titular de la entidad tiene la responsabilidad de liderar y asegurar que se asignen roles y responsabilidades, se establezca una política de seguridad de la información y se fije objetivos para la seguridad de la información, todo ellos con el fin de mostrar compromiso y liderazgo en materia de SGSI en la institución.	**25%**
5.1	**Liderazgo y compromiso.** La alta dirección debe demostrar liderazgo y compromiso respecto al SGSI	**No diseñado**	El titular (máxima autoridad de la organización) de la entidad debe mostrar liderazgo y compromiso	**20%**
5.2	**Política**	**No diseñado**	Es necesario establecer la política de seguridad que estén alineados con los objetivos y propósitos de la organización como lo manifiesta en la (Sección 6.2), luego definir las reglas y directrices para proteger la información. Asegurando que todos los empleados tengan conocimiento de ello.	**15%**
5.3	Roles, responsabilidades y autoridades organizacionales	**No diseñado**	La alta dirección debe garantizar que se asigne y comunique responsabilidades y la autoridad para los roles relacionados con la seguridad la información Esto ar que los miembros de la organización sepan los términos de protección de la de información.	**20%**
. . .	. . .	. . .	. . .	. . .
	PUNTAJE TOTAL DE LA EVALUACIÓN DE REQUISITOS DE LA NTP ISO/IEC 27001:2014			**14%**

Fuente: Adaptada de (Ccesa Quincho, 2016)

5.1.2 Resultado de la evaluación del estado inicial de la empresa ITS Business SAC con relación a los requisitos de la Norma Técnica Peruana ISO/IEC 27001

La empresa ITS Business SAC solo la logrado cumplir el 14% de los requisitos establecidos por la norma NTP ISO/IEC 27001. Esto explica que la empresa ITS Business se sitúa en una fase inicial básica de cumplimiento de la norma, lo que significa que aún no ha alcanzado un nivel de diseño adecuado para satisfacer todos los requisitos establecidos en la norma.

5.1.3 Estudio de aceptación del SGSI y diagnóstico del estado inicial de seguridad de la información

El objetivo principal de la recolección de datos fue evaluar la aceptación del sistema de gestión de seguridad de la información. Para cumplir este fin, se utilizó una encuesta que se encuentra en el **Anexo B** de esta investigación. Dicha encuesta conto con veinte preguntas de respuesta dicotómica, que permitan medir las actitudes, opiniones y nivel básico de seguridad de la información en el área de sistemas de la empresa ITS Business SAC.

El propósito de esta encuesta era verificar el estado inicial de la seguridad de la información y determinar la posibilidad de aceptación del diseño del SGSI. Seguidamente, se muestran los resultados de las encuestas realizadas a los seis trabajadores del área de sistemas de la empresa ITS Business SAC con sus respectivos gráficos.

Pregunta 1. ¿Tiene conocimiento de la existencia de un sistema de gestión de seguridad de la información (SGSI) dentro de la empresa ITS Business SAC?

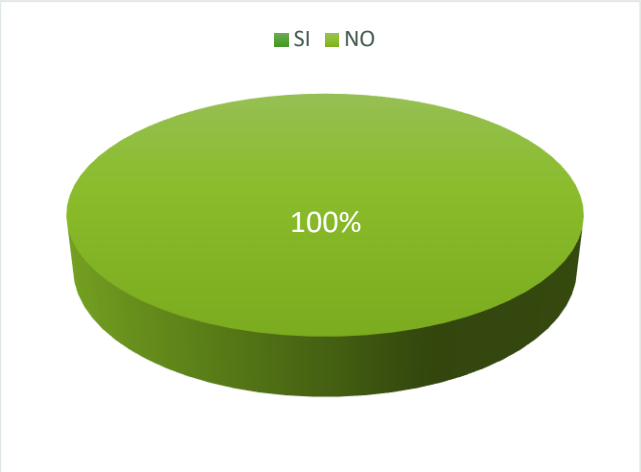


Figura 3: Existencia de un SGSI en ITS BUSINESS SAC

Fuente: Elaboración propia

Explicación

Concluimos a partir de la figura 3, que el 100 % (seis) de los trabajadores encuestados afirman que no existe un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de la empresa ITS Business SAC.

Conclusión:

La empresa ITS Business SAC necesita urgentemente diseñar e implementar un SGSI debido a los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en la organización. también se requiere para abordar y corregir las no conformidades identificadas durante las auditorías a las que la organización se somete.

Pregunta 2. ¿indique si cree que el diseño de un sistema de gestión de la seguridad de la Información (SGSI) ayudara con mejorar la seguridad de información de su área de trabajo?

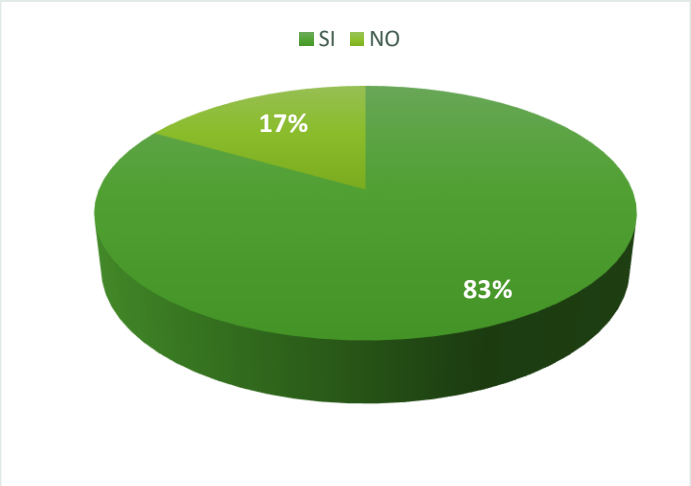


Figura 4: Seguridad de información en su área de trabajo

Fuente: elaboración propia

Explicación

De acuerdo con la figura 4, se observa que un 17% del total de trabajadores (uno) menciono que un SGSI no mejoraría con la seguridad de la información, mientras que 83% de los encuestados (cinco) indican que si mejoraría con la seguridad de la información en su oficina.

Conclusión

Concluimos que la mayoría de los trabajadores de la empresa ITS Business SAC están al tanto del diseño de un sistema de gestión de seguridad de la información en su oficina.

Pregunta 3. ¿Indique si con el uso del sistema de gestión de seguridad de la información se logrará un cambio positivo en su área de trabajo?

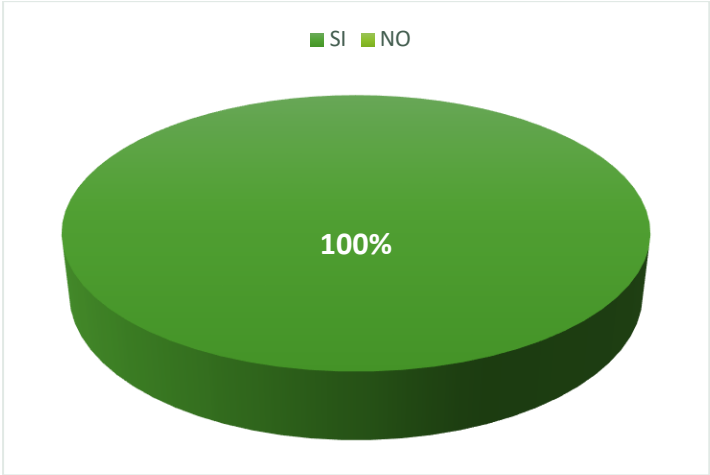


Figura 5: Cambio positivo con el uso de este SGSI

Fuente: elaboración propia

Explicación

De acuerdo con la figura 5, todos los trabajadores encuestados (seis en total) afirmaron que el uso de un SGSI resultara en cambios positivos en la seguridad información.

Conclusión

Concluimos que todos los trabajares del área de sistemas de empresa ITS Business SAC son conscientes de los beneficios que traería el uso de un SGSI. Además, mejorará y ampliará en cuanto a la calidad de los activos tecnológicos y así como en los servicios prestados.

Pregunta 4. ¿Usted estaría de acuerdo con la implementación del sistema de gestión de la seguridad de la información en su área de trabajo?

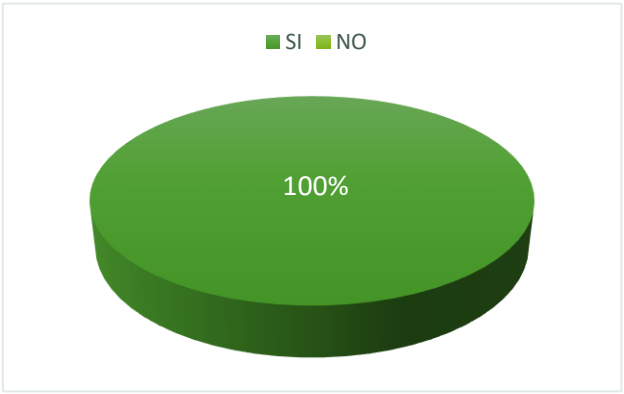


Figura 6: Aprobación de la implementación SGSI en el área de trabajo

Fuente: Elaboración propia

Explicación

Del grafico 6, observamos que el total de los trabajadores encuestados están de aprobar la implementación de un SGSI dentro de su área de trabajo.

Pregunta 5. Dentro de su área de trabajo, ¿estaría de acuerdo con programas y capacitaciones dirigidos a todos los trabajadores con el propósito de concientizar sobre la seguridad de la Información?

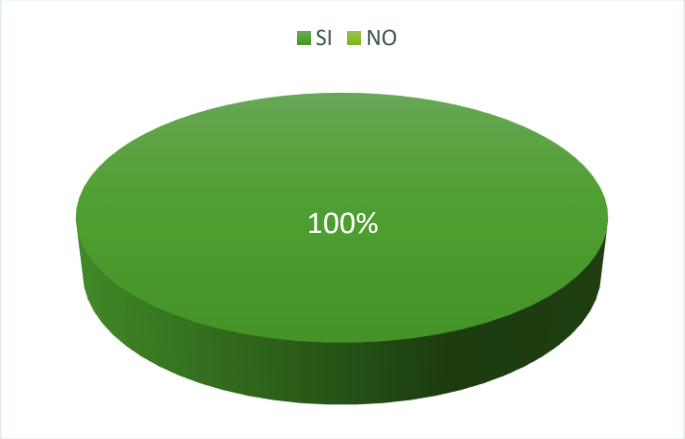


Figura 7: Aprobación de programas dirigidos a los empleados para concientizar sobre la seguridad de la Información

Fuente: Elaboración propia

Explicación

De acuerdo al grafico 7, concluimos que la totalidad de los trabajadores 100% encuestados están dispuesto a aprobar programas y capacitaciones de concientización sobre la seguridad de la información.

Pregunta 6. ¿Estarías dispuesto a trabajar en colaboración para diseñar e implementar un sistema de gestión de seguridad de la información en tu puesto de trabajo?

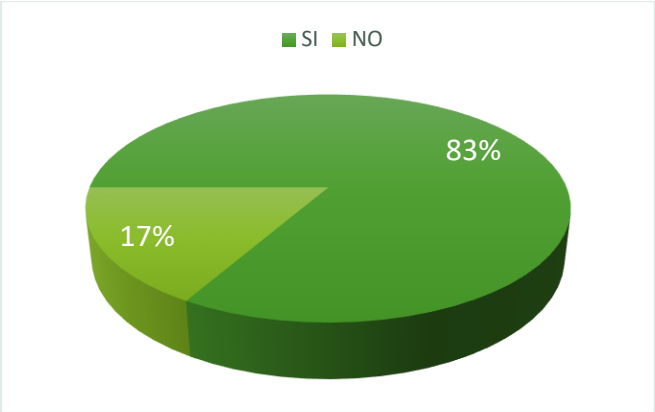


Figura 8: Colaboración del empleado para el diseño e implementación del SGSI

Fuente: Elaboración propia

Explicación

Del grafico 8, observamos que uno de los trabajadores encuestados no está dispuesto a colaborar con el diseño del SGSI mientras que 5 trabajadores si lo están.

Conclusión

Es un buen indicativo que la mayoría de los trabajadores encuestados estén dispuesto a colaborar en el diseño del SGSI. Esto es beneficioso ya que reduce esfuerzos necesarios para implementar el SGSI en el área de sistemas de la empresa. Además, facilita el progreso de programas de capacitaciones de concientización en materia de seguridad de información

Pregunta 7. ¿Considera usted que existe información que debe ser resguarda debidamente en su área de trabajo?

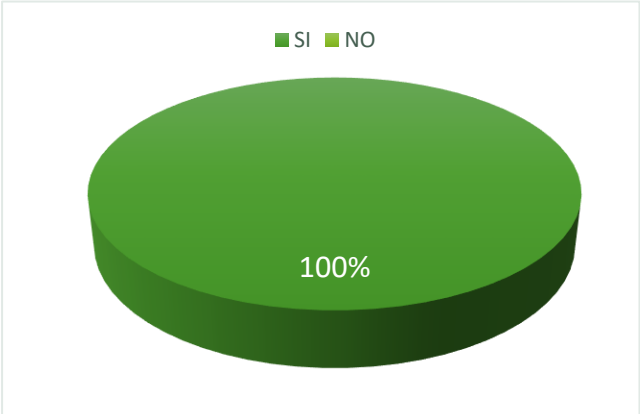


Figura 9: Existencia de información que debe ser resguardada

Fuente: Elaboración propia

Explicación

Del grafico 9, observamos que la totalidad (100%) de los trabajadores encuestados considera que existe información que debe ser resguarda debidamente.

Conclusión

Es crucial que los trabajadores comprendan lo importante que es proteger la información al diseñar de un sistema de gestión de seguridad de la información (SGSI).

Pregunta 8. ¿considera que en su área de trabajo se ha clasificado la información de acuerdo a la importancia que tienen para la empresa ITS BUSINESS SAC?

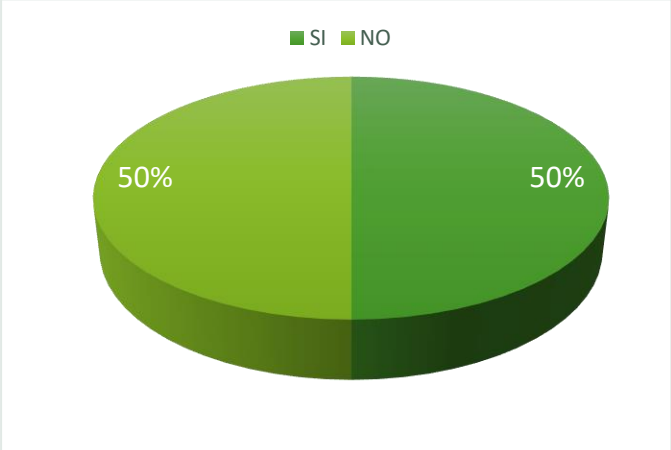


Figura 10: Clasificación de la información de acuerdo a la importancia

Fuente: Elaboración propia

Explicación

De grafico 10, observamos que la mitad (50%) de los trabajadores coinciden que se tiene clasificado la información dentro de la empresa, considerando la importancia para la empresa ITS Business SAC. Mientras que el otro 50 % considera que no.

Conclusión

Es importante el diseño de SGSI puesto que ayudara a la empresa ITS Business SAC a clasificar su información de forma adecuada teniendo en consideración la valoración de los activos de información.

Pregunta 9. ¿Recibió capacitaciones en su área laboral en referencia a la seguridad de la información?

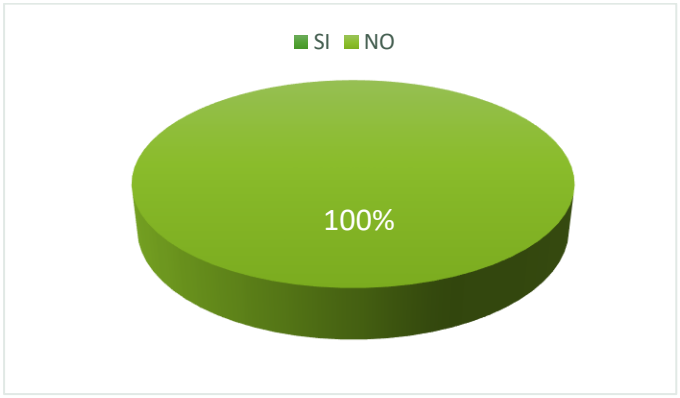


Figura 11: ***Capacitación sobre seguridad de la información***

Fuente: Elaboración propia

Explicación

Según la figura 11, observamos que el total (100%) de los encuestados indica que nunca fueron capacitados en referencia a la seguridad de la información.

Conclusión

Considerando que la totalidad de los encuestados nunca recibieron capacitaciones con relación a la seguridad de la información se tiene una alta probabilidad que la información pueda ser afectado en cualquiera de sus tres dimensiones.

Pregunta 10. ¿Dentro de su contrato laboral existe cláusulas que establezcan responsabilidades en relación con la protección de la información?

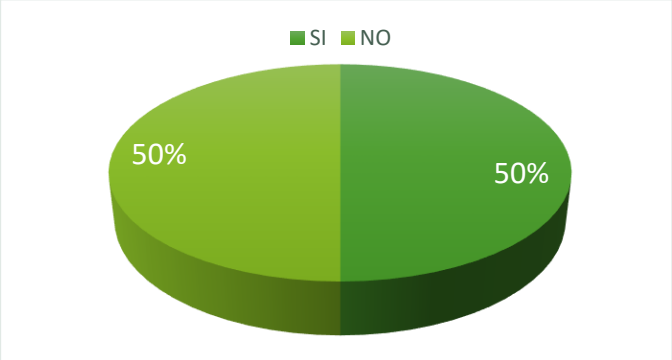


Figura 12: ***Contrato laboral contempla cláusulas de seguridad de la información***

Fuente: Elaboración propia

Explicación

Observamos en el grafico 12 que la mitad (50%) de los trabajadores encuestados afirman que en su contrato laboral existen cláusulas sobre la seguridad de la información. Mientras que el otro 50% afirma no contemplan estas cláusulas.

Pregunta 11. En su área de trabajo ¿se consideran la seguridad de información cuando se gestiona un proyecto?

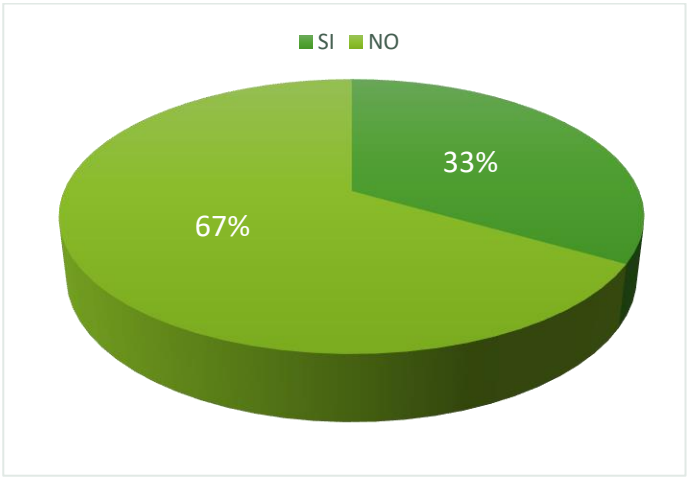


Figura 13: ***Seguridad de la información en gestión de proyecto***

Fuente: elaboración propia

Explicación

De acuerdo al grafico 13, observamos que el 33% de los trabajadores (dos) encuestados confirmaron que consideran la seguridad de la información cuando se desarrolla un proyecto nuevo. Mientras que el 67% de los trabajadores (cuatro) afirman lo contrario.

Pregunta 12. ¿Cuándo ingresa a su computador y/o laptop cuenta con una clave de acceso?

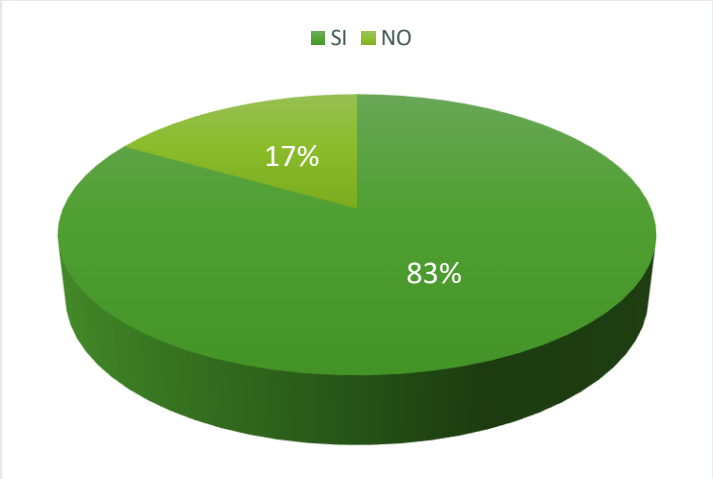


Figura 14: ***Accesos de ingreso a un computador y/o laptop***

Fuente: Elaboración propia

Explicación

Según la figura 14, observamos que 83% de los trabajadores (cinco) encuestado afirma que si tienen una clave de acceso para ingresar a su pc y realizar sus funciones. Mientras el 17% de los encuestados indique que no tienen claves de acceso.

Pregunta 13. Cuando su laptop o computador no está en uso ¿Se activa de forma automática el bloqueo de pantalla con contraseña para proteger la información?

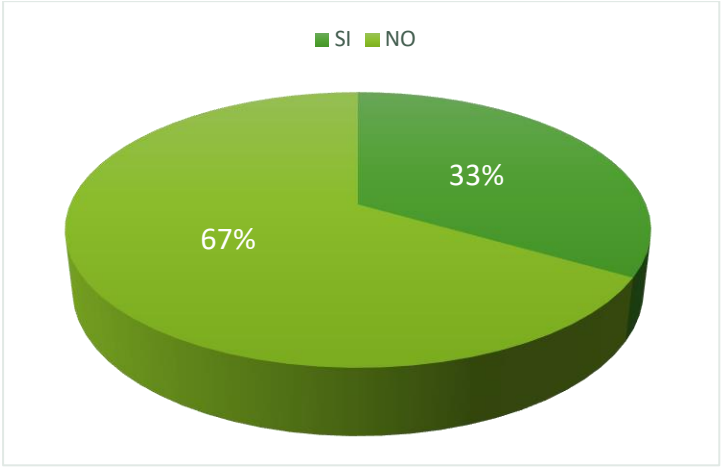


Figura 15: Bloqueo de pantalla con contraseña

Fuente: Elaboración propia

Explicación

De acuerdo al grafico 15, observamos que el 67% de los colaboradores encuestados afirmaron que cuando su pc o laptop no está en uso se activa el bloqueo de pantalla. Mientras que un 33% de los encuestados (dos) afirman que si se activa el bloqueo de pantalla.

Pregunta 14. ¿A lo largo de este año ha sufrido alguna modificación o perdidas de información sin autorización (virus, deterioro, tras papeleo, accesos no autorizado, etc.)?

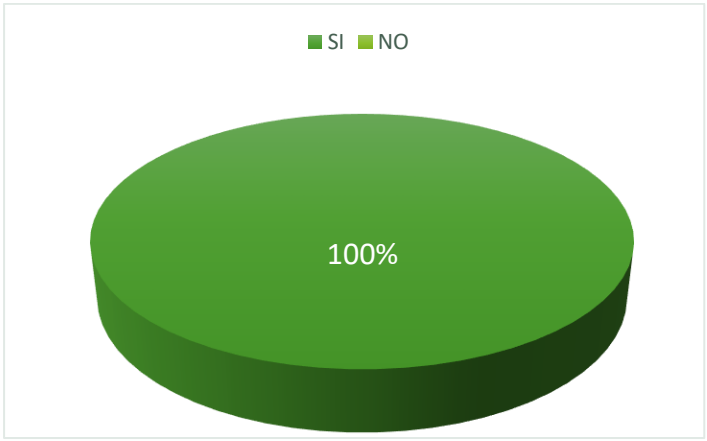


Figura 16: Modificación o pérdida de información

Fuente: Elaboración propia

Explicación

De acuerdo al grafico 16, observamos que el 100% de los colaboradores (seis) encuestado indican haber sido víctima de perdida y/o modificación de información.

Pregunta 15. ¿Durante el año se ha filtrado o divulgado información sensible para la empresa ITS Business SAC sin su autorización o conocimiento?

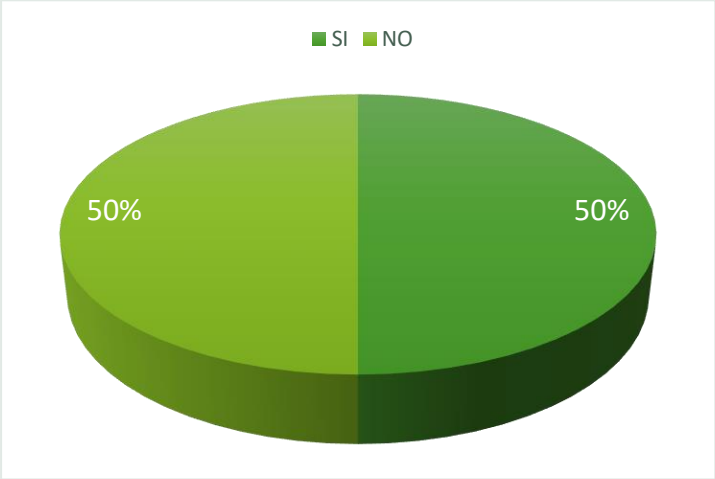


Figura 17: Divulgación de información sensible

Fuente: Elaboración propia

Explicación

De acuerdo a la figura 17, observamos que el 50 % de los encuestados (tres) afirman que se han divulgado información sensible para la empresa ITS Business sin su autorización o conocimiento. Mientras que el otro 50% de los encuestados (tres) considera que no se ha divulgado información sensible que afecte a la organización.

Pregunta 16. ¿se ha llevado a cabo una evaluación de los riesgos asociados a la información en tu puesto de trabajo?

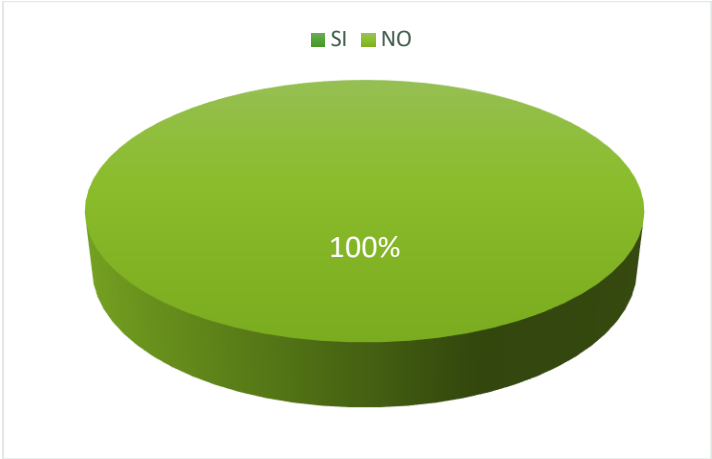


Figura 18: ***Evaluación de riesgos en el puesto de trabajo***

Fuente: *Elaboración propia*

Explicación

De acuerdo al grafico 18, observamos que el 100% de los colaboradores encuestados opinan que no se ha realizado el análisis de riesgo con relación a la seguridad de la información en la empresa ITS Business.

Pregunta 17. ¿Se ha llevado a cabo análisis de seguridad de la red en su área de trabajo?

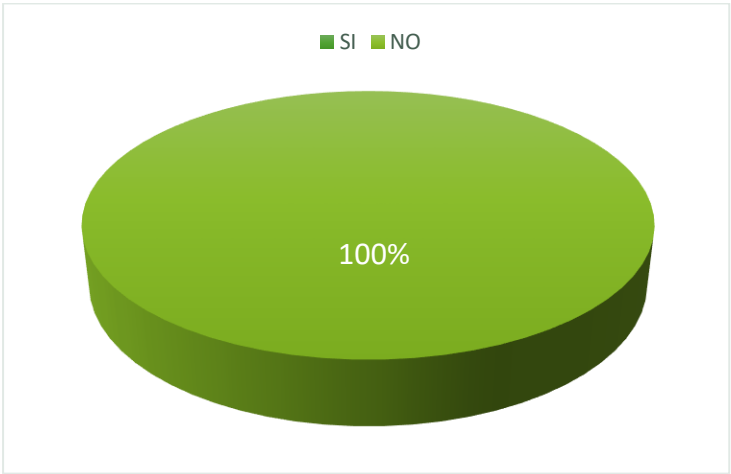


Figura 19: ***Evaluación de vulnerabilidades de la red***

Fuente: Elaboración propia

Explicación

De acuerdo al grafico 19, observamos que el 100% de los encuestados (seis) desconocen que en la empresa ITS Business SAC se hayan desarrollado evaluaciones de vulnerabilidades de la red.

Conclusión

Al observar que el 100% de los trabajadores encuestados afirman que no ha se realizó ninguna evaluación de vulnerabilidad de la red, esto indica que hay una alta probabilidad de que existan vulnerabilidad, por lo tanto, una debilidad en la seguridad de la información.

Pregunta 18. ¿Cuenta con software antivirus actualizado en su puesto de trabajo?

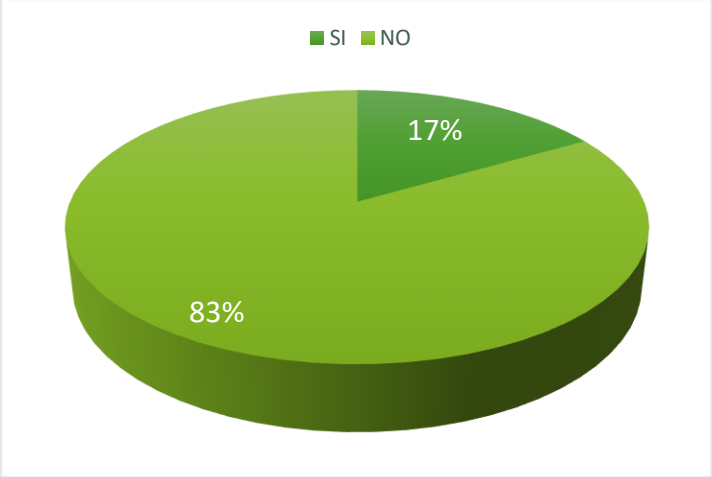


Figura 20: ***Puesto de trabajo cuenta con antivirus actualizado***

Fuente: Elaboración propia

Explicación

Del grafico 20 observamos que el 83% de los encuestados (cinco) indica que no cuentan con un software antivirus actualizado, mientras que el 17% de los encuestados (uno) afirma que si tiene el software antivirus actualizado.

Pregunta 19. ¿genera copias de seguridad (backups) para proteger su información?

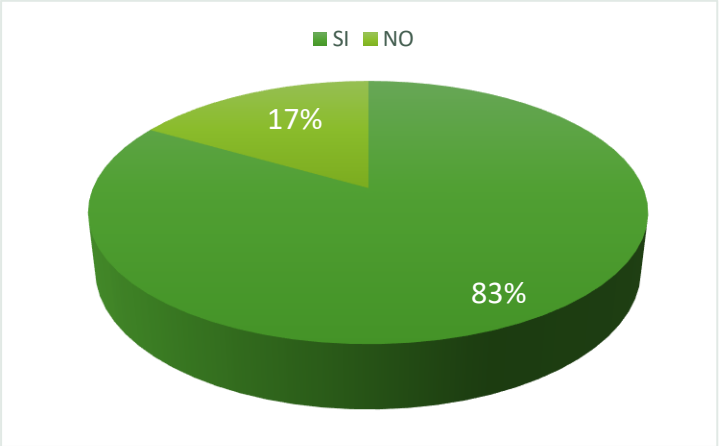


Figura 21: ***Frecuencia de generación copias de seguridad***

Fuente: *Elaboración propia*

Explicación

Se observa en la figura 21 que el 83% de los colaboradores encuestados generan copias de seguridad para respaldar su información. Mientras que el 17% (uno) no genera ningún respaldo.

Conclusión

A pesar de que la mayoría de los trabajares encuestados generan su copia de respaldo, estas backups son almacenados en sus propias computadoras, por lo tanto, siguen siendo un riesgo de pérdida de información.

Pregunta 20. ¿cree usted que su oficina esta resguarda contra amenazas externas o ambientales que puedan generar perdidas de información?

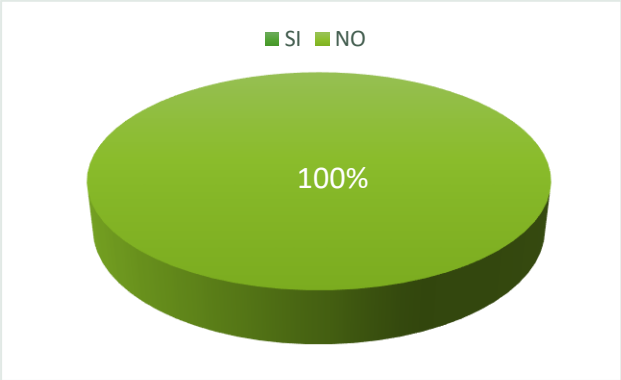


Figura 22: ***Pérdidas de información por amenazas externas o ambientales***

Fuente: Elaboración propia

Explicación

De acuerdo con el grafico 22, observamos que el 100% de los colaboradores encuestados, indican que la empresa ITS Business SAC es vulnerable a amenazas externas, ambientales que generen perdida de información.

Conclusión

El objetivo del diseño del SGSI para la empresa ITS Business SAC es identificar las amenazas potenciales a las que se enfrenta, analizar los riesgos y establecer mecanismo de control para proteger los activos de información, esto implica implementar medidas preventivas y buscar la mejora contina en términos de seguridad.

5.2 FASE II. Preparación del SGSI

Estos fueron los objetivos de esta fase: determinar el alcance (ámbito y limites) del SGSI, también se desarrolló una política de seguridad de la información y se establecieron los objetivos específicos en la seguridad de la información, también se llevó a cabo un análisis exhaustivo de los requisitos legales que afecten a la empresa en relación con la seguridad de la información. Esto permite asegurar el cumplimiento con las leyes reguladoras. Así mismo se propuso la creación del comité de seguridad de la información en la empresa ITS Business SAC quienes estarán encargados en la supervisión y toma dediciones. Estos objetivos se lograron mediante un análisis del entorno externo e interno de la organización, lo que ayudo a entender las necesidades y expectativas de las partes interesadas en el SGSI.

5.2.1 Contexto de la organización

La norma técnica peruana ISO/IEC 27001:2014 enfatiza la importancia de comprender la organización y su entorno como menciona en el capítulo 4, donde se centra en el contexto de la organización; esto implica entender los aspectos internos y externos de la entidad que son esenciales para establecer un SGSI. Además, destaca identificar las necesidades y expectativas de las partes interesas y determinar el alcance del SGSI.

5.2.2 Contexto externo

Para el diseño e implementación del SGSI se procedió a analizar los aspectos externo (relevantes) que afectan a la empresa ITS Business SAC. Para ello se utilizó la herramienta de análisis PEST (Políticos, Económicos, Sociales - Culturales y Tecnológicos) que están mencionadas en el ítem 4.7 (Plan de Tratamiento de Datos) de esta investigación.

Los resultados obtenidos del análisis se muestran en siguiente la figura de forma detallada:

Tabla 6. *Análisis PEST*

POLITICO LEGAL	➢ Marco regulatoria sobre seguridad de la información ➢ Estandarización de procesos y sistemas de información
ECONÓMICO	➢ Alto costo de consultores para establecer un SGSI ➢ Poco presupuesto por parte de la gerencia
SOCIO CULTURAL	➢ Mas empresas con acceso a internet y dispuesto a digitalizarse (facturación electrónica, estudios contables, etc) ➢ Sociedad preocupada por la seguridad de la información ➢ Sociedad peruana cada vez más tecnológica y móvil ➢ incremento de personas dedicados a delitos informáticos
TECNOLOGICO	➢ Desarrollo de nuevas tecnologías de información ➢ Nuevas necesidades de implementación tecnológicas ➢ Implementación de fibra óptica y la adopción de la tecnología 5G ➢ vulnerabilidades en la seguridad de la información

Fuente: adaptado de (Ccesa Quincho, 2016)

5.2.3 Contexto interno

El Sistema de Gestión de Seguridad de la Información que se pretende implementar debe estar alineado con la cultura, los procesos, la estructura y la estrategia de la organización.

a) Naturaleza de la entidad

ITS Business SAC es una empresa que realiza actividades económicas en el área de desarrollo de tecnología de la información y de servicios informáticos, actividades de contabilidad, teneduría de libros, auditoría, consultoría fiscal y educación especializada en temas contables, a personas y

empresas, para lograrlo gestiona: Personal, equipamiento especializado, Información, Software operativo y de gestión, un sistema integral empresarial enfocado en procesos y un pensamiento basado en riesgos.

El perfil de la empresa es absolutamente técnico y de alta especialización multidisciplinaria. La disponibilidad en la atención de los servicios es abierta al requerimiento de sus clientes, teniendo la capacidad de atención de servicios las 24 horas del día en sus procesos operativos. (ITS Business S.A.C - 2020)

b) Misión

"Somos una empresa que desarrolla y comercializa software dirigido a pequeñas, medianas empresas y profesionales independiente de Perú ofreciendo al público un software eficaz y de calidad a un precio competitivo mediante nuestro servicio de asistencia al cliente, nuestro público automatiza fácilmente sus procesos de negocios, aportando de esta manera productividad que se refleja en su rentabilidad." (Fuente: ITS Business S.A.C)

c) Visión

"Ser uno de los Softwares empresariales, más reconocidos a Nivel Nacional e Internacional, brindando aportes tecnológicos al área de Contabilidad y así optimizar los procesos administrativos". (Fuente ITS Business S.A.C)

d) Actividades que desarrolla

- Desarrollo de tecnología de la información y de servicios informáticos (Sistema VisualFact, VisualCont, Visual Plan y Facturador Electrónico)
- Brinda soporte técnico a los diferentes sistemas informáticos, así como capacitaciones de los mismos.

- Consultoría fiscal y educación especializada en temas contables a personas y empresas (cursos, talleres).

e) Líneas estratégicas

- **Competitividad local:** Hace referencia de las condiciones institucionales que promueve el desarrollo competitivo de la región.
- **Calidad de servicio:** Hacer referencia a los procesos internos y las mejoras continuas que una empresa pretende implementar para ofrecer un servicio de alta calidad a sus clientes, esto implica medir la satisfacción de usuarios.
- **Recursos y tecnología:** comprende abarcar los actos y recursos de la organización como su personal, bienes, patrimonio, compensaciones económicas y también incluye la tecnología de información y comunicaciones que son usados para optimizar sus operaciones.

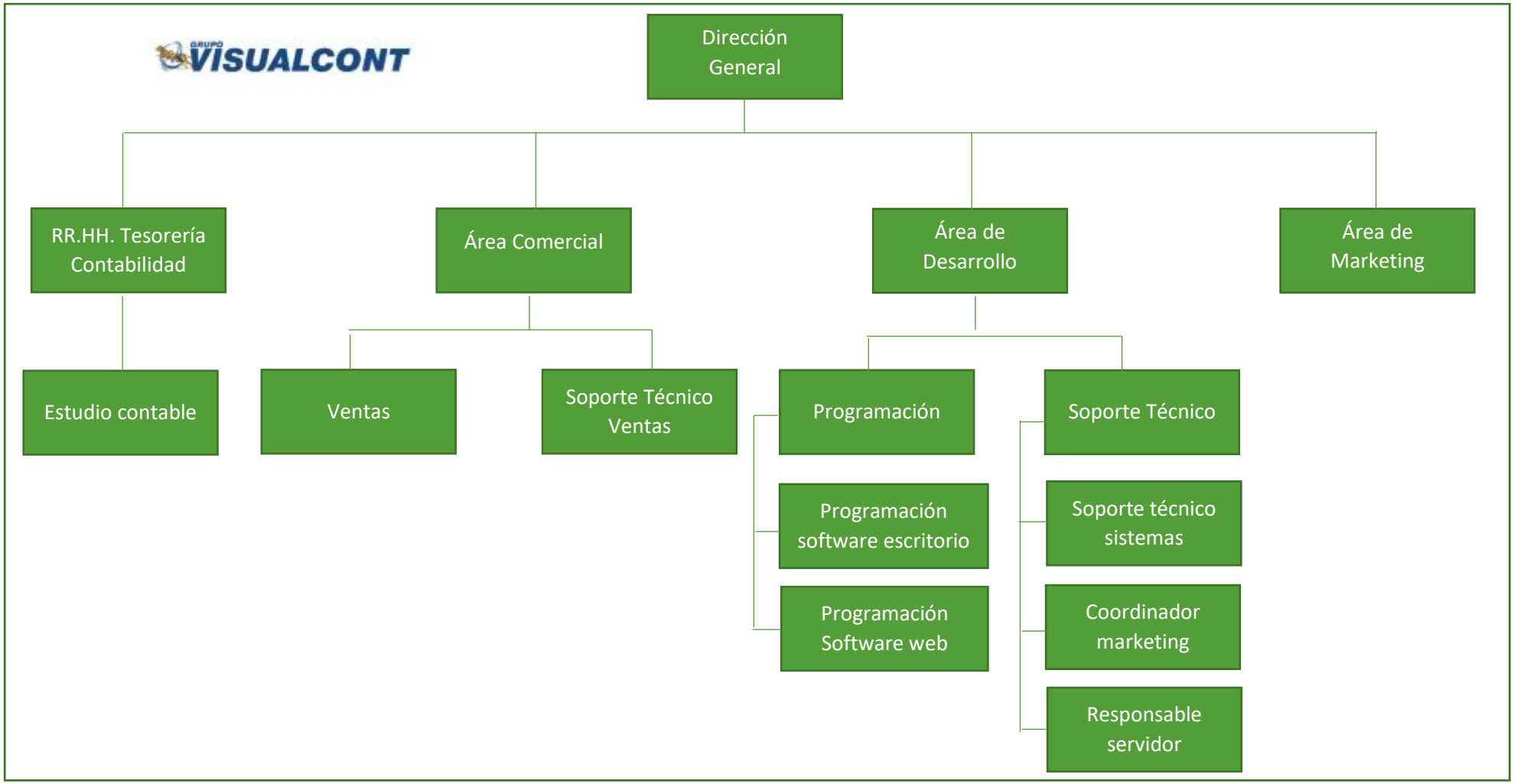
f) Objetivos estratégicos

- Garantizar que los usuarios reciban un servicio de atención satisfactorio y de calidad.
- Crear y proporcionar soluciones tecnológicas y servicios informáticos que se ajusten y satisfagan las necesidades de los clientes.
- Fortalecer su posición de liderazgo de la empresa ITS Business SAC en el campo del desarrollo de tecnología de la información y servicios informáticos en la región.
- Digitalizar a las empresas en la emisión de documentos electrónicos.

g) Estructura orgánica

Se muestra la estructura orgánica de la empresa ITS Business SAC en la siguiente figura 23.

Figura 23: ***ORGANIGRAMA DE LA EMPRESA ITS BUSINESS S.A.C***



Fuente: *ITS Business SAC*

h) Mapa de Procesos

Se procedió a identificar los procesos de la empresa luego de realizar un análisis exhaustivo de las diferentes áreas a la empresa ITS Business S.A.C para luego desarrollar el siguiente mapa de procesos:

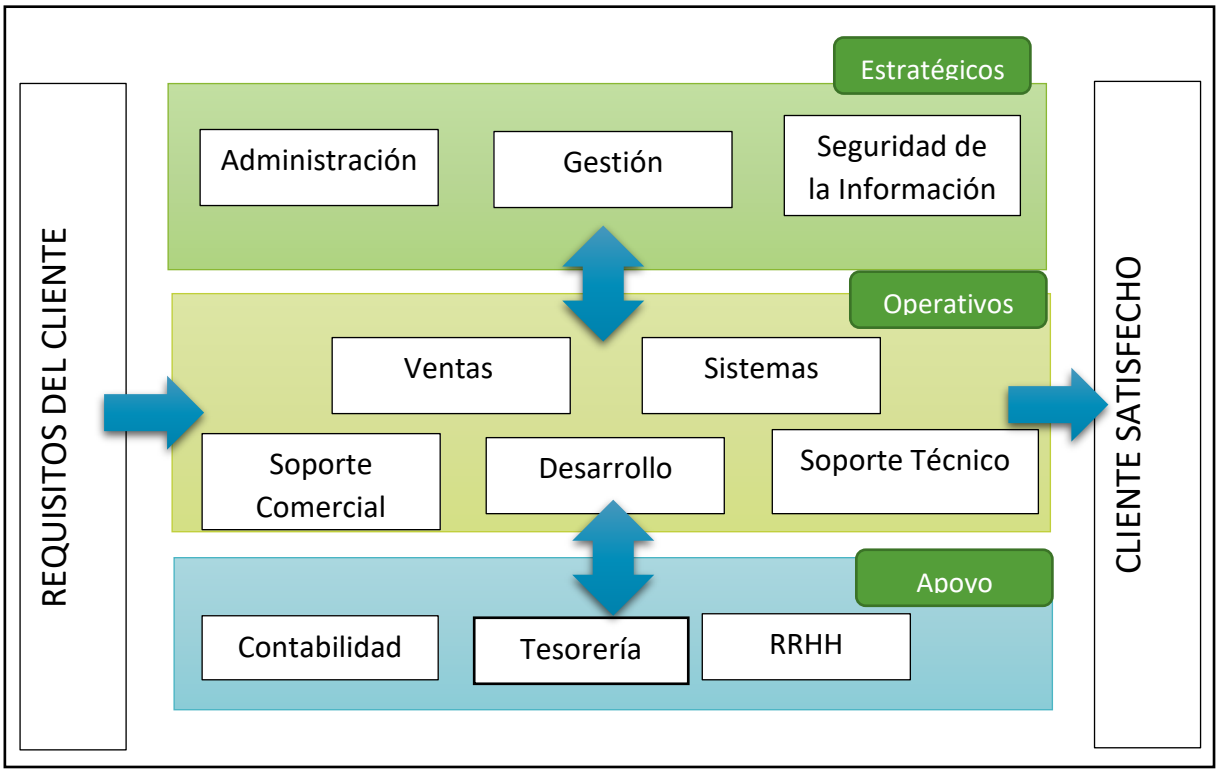


Figura 24: Mapa de Procesos de la ITS

Fuente: Elaboración Propia

i) Aspectos técnicos

La empresa ITS Business SAC, está distribuida de la siguiente manera teniendo en su sede principal una red de área local (LAN), está compuesta por un conjunto de 20 lugares a áreas de trabajo, 2 servidores, 03 páginas web, la primera es la página principal (*https://grupovisualcont.com/*), página web del instituto de contabilidad electrónica (*https://institutocontable.org/*) y la página web de revista de consultoría (*https://revistadeconsultoria.com/*), también

cuenta con correos corporativo Gmail para sus usuarios, finalmente cuentan con un área de sistema

La información que tiene la empresa concentra en los servidores y las pcs, la cual es usada para el funcionamiento de los sistemas, se generan copias de seguridad backups cada cierto tiempo y se almacenan en el mismo servidor, así como en otra unidad de almacenamiento externo.

En cuanto al cableado de red está expuesto y desordenado en ciertas áreas, y todos los equipos están vulnerables a amenazas que puedan comprometer su integridad, disponibilidad y confidencialidad. Se adjuntas algunas imágenes del servidor en el Anexo “C”.

i.1 Servicios de atención en línea de la ITS Business SAC

De acuerdo a la información brindada por el personal y de la página web de la empresa ITS Business SAC se identificó los siguientes servicios:

1. **Para usuarios Externos**
   - **a.** Consultas sobre los servicios de los softwares: los clientes y público en general puede realizar consultas sobre los módulos, planes, costos, talleres y capacitaciones de los diferentes sistemas (softwares) así como de los servicios de consultoría contable, entre otros. Todo ello será brindado por el personal de ventas.
   - **b.** atención en línea: los clientes y público en general puede realizar consultas y recibir orientación por parte del personal de soporte técnico sobre las dificultades o inconveniente que se pueda presentar en los respectivos softwares o servicios.
   - **c.** cursos online y presencial: los clientes y público en general pueden obtener cursos, talleres y

capacitaciones de forma online o presencial de diferentes temas que son programas durante el año.

d. atención de forma remota: los clientes que presentan inconvenientes en los softwares son atendidos de forma remota por el personal de soporte técnico.

2. Para usuarios Internos

- ✓ Plataforma de actividades programadas en CRM
- ✓ Acceso al sistema de Facturación electrónica
- ✓ Acceso a los softwares (VisualCont, VisualFact, VisualPlan)
- ✓ Acceso restringido a archivos en el servidor

j) Matriz FODA

Luego de realizar el análisis los factores internos y externos de la empresa ITS Business SAC se elaboró la siguiente matriz FODA.

Figura 25: Matriz FODA

Fuente: Elaboración Propia

Tabla 7. *Inventario de sistemas de información de la ITS BUSINESS SAC*

N°	Sistema de información	Lenguaje de programación	Base de datos	Fecha de producción	Desarrollo interno / externo	Servidor	Documentación
1	PAGINA WEB PRINCIPAL	Php (WordPress)	MySQL	2016	Externo/ personalizado	Servidor Externo	NO
2	REVISTA DE CONSULTORIA	Php (WordPress)	MySQL	2016	Externo/ personalizado	Servidor Externo	NO
3	INSTITUTO CONTABLE	Php (WordPress)	MySQL	2016	Externo/ personalizado	Servidor Externo	NO
4	FACTURADOR ELECTRONICO	php	MySQL	-	interno	Amazon	SI (Desactualizada)
5	VISUAL FACT	Visual Basic 6.0	SQL Server	-	interno	Servidor Interno	SI (Desactualizada)
6	VISUAL CONT	Visual Basic 6.0	SQL Server	-	interno	Servidor Interno	SI (Desactualizada)
7	VISUAL PLAN	Visual Basic 6.0	SQL Server	-	interno	Servidor Interno	SI (Desactualizada)

Fuente: *Elaboración Propia*

k) Partes interesadas

En esta sección se identificaron a las partes interesas involucradas en el diseño y su posterior implantación del SGSI. De acuerdo en lo dispuesto en el requisito (ítems 4.2) (comprende las necedades y expectativas de las partes interesadas) de la NTP ISO/IEC 27001:2014.

1. Partes interesadas Externas

- **Sunat:** La Superintendencia Nacional de Aduanas y de Administración Tributaria es una entidad técnica especializado del estado, vinculada al Ministerio de Economía y Finanzas tiene como finalidad primordial administrar los tributos del gobierno nacional y los conceptos tributarios y no tributarios cuya administración o recaudación se le encarga por ley o convenio institucional.
- **Clientes:** son las personas naturales o jurídicas que adquieren los servicios de los softwares.
- **Proveedores:** Persona natural o jurídica que presta servicios a la empresa ITS Business

2. Partes interesadas internas

- **Gerencia:** Debe mostrar habilidades de liderazgo y compromiso solido con la seguridad de la información, esto implica garantizar los objetivos establecidos sean coherentes con la planificación estratégica de la organización.
- **Responsable de sistemas:** es el responsable de la seguridad de la información y continuidad tecnología de la empresa.
- **Responsable de recursos humanos:** responsable de la seguridad antes, durante y después de la vinculación de los trabajadores.
- **Trabajadores de la ITS Business SAC:**

  Son los responsables de velar por la seguridad ellos activos de información de la empresa ITS BUSINESS SAC, cumplir rigurosamente con las normas y política de seguridad establecidas en la organización, también son responsables de manejar de forma adecuada los datos personales de los trabajadores de la entidad.

  En la tabla N°8 se muestran los requisitos de las partes interesadas del SGSI

Tabla 8. *Requisitos de las partes interesadas del SGSI*

	PARTES INTERESADAS	REQUISITOS
externas	Sunat	➢ Supervisar la información recibida ➢ Seguridad de los datos que son recepcionados ➢ Certificación con la ISO 2007
	clientes	➢ Seguridad de sus datos(información)
	Proveedores	➢ Documentos de contratos claros en cuanto a la seguridad de la información
internas	Gerencia	➢ Monitorear y controlar las acciones y proyectos del encargado de informática en relación a la seguridad de la información. ➢ Debe mostrar liderazgo y compromiso con la seguridad de la información

	Responsable de sistemas	➢ Levantamiento de no conformidades (respecto a la seguridad de la información) de las auditorias que se realicen en la ITS Business ➢ Brindar capacitaciones a los empleados en referencia con la seguridad de la información
	Responsable de RR.HH	➢ Revisar y verificar la información antes, durante y después de la contratación de los empleados.
	Trabajadores de la ITS Business	➢ Tener conocimiento de normas y políticas de seguridad de la información ➢ Velar por los activos de información de la ITS Business SAC ➢ capacitaciones en temas de seguridad de la información ➢ Protección de su información personal

Fuente: Adaptado de (Escalante Coronel, 2019)

5.2.4 Políticas de seguridad de la información

De acuerdo a lo estipulado en el requisito 5.2 de la NTP ISO/IEC 27001:2014, se defino la política de seguridad de la información de la empresa ITS Business SAC. Esta política de seguridad tendrá que ser aprobada por la gerencia y revisada anualmente. La misma que está diseñada específicamente para cumplir con los objetivos y necesidades de la entidad en referencia a la seguridad de la información. Estas medidas toman en cuenta los requisitos normativos actuales relacionados con la seguridad de la información y el compromiso de buscar constantemente mejoras en sus prácticas de seguridad.

Después de ser aprobada la política de seguridad, la empresa ITS Business SAC informara a todos los trabadores de la entidad sobre estas políticas.

La empresa ITS BUSINESS S.A.C, en cumplimiento de nuestra misión, visión y objetivos estratégicos, y para satisfacer las necesidades de nuestros clientes, colaboradores, comunidad y demás partes interesadas, establecer la función de seguridad de la información en la entidad, con el objetivo de:

Proteger los activos de información de la empresa ITS Business SAC.

Es política de la empresa ITS Business SAC asegurar que:

- Proteger la información contra la perdida de sus confidencialidad, disponibilidad e integridad.
- Cumplir con los requisitos legales y reglamentos aplicables a la entidad y al sistema de gestión de seguridad de la información.
- Gestionar los riesgos de la seguridad de la información mediante la aplicación de una metodología, estándares y controles.
- Fomentar la cultura de seguridad de la información entre los trabajadores de la entidad.
- Garantizarla la continuidad de los servicios de la entidad
- La empresa ITS Business SAC tiene la política de implementar, mantener y realizar un seguimiento del SGSI

Aplicabilidad de la política del SGSI

Esta política se aplica a toda la organización, incluyendo empleados, proveedores terceros y demás partes interesadas.

Figura 26: Políticas de Seguridad

Fuente: elaboración propia ()

5.2.5 Alcance de SGSI

El alcance permite determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información de la entidad.

En el anexo “D“ de esta investigación se adjunta el documentos del alcance del sistema de gestión de seguridad de la información para la empresa ITS Business SAC, se presenta a continuación un extracto del documento.

Alcance del SGSI

En la empresa ITS BUSINESS S.A.C el alcance definido del sistema de seguridad de la información (SGSI), abarca todos los sistemas de información, procesos, tecnología y personas. Ya que se ha identificado que todos sus procesos de negocio son claves en el SGSI.

La aplicabilidad de este Sistema de Gestión de Seguridad de la Información (SGSI) es solo aplicable para la sede principal de la empresa que se encuentra ubicada en Zarate, San Juan de Lurigancho, Lima. Esto Limitando las actividades y los procesos que se ejercen en esta sede.

Figura 27: Alcance del SGSI de la ITS

Fuente: Elaboración Propia ()

5.2.6 Objetivos de la Seguridad de información

Los objetivos del SGSI se muestran en la siguiente figura

- Incrementar el nivel de satisfacción de los clientes de la ITS Business SAC
- Garantizar la privacidad y protección de la información confidencial de los clientes que se encuentran almacenados en los sistemas de información de la ITS Business SAC
- Garantizar que la información sensible de la empresa ITS Business SAC este protegido en términos de confidencialidad, integridad y disponibilidad
- Garantizar que la información de la ITS Business SAC esté disponible para los usuarios o procesos autorizados en el momento requerido.
- Reducir a un nivel aceptable los riesgos de seguridad de la información para la empresa ITS Business SAC.
- Comunicar a toda la organización mediante los responsables de cada área la política de seguridad.
- Elaborar evaluaciones de la efectividad del SGSI y realizar la mejora continua

Figura 28: Objetivos de la Seguridad de la Información

Fuente: Elaboración propia ()

5.2.7 Requisitos legales

- **Ley N° 29733** – Ley de protección de datos personales y su reglamento aprobado mediante decreto supremo N° 003-2013-JUS. Promulgada en 2011, pero entro en aplicación el 8 de mayo de 2015, la presente ley tiene el objetivo de garantizar el derecho fundamental a la protección de datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen (ATENCIO BAZAN, 2019)

  Esto significa que las empresas y entidades públicas tienen la responsabilidad de asegurar la seguridad de los datos almacenados en sus sistemas informáticos, impidiendo el acceso no autorizados de terceros.

- **Ley delitos informáticos**

  Ley N° 30096 Entro en vigencia el 23 de octubre de 2013. La presente ley tiene por objetivo prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informativos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnología de información o de la comunicación, con la finalidad de garantizar la lucha eficaz de ciberdelincuencia (ATENCIO BAZAN, 2019)

  Ley N° 30171 publicada el 10 de marzo de 2014. Ley que modifica los artículos 2, 3, 4, 5, 6, 7, 8 y 10 de la ley 30096 ley de delitos informáticos.

5.2.8 Comité de la seguridad de la información

De acuerdo a los requisitos 5.3 roles, responsabilidad y autoridades organizacionales de la NTP ISO/IEC 27001:2014, la gerencia de la organización debe asegurar de que se asignen y ccomuniquen las

responsabilidades y los roles relevantes para la seguridad de la información.

Este comité de seguridad se conformará por:

- La gerencia
- El administrador
- El responsable de sistema
- El responsable de asesoría jurídica
- El oficial de seguridad de la información
- El responsable de desarrollo de aplicaciones

5.2.8.1 La Gerencia

- Aprobar y comunicar a todos los colaboradores de la organización la política de seguridad de la información.
- Definir y establecer los roles y responsabilidades específicos tanto a nivel de directivo como operativo relacionados con la seguridad de la información.
- Fomentar y crear conciencia sobre cultura de seguridad de la información en la organización.

5.2.8.2 El administrador

- Presentar a la gerencia propuestas de políticas de seguridad de la información para la organización.
- Asegurar que se implemente y se siga la política de seguridad de la información dentro de la organización.

5.2.8.3 El responsable Sistemas

- Asegurar que los sistemas de información y los equipos informáticos de la organización estén disponibles y en funcionamiento correcto.
- Crear y seguir un conjunto de pasos y practicas para gestionar y administrar los riesgos y la seguridad de la información. Además, es importante asegurarse de que el personal de la entidad este capacitado en estos temas

- Comunicar al administrador sobre los aspectos relacionados con el SGSI
- Garantiza que haya métodos para manejar los riesgos y oportunidades, políticas de seguridad de la información, y que cuenten con los documentos requeridos para la norma NTP ISO/IEC 27001:2014
- Garantizar que se cumplan las políticas y requisitos de seguridad establecidos para todos los aspectos relacionados con la adquisición, diseño, desarrollo, operación, administración y mantenimiento de la infraestructura tecnológica de la entidad.
- Asignar tareas y responsabilidades relacionados con la seguridad a los trabajadores que están a cargo de operar y administrar la infraestructura tecnológica de la organización.

5.2.8.4 El responsable de asesoría jurídica

- Comprender y dar sentido a las leyes y regulaciones actuales que están relacionadas con la seguridad de la información en el contexto de la organización.
- Evaluar el cumplimiento de las leyes y normatividad vigente en temas se seguridad de la información dentro de la organización.
- Mantener los archivos actualizados con respectos a las normas legales que están relacionados con la seguridad de la información.

5.2.8.5 El oficial de seguridad de la información

- Diseñar y coordinar la aplicación de las políticas, reglas y procesos se seguridad de la información, involucrando de manera activa a todas las dependencias o departamento de la entidad.

- Reconocer las riesgos y amenazas que pueden afectar los activos de información de la empresa ITS Business SAC
- Determinar los controles relacionados al SGSI y evaluarlos.
- Impartir charlas de formación y sensibilización sobre seguridad de la información al personal de la organización.
- Realizar evaluaciones internas y externas relacionadas con la Seguridad de la información y tomar las medidas necesarias para abordar cualquier problema identificado.
- Informar al responsable de informática sobre los incidentes de Seguridad de la información, los resultados de las auditorias, también sobre la revisión y supervisión del SGSI

5.2.8.6 El responsable de desarrollo de aplicaciones

- Garantizar la disponibilidad y operatividad de los SI, optimizar la seguridad de los sistemas en desarrollo
- Coordinar con el responsable de sistema y soporte técnico para mejorar y corregir las observaciones y/o errores de los sistemas en desarrollo.
- Informar a gerencia sobre los cambios y/o mejoras desarrollados en los diferentes sistemas para su evaluación, aprobación y su posterior implementación.

5.3 FASE III. Planificación del SGSI

En esta etapa se realizaron acciones necesarias para abordar los riesgos y garantizar que el diseño del sistema de gestión se seguridad de la información (SGSI) logre los siguientes objetivos que son evaluar los riegos de seguridad de la información den la empresa ITS Business SAC y desarrollar controles de seguridad para mitigar los riesgos identificados.

5.3.1 Evaluación de riesgo

5.3.1.1 Inventario de Activos

La clasificación de los activos se estableció en base a la metodología de análisis y gestión adoptada, esta clasificación categoriza los activos según ciertos criterios y características relevantes.

Tabla 9. *Clasificación de los activos de información*

Tipo de activos	Descripción
Datos / información	Los datos es el activo que permite a una organización puede prestar sus servicios La información es un activo abstracto que será almacenado en equipos de información (BD)
Servicios	Los servicios satisfacen la necesidad de los usuarios, completan servicios presentados por los sistemas.
Software / aplicaciones informáticas	Sin actividades automatizadas delegados a un sistema informático para que lo realice automáticamente Las aplicaciones tiene la capacidad de manejar, analizar y modificar los datos, lo que a su vez posibilita aprovechar la información de manera efectiva para ofrecer servicios
Sistemas informáticos	Son los diferentes sistemas que están siendo desarrollados dentro la entidad para su comercialización o brindar el servicio del mismo. Estos sistemas Ayudan a administrar, recolectar, procesar, almacenar y distribuir información relevante para los usuarios.
Equipos informáticos	Son los medios materiales, elementos físicos utilizados para respaldar de manera directa o indirecta los servicios proporcionados por la organización (contenedores temporales o como permanentes de datos)
Redes de comunicaciones	Son los medios de trasporte encargados de trasladar los datos (información) de un lugar a otro.
Soporte de información	Dispositivos físicos son aquellos que tiene la capacidad de almacenar la información de manera duradera, ya sea de forma permanente o por largo periodos de tiempo
Instalaciones	Son los sitios o lugares donde se alojan y operan los sistemas de información y comunicaciones
Personal	Personas que están relacionados con los sistemas de información

Fuente: elaboración propia

Para identificar los activos de información de la empresa ITS Business SAC, utilizo el formato del **Anexo E** llamado “cuestionario para identificar activos”, se puede encontrar una muestra de la lista de activos identificados en el proceso de gestión de la

infraestructura tecnológica en a **tabla 10**. Sin embargo, el inventario completo de encuentra en el **Anexo F** de esta investigación.

Tabla 10. *Inventario de activos de información*

N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO	UBICACIÓN
1	Datos vitales	Dados almacenados en diferentes sistemas de información esenciales para el funcionamiento de la ITS BUSINESS SAC	Dato / información	servidor
2	Archivos personales	Documentos personales de los trabajadores de la ITS BUSINESS SAC	Dato / información	Computadores personales
3	Copias de seguridad (backup)	Copias de respaldo de datos y/o información que maneja los distintos sistemas de la ITS BUSINESS SAC	Dato / información	Servidos y PCs personales
4	Datos de configuración de los SI	Corresponde a los documentos, manuales y procedimientos relacionados con la administración de los diferentes SI	Dato / información	Archivos físicos
5	Datos de gestión interna	Corresponde a los documentos de la ITS BUSINESS SAC	Dato / información	Archivo físico
6	Credenciales (contraseñas)	Usuarios y contraseñas que utilizan los usuarios ara ingresar a los recursos tecnológicos	Dato / información	C/ usuario guarda sus contraseñas
7	Datos de control de acceso	Corresponde a los datos de usuarios internos que utilizan los sistemas de información y/o aplicaciones	Dato / información	BD / usuarios internos
8	Log de los sistemas de información	Son los datos de los usuarios internos que utilizan los sistemas de información y/o aplicaciones	Dato / información	Servidor
9	Correos electrónicos	Correos electrónicos corporativos	Servicios	Correos electrónicos (gmail)

10	Gestión de permisos (privilegios)	Son los mecanismos para la administración y asignación de privilegios de acceso a los recueros tecnológicos y aplicaciones	Servicios	Sistemas de información
11	Base de datos	BD de los diferentes sistemas almacenados la información de la entidad	Servicio	Servidor terminal
12	Base de datos clientes	BD almacenados de los clientes del facturador	Servicio	Servidor AWS
13	Página web principal	Página web principal de la entidad	Software	VPS
14	Página web revisar de consultoría	Página web Revista de consultoría	Software	VPS
15	Página web instituto de contabilidad electrónica	Página web instituto de contabilidad electrónica	Software	VPS
16	Facturador Electrónico	Sistema de facturación electrónica	Software/aplicación informática	Servidor AWS
17	Sistema VISUAL FACT	Sistema de gestión empresarial	Sistema Informático	Servidor terminal
18	Sistema VISUAL CONT	Sistema contable	Sistema Informático	Servidor terminal
19	Sistema VISUAL PLAN	Sistema de planillas	Sistema Informático	Servidor terminal

Fuente: Elaboración propia

5.3.1.2 Valoración de activos

Para evaluar los activos de información es importante tener en cuenta tres aspectos principales: su valor económico, los requisitos legales y la reputación de la organización. Estos pueden impactar en la seguridad y protección de la confidencialidad, integridad y disponibilidad de los activos de información. Los criterios seguidos para la valorización de los activos se encuentran en la tabla 11

Tabla 11. *Criterio para la valoración de activos*

Aspectos	Criterio de calificación	Valorización
Económico (E) pérdidas económicas para la empresa ITS BUSINESS SAC	Pérdidas económicas excepcionalmente elevadas	5
	Causa de pérdidas económicas elevadas	4
	causas de graves pérdidas económicas	3
	Causas de pérdidas financieras o pérdidas de ingresos	2
	causa de pérdidas económicas mínimas	1
Legal (L) incumplimiento de leyes y normas	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación	5
	Probablemente cause un incumplimiento grave de una ley o regulación	4
	probablemente sea causa de incumplimiento de una ley o regulación	3
	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación	2
	Pudiera causar el incumplimiento leve o técnico de una ley o regulación	1
Imagen (IMG) Afecta la imagen de la empresa ITS BUSINNES SAC	Probablemente causaría una publicación negativa generalizada por afectar gravemente a las relaciones con otras organizaciones	5
	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones	4
	probablemente por publicidad negativa y afecte las relaciones con otras organizaciones	3
	Probablemente afecte negativamente a las relaciones internas de reorganización	2
	Pudiera causar una perdida menor de la confianza dentro de la organización	1

Nota: adaptado de "Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso" (Guzman Silva, 2015, pág. 85) ()

Seguidamente, se formuló un cuestionario de preguntas para determinar el nivel de criticidad del activo de información. Estas interrogantes de muestran a continuación:

Tabla 12. *Preguntas para determinar la criticidad del activo de información*

Parámetros	Aspectos	Preguntas
Confidencialidad (C)	Económico	¿su divulgación no autorizada puede revelar información sensible de la entidad requerida para toma de decisiones estratégicas y financieras causando pérdidas económicas?
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de leyes o normas impartidas por entes de control?
	Imagen	¿Su divulgación puede afectar la imagen de la entidad?
Integridad (I)	Económico	¿si el activo de la información que se gestiona a través de él son alterados sin autorización puede genera pérdidas económicas para la entidad?
	Legal	¿si el activo o la información que se gestiona a través de él son alternados sin autorización puede generar sanciones de entes de control?
	Imagen	¿si el activo e información que se gestiona a través de él no están disponibles queden genera pérdidas económicas para la entidad?
Disponibilidad	Económicas	¿si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad?
	Legal	¿si el activo o la información que se gestiona a través de él no están disponibles pueden generar sanciones legales de antes de control?
	Imágenes	¿si el activo a información que se gestiona a través de él no está despabiles pueden afectar la imagen de la entidad?

Nota: adaptado de "Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso" (Guzman Silva, 2015, pág. 86) ()

Finalmente, realizar la evaluación del nivel de criticidad de los activos valorados en el proceso de la infraestructura tecnología, se utilizó el criterio establecido en la tabla 13. Esto permitió determinar la importancia de los activos de información tecnológica.

Tabla 13. *Niveles de criticidad de los activos de información*

Criterios de evolución	Valor	Nivel
El activo de información en un nivel de alto de integridad y/o confidencialidad de la información	3 <VF<=5	ALTO
El activo de información comprende de un nivel medio de integridad y/o confidencialidad y/o disponibilidad de la información	VF = 3	MEDIO
El activo de información comprende en un nivel bajo de integridad y/o confidencialidad y/o disponibilidad de la información	O<VF<3	BAJO

Nota: adaptado de "Diseño de un sistema de gestión de seguridad de la información para entidad financiera de segundo piso" (Guzman Silva, 2015, pág. 86) ()

Seguidamente, se muestra un resumen de los resultados obtenidos de la valoración realizada a los activos de información en la tabla 14.

Tabla 14. *Valoración de activos de la información y niveles de criticidad*

N°	NOMBRE DE ACTIVO	CONFIDENCIALIDAD			INTEGRIDAD			DISPONIBILIDAD			CFC	VFI	VFD	VF	NIVELES DE CRITICIDAD
		E	L	IMG	E	L	IMG	E	L	IMG					
1	Datos vitales	4	2	3	2	3	3	3	2	3	3	3	3	3	MEDIO
2	Copias de respaldo(backup)	4	3	4	5	4	4	5	4	5	4	4	5	4	ALTO
3	Datos de gestión interna	4	4	3	3	3	3	2	2	2	4	3	2	3	MEDIO
4	Credenciales (contraseñas)	4	4	5	4	3	3	3	3	2	4	3	3	3	MEDIO
5	Datos de control de acceso	4	4	5	4	4	4	4	4	4	4	4	4	4	ALTO
6	Log de los sistemas de información	3	3	3	3	3	3	3	3	3	3	3	3	3	MEDIO
7	Correo electrónico	3	3	3	2	2	3	3	3	3	3	2	3	3	MEDIO
8	Gestión de privilegios	5	5	5	4	4	5	4	2	3	5	4	3	4	ALTO
9	Base de datos	4	4	4	5	5	5	5	4	4	4	5	4	4	ALTO
10	Base de datos clientes	5	5	5	5	5	5	5	4	5	5	5	5	5	ALTO
11	Facturador Electrónico	4	4	4	5	5	5	5	5	5	4	5	5	5	ALTO
12	Sistema VISUAL FACT	5	5	5	5	5	5	5	5	5	5	5	5	5	ALTO
13	Sistema VISUAL CONT	5	5	5	5	5	5	5	5	5	5	5	5	5	ALTO
14	Sistema VISUAL PLAN	5	5	5	5	5	5	5	5	5	5	5	5	5	ALTO
15	Computador de los trabajadores	3	3	2	3	2	3	3	1	3	3	3	2	3	MEDIO
16	firewall	4	4	3	4	3	3	5	4	4	4	3	4	4	ALTO
17	Internet	3	1	1	3	1	1	4	3	4	2	2	4	3	MEDIO
18	Equipos de comunicación (tel. cel., mjs)	3	3	3	1	1	2	4	3	5	3	1	4	3	MEDIO
19	Disco duro externo	5	4	4	5	4	4	4	4	3	4	4	4	4	ALTO
20	Dispositivos de almac. externos	4	3	4	3	3	3	3	3	3	4	3	3	3	MEDIO
21	Servidor interno	5	5	5	5	5	5	5	5	5	5	5	5	5	ALTO
22	Servidor terminal server	5	5	5	5	5	5	5	5	5	5	5	5	5	ALTO
23	servidor AWS	5	5	5	5	5	5	5	5	5	5	5	5	5	ALTO
24	Usuarios externos	2	2	3	3	2	3	4	2	4	2	3	3	3	MEDIO
25	Personal análisis de software (analista)	4	4	4	4	4	4	4	3	3	4	4	3	4	ALTO
26	Personal de desarrollo de software	5	4	5	5	5	4	5	4	4	5	5	4	5	ALTO
27	Personal de servicio soporte de ventas	4	4	4	5	3	4	5	3	5	4	4	4	4	ALTO
28	manuales de Aplicaciones	3	2	3	3	2	3	3	1	3	3	3	2	3	MEDIO

Fuente: Elaboración Propia

Nota: **E**= económico, **L**=Legal, **IMG**=Imagen, **VFC**= valor final de confiabilidad, **VFI**=valor final de integridad, **VFD**= valor final de disponibilidad, **VF**=valor final de activo de información

De la tabla 14:

- El valor de la columna VFC (valor final de confidencialidad) representa el máximo valor de los aspectos económicos, legales e imagen que impacta la seguridad de un activo en términos de confiabilidad, se utilizó el mismo criterio para obtener los valores de VFI(valor final de integridad) y VFD(valor final de disponibilidad) cada uno dentro de su respectiva dimensión.
- El valor de VF (valor final del activo de información) es el promedio de valor de VFC, VFI, VFD.
- El nivel de criticidad del activo se obtiene de acuerdo a la (tabla 13)

Finalizada la valoración de los activos de información, se procedió a seleccionar los activos con nivel de criticidad alto y medio, para luego agruparlos en los activos que lo contienen.

Los resultados obtenidos de esta actividad se visualizan en la siguiente tabla 15

Tabla 15. *Activos por contenedor*

ACTIVO DE INFROMACION	NIVEL DE CRITICIDAD	CONTENEDOR
Copias de respaldo (backup)	ALTO	Servidor y PCs personales
Datos de gestión interna	MEDIO	Archivo físico(estantería)
Credenciales (contraseñas)	MEDIO	C/ usuario guarda sus contraseñas
Datos de control de acceso	ALTO	BD/Usuarios internos
manuales de Aplicaciones	MEDIO	servidor interno
Datos vitales	MEDIO	servidor interno
Log de los sistemas de información	MEDIO	servidor interno
Correo electrónico	MEDIO	Correo electrónico GMAIL
Gestión de privilegios	ALTO	Sistemas de información
Base de datos interno	ALTO	Servidor terminal
Base de datos clientes	ALTO	Servidor AWS
Facturador Electrónico	ALTO	Servidor AWS
Sistema VISUAL FACT	ALTO	Servidor terminal
Sistema VISUAL CONT	ALTO	Servidor terminal
Sistema VISUAL PLAN	ALTO	Servidor terminal
Computador de los trabajadores	MEDIO	Oficina de la ITS BUSINESS SAC
firewall	ALTO	Oficina de informática
Internet	MEDIO	Red local
Equipos de comunicación de datos (teléfonos, celulares, mensajería)	MEDIO	Oficinas de la ITS BUSINESS SAC

Dispositivos de almacenamientos externos	MEDIO	Archivos físicos o estantes
Usuarios externos	MEDIO	Usuarios externos
servidor AWS	ALTO	Externo
Servidor interno	ALTO	Oficina de sistemas de la ITS BUSINESS SAC
Servidor terminal	ALTO	Oficina de sistemas de la ITS BUSINESS SAC
Disco duro externo	ALTO	Oficina de sistemas de la ITS BUSINESS SAC
Personal desarrollo software (analista)	ALTO	Oficina de sistemas de la ITS BUSINESS SAC
Personal de desarrollo de software (programadores)	ALTO	Oficina de sistemas de la ITS BUSINESS SAC
Personal de servicio soporte de ventas	ALTO	Oficina de ventas de la ITS BUSINESS SAC
Código fuente de los sistemas de información	ALTO	Pc desarrolladores/servidor

Fuente: Elaboración Propia

5.3.1.3 Identificación y valoración de amenazas

En esta etapa, se creado un listado de amenazas que pueden afectar a los activos de información, Estas amenazas se han identificad utilizando el catálogo de amenazas proporcionadas por MAGERIT V.3 **(anexo G)**

Luego en colaboración con el equipo de sistemas de la empresa ITS Business SAC se llevó a cabo la identificación de las amenazas que podrían afectar los activos mencionados anteriormente, seguidamente se determinó la probabilidad de que estas amenazas ocurran.

Para calcular la probabilidad de que estas amenazas se materialicen, se utilizó el criterio que se muestra en la table número 16.

Tabla 16. *Probabilidad de materialización de amenazas*

Probabilidad de que se materialicen la amenazas		
Criterio	**Valor**	**Puntuación**
Mas de 2 años	Imposible	1
Anual	Poco probable	2
Mensual	Posible	3
Semanal	Probable	4
Diario	Muy probable	5

Fuente: Elaboración propia

En la tabla a continuación se presenta la relación de amenazas identificas, indicando la dimensión de seguridad que afecta al activo y la probabilidad de que las amenazas se materialicen. Puedes encontrar la tabla completa de identificación de amenazas, riesgo y consecuencias en el **Anexo H** de este documento

Las amenazas pueden impactar los activos de información en diferentes dimensiones de seguridad, se clasifican en tres niveles de relevancia, el nivel 1 indica una relevancia alta, el nivel 2 indica una relevancia moderada y el nivel 3 indica una relevancia baja.

Tabla 17. *Identificación de amenazas*

N°	AMENAZAS	DIMENCIONES			PROBABILDIAD DE OCURRENCIA
		C	I	D	
1	fuego			1	1
2	desastres naturales(sismo)			1	2
3	Corte del suministro eléctrico			1	3
4	Condiciones inadecuadas de temperatura o humedad			1	2
5	Degradación de soporte de almacenamiento de la información			1	1
6	Fallo de servicios de comunicación			1	3
7	Error de usuarios	2	1	3	4
8	Errores de configuración		1		2
9	error del administrador	3	2	1	2
10	Alteración occidental de la información		1		2
11	Destrucción de la información			1	4
12	Caídas del sistema por agotamiento de recursos			1	2
13	Difusión de software dañino	3	2	1	3
14	Fugas de información	1			2
15	Vulnerabilidades de los programas	3	1	2	3
16	Errores de mantenimiento actualización de programas		1	2	3
17	Errores de actualización de equipo (hardware)			1	2
18	Indisponibilidad del personal			1	3
19	Suplantación de identidad del usuario	1	2		2
20	Abuso de privilegios de acceso	1	2	3	3
21	acceso no autorizado	1	2		3
22	análisis de trafico	1			2
23	modificación deliberada de información		1		3
24	divulgación de información			1	2
25	robo de quipos	2		1	1
26	Inestabilidad de la línea de internet			1	4
27	Manipulación de equipos	1		2	4
28	Instalación de software no autorizados	1			3

Fuente: Elaboración propia ()

Nota: C= confidencialidad, I= Integridad , D=disponibilidad

Se ha clasificado las amenazas por activo de información temiendo en cuenta que no todas las amenazas afectan a todos los activos, pero existe una relación entre el tipo de activo y lo que podrá suceder luego, se evaluó la degradación de cada activo utilizando el criterio de la tabla 18. El resultado final de esta evaluación se muestra en la tabla 19.

Tabla 18. *Criterio de valoración de degradación del activo*

CRITERIO	VALOR
Sin degradación (SD)	1
Degradación baja (B)	2
Degradación media (M)	3
Degradación alta (A)	4

Fuente: Elaboración propia ()

Tabla 19. *Degradación de los activos: SERVIDORES Y PC's*

AMENAZAS	PROBABILIDAD	DEGRADACIÓN CONFIDENCIALIDAD	DEGRADACIÓN INTEGRIDAD	DEGRADACIÓN DISPONIBILIDAD
SERVIDORES (INTERNO, TERMINAL) - VISUALCONT, VISUALFACT, VISUALPLAN				
Fuego	1	1	1	4
desastres naturales(sismo)	2	1	2	4
error del administrador	2	2	1	3
Suplantación de la entidad del usuario	2	4	2	3
Abuso de privilegios de acceso	3	3	2	1
Accesos no autorizados	3	3	3	1
Robo de equipos	1	3	1	4
Corte de suministro eléctrico	3	1	1	4
Condiciones inadecuadas de temperatura o humedad	2	1	2	4
Vulnerabilidades de los programas (software)	3	2	4	3
Errores de mantenimiento actualización de programas (software)	3	1	4	3
Difusión de software dañino	3	4	3	4
Caídas del sistema por agotamiento de recursos	2	1	1	4
vulnerabilidades de los programas(software)	3	2	4	3
Inestabilidad de la línea de internet	4	1	1	4
errores de configuración	2	1	4	2
fallo de servicios de comunicación	3	1	1	4
degradación de soportes de almacenamiento de la información	1	1	1	3
PC's				
Fuego	1	1	1	4
Movimiento sísmico	2	1	2	4
Errores de usuarios	4	3	4	1
Errores de configuración	2	1	4	1
Suplantación de identidad del usuario	2	4	3	2
Acceso no autorizado	3	4	3	1
Robo de equipos	2	2	1	4
Corte de energía eléctrica	4	1	2	4
Condiciones inadecuadas de temperatura o humedad	3	1	2	4
Vulnerabilidades de programas (software)	3	2	4	3
Error de manteamiento actualización de equipos (hardware)	2	1	1	3
instalación de software no autorizado	3	4	1	1
manipulación de quipos	4	3	1	2

Fuente: *Elaboración Propia* ()

5.3.1.4 Cálculo de impacto

En este segmento se realizado el cálculo de impacto, que se determina teniendo en cuenta el valor del activo en requisito y la posible degradación de la amenaza causaría en caso de que ocurra. Para llevar a cabo este cálculo, se establecieron los siguientes criterios:

Tabla 20. *Criterio para calcular el impacto*

DEGRADACIÓN DE LAS AMENAZAS	VALOR DEL ACTIVO				
	1	2	3	4	5
1 (sin degradación)	1	1	1	1	1
2 (degradación baja)	1	2	2	2	4
3 (degradación media)	1	2	3	4	4
4 (degradación alta)	1	2	4	4	5

Fuente: Elaboración propia ()

Tabla 21. *Valor del impacto*

VALOR	DESCRIPCIÓN
1	Insignificante
2	Menor
3	Medio
4	Critico
5	catastrófico

Fuente: Elaboración propia ()

En esta evaluación de realizado el cálculo sin tener en cuenta las medidas de seguridad que estén implementados en la actualizad. Objetivo es determinar el nivel máximo de riesgo para cada uno delo activos

En la **tabla 24** se muestra el resultado del impacto para los activos SERVIDOR TERMINAL (VisualCont, VisualFact, VisualPlan), PC's.

5.3.1.5 Cálculo de riesgo

El cálculo del riesgo se basa en los factores principales_ el impacto que tendría la materialización del riesgo sobre el activo y la probabilidad de que ocurra dicha materialización. El riesgo aumenta a medida que aumenta el impacto y la probabilidad. Con el fin de gestionar adecuadamente el riesgo, se han definido varias zonas que deben tenerse en cuenta. Para este estudio en particular, se ha elaborado la siguiente matriz de evaluación de riesgo.

Tabla 22. *Matriz de evaluación de riesgo*

IMPACTO		MATRIZ DE EVALUACIÓN DE RIESGO				
Catastrófico	5	15	19	22	24	25
Critico	4	10	14	18	21	23
Medio	3	6	9	13	17	20
Menor	2	3	5	8	12	16
Insignificante	1	1	2	4	7	11
		1	2	3	4	5
		Prácticamente imposible	**Poco Probable**	**Posible**	**Probable**	**Muy Probable**
		PROBABILIDAD (DE LA AMENAZA) = FUTURO				

Fuente: Elaboración propia ()

La matriz permite clasificar los niveles de riesgo en alto, medio y bajo. Esta asignación se realiza siguiendo el siguiente criterio:

Tabla 23. *Niveles de riesgo*

NIVELES DE RIESGO	
CRITERIO	**NIVEL**
O<nivel de riesgo<=8	**Bajo**
9 <nivel de riesgo<=17	**Medio**
18<nivel de riesgo<=25	**Alto**

Fuente: *Elaboración Propia* ()

En la tabla 24 se muestra el resultado de la valoración de riesgo para los activos Servidor – (VisualCont, VisualFact, VisualPlan) y PC's.

Finalmente se identificó los activos que están expuestos a mayor riesgo y las amenazas que causan esos riesgos.

Tabla 24. *Impacto y riesgo para el servidor terminal y PC´S*

AMENAZAS	PROBABILIDAD	DEGRADACION			IMPACTO			ESTIMACIÓN DEL RIESGO		
		CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
SERVIDOR TERMINAL - VISUALCONT, VISUALFACT, VISUALPLAN										
fuego	1	1	1	4	insignificante	menor	catastrófico	bajo	Bajo	medio
desastres naturales(sismo)	2	1	2	4	insignificante	Menor	catastrófico	bajo	bajo	alto
error del administrador	2	2	1	3	medio	insignificante	critico	medio	Bajo	medio
suplantación de identidad del usuario	2	4	2	3	catastrófico	menor	medio	alto	bajo	medio
abuso de privilegios de acceso	3	3	2	1	critico	medio	menor	alto	medio	bajo
acceso no autorizado	3	4	3	1	catastrófico	critico	insignificante	alto	alto	bajo
robo de equipos	1	3	1	4	medio	menor	catastrófico	bajo	bajo	medio
corte de suministro eléctrico	3	1	1	4	insignificante	menor	catastrófico	bajo	bajo	alto
condiciones inadecuadas de temperatura o humedad	2	1	2	4	insignificante	menor	Critico	bajo	bajo	medio
vulnerabilidades de los programas(software)	3	2	4	3	medio	catastrófico	Critico	medio	alto	alto
errores de manteamiento de actualización de programas (software)	3	1	4	3	menor	catastrófico	Critico	bajo	alto	alto
difusión de software dañino	3	4	3	4	critico	medio	Critico	alto	medio	alto
caídas del sistema por agotamiento de recursos	2	1	1	4	insignificante	insignificante	catastrófico	bajo	bajo	alto
vulnerabilidades de los programas(software)	3	2	4	3	menor	catastrófico	Critico	bajo	alto	alto

inestabilidad de la línea de internet	4	1	1	4	insignificante	menor	catastrófico	bajo	medio	alto
errores de configuración	2	1	4	2	menor	critico	medio	bajo	medio	medio
fallo de servido de comunicación	3	1	1	4	menor	menor	catastrófico	bajo	Bajo	alto
degradación de soporte de almacenamiento de la información	1	1	1	3	insignificante	insignificante	Critico	bajo	Bajo	medio
PCs										
fuego	1	1	1	4	insignificante	menor	catastrófico	bajo	bajo	medio
movimiento sísmico	2	1	2	4	insignificante	menor	catastrófico	bajo	bajo	alto
error de usuario	4	3	4	1	menor	critico	insignificante	medio	alto	bajo
error de configuración	2	1	4	1	menor	menor	Critico	bajo	bajo	medio
suplantación de la identidad del usuario	2	4	3	2	catastrófico	critico	menor	alto	medio	bajo
acceso no autorizado	3	4	3	1	critico	medio	menor	alto	medio	bajo
robo de equipos	2	2	1	4	critico	insignificante	catastrófico	medio	bajo	alto
corte de energía eléctrica	4	1	2	4	insignificante	menor	catastrófico	bajo	medio	alto
condiciones inadecuadas de temperatura o humedad	3	1	2	4	insignificante	menor	Critico	bajo	bajo	alto
vulnerabilidades de los programas (software)	3	2	4	3	menor	critico	medio	bajo	alto	medio
error de mantenimiento actualizado de equipos (hardware)	2	1	1	3	medio	menor	Critico	medio	bajo	medio
instalación de software no autorizado	3	4	1	1	critico	menor	insignificante	alto	bajo	bajo
manipulación de quipos	4	3	1	2	critico	insignificante	menor	alto	bajo	medio

Fuente: Elaboración Propia ()

5.3.2 Propietario del riesgo

En la siguiente etapa de determino quien es el propietario del riesgo, es decir, la persona o entidad responsable de aprobar los riesgos adicionales y las estrategias de tratamiento para disminuir los riesgos a un nivel aceptable. En este caso de la investigación, se identificó que la única entidad propietaria del riesgo es la oficina de sistema de la empresa ITS Business SAC

5.3.3 Tratamiento de los riesgos

según la naturaleza del riesgo, existen cuatro opciones para manejarlo: eliminar, transferir, mitigar o asumir el riesgo.

Tabla 25. *Jerarquía de controles*

TRATAMIENTO	DESCRIPCIÓN
Eliminar	Una de las alternativas más difíciles de implementar y más costosas ya que puede implicar la eliminación de un archivo, proceso o del área del negocio es fuente de riesgo
Transferir	El riesgo fuera del apetito del riesgo se comparte con una o varias partes, pueden ser agentes externos.
Mitigar	Reducir el riesgo cuando se encuentra fuera del apetito del riesgo, se puede cambiar la probabilidad de ocurrencia cambar las consecuencias
Asumir	En este escenario se decide aceptar el riesgo cuando no es posible mitigarlo y se puede continuar la actividad que lo origino

Fuente: adaptado de "Diseño de un sistema de gestión de seguridad de la información para una empresa inmobiliaria alineado a la norma IO/IEC 27001:2013" Tesis (Justino Salinas, 2015) ()

Para el siguiente trabajo de investigación, consideraron los niveles de riesgo obtenidos y se estableció que los riesgos de nivel bajo serian el máximo riesgo asumible, por lo tanto, se empentaran controles para que todos los riesgos de nivel medio y alto, con el objetivo de reducir el riesgo producido por amenazas a nivel aceptable en las áreas afectadas.

Se dará prioridad de tratamiento a los riesgos de nivel alto, ya que es necesario aplicarles de manera urgente todas las medidas de

seguridad posible, así mismo, también es necesario aplicar urgente todas las medidas de seguridad posible. También es importante mencionar que los riesgos de nivel bajo se monitorean para evitar que su impacto y probabilidad aumenten con el tiempo.

5.3.4 Determinar los controles y declaración de aplicabilidad

En esta parte de han identificado las amenazas y se han establecido controles específicos para reducir los riesgos aun nivel aceptable. En la **tabla 26** se presentan los controles diseñados para disminuir los riesgos asociados al servidor de base de datos. Además, en el **anexo J** se contiene controles adicionales destinados a reducir los riesgos relacionados con el resto de los activos para reducir los riesgos de los activos de la empresa ITS Business SAC.

Tabla 26. *Controles para el tratamiento de riesgos de ITS Business S.A.C*

ACTIVO Y VALORACIÓN	AMENAZA, VULNERABILIDAD		ANÁLISIS Y EVALUACION DE RIESGO			TRATAMIENTO DEL RIESGO			
NOMBRE DEL ACTIVO	AMENAZA	VULNERABILIDAD	EVALUACION DE RISGO			JERARQUÍA DEL CONTROL	CONTROL ALIENADO A LA NTP ISO/IEC 27001:2014	CONTROL ESPECIFICO	RESPONSABLE
			C	I	D				
SERVIDORES -VISUALFACT, VISUALCONT, VISUALPLAN	Errores de administrador	No existe un plan/manual de las BDs que se manejan y sus requerimientos técnicos, ausencia de procedimientos de control de cambios.	Medio	bajo	Medio	Mitigar	**A.8.2** Clasificación de la información **A.12.4.3** Registros del administrador y del operador	Elaboración de un manual de procedimientos formal de control de cambios. Elaboración de un manual de procedimientos de manejo de servidores, capacitación en temas de seguridad	Oficial de seguridad/ Administrador de Servidores de BD
	Errores de configuración	Inexistencia de plan de configuración y manejo de log	bajo	medio	Medio	Mitigar	**A.12.4.3** Registros del administrador y del operador. **A.12.4.1** Registro de eventos.	Elaboración del manual de configuraciones servidor. Registro y actualizaciones de log de eventos	Oficial de seguridad/ Administrador de Servidores de BD
	Alteración accidental de la información	Inexistencia de normas de seguridad, mala configuración de roles y permisos.	Medio	bajo	medio	Mitigar	**A.8.2** Clasificación de la información **A.12.4.3** Registros del administrador y del operador. **A.12.4.1** Registro de eventos.	Control de versiones de software. Procedimiento formal de control de cambios. Verificación de roles y permisos	Oficial de seguridad/ Administrador de Servidores de BD
	Eliminación accidental de la información	Inexistencia de normas de seguridad y plan de contingencia.	bajo	alto	bajo	Mitigar	**A.8.2** Clasificación de la información **A.12.4.3** Registros del administrador y del operador. **A.12.4.1** Registro de eventos.	Control de versiones del software. Procedimiento formal de control de cambios. Verificación de roles y permisos.	Oficial de seguridad/ Administrador de Servidores de BD
	Figas de información	Inadecuada administración de seguridad, contraseñas poco seguras.	alto	bajo	bajo	Mitigar	**A. 12.4.3** Registros del administrador y del operador **A.7.2.3** Proceso disciplinario.	Establecimiento de métodos de cifrado y backup Gestión de permisos.	Oficial de seguridad/ Administrador de Servidores de BD

	Vulnerabilidades de los programas (software)	Falta de licencias, Poca monitorización de software/versiones	Medio	alto	alto	Mitigar	**A.14.2.4** Restricción sobre cambios a los paquetes software. **A.16.6.1** Gestión de vulnerabilidades técnicas.	Adquisición de licencia de programas y/o evaluaciones de uso de software libre. Gestión de vulnerabilidades	Oficial de seguridad/ Administrador de Servidores de BD
	Errores de mantenimiento / actualización de programas (software)	Falta de licencia, inexistencia de plan de mantenimiento y vigilancia tecnológica.	bajo	alto	alto	Mitigar	**A.16.6.1** Gestión de vulnerabilidades técnicas	Elaboración de un plan de mantenimiento y actualizaciones de software. Elaboración de un plan de contingencia	Oficial de seguridad/ Administrador de Servidores de BD
	Errores de mantenimiento/ actualización de equipos (hardware)	Inexistencia de plan de mantenimiento y vigilancia tecnológica, ausencia de un sistema de continuidad del negocio.	Medio	Bajo	Medio	Mitigar	**A.11.2.4** Mantenimiento de equipos **A.16.6.1** Gestión de vulnerabilidades técnicas	Elaboración de un plan de contingencia. Plan de mantenimiento de hardware	Oficial de seguridad/ Administrador de Servidores de BD
	Abuso de privilegios de acceso	Falta de políticas de acceso y auditorías internas. (cuentas de usuario sin auditar)	alto	medio	bajo	Mitigar	**A.7.2.3** Proceso disciplinario **A.9.4.1** Restricción de acceso a la información.	Elaboración de políticas de acceso. Rediseñar esquemas de seguridad basado en roles y permisos. Diseñar un esquema de privilegios sobre el servidor (fileserver)	Oficial de seguridad/ Administrador de Servidor de BD/ jefe de RR. HH.
	Difusión de software dañino	Falta de monitoreo del estado y reglas del firewall y antivirus, inadecuada asignación de roles y permisos, no existe políticas de seguridad.	alto	medio	alto	Mitigar	**A.12.2.2** Controles contra códigos maliciosos. **A.16.6.2** Restricción sobre la instalación de software	Plataforma de seguridad perimetral. Control de la red. Control de instalación de software Actualización de antivirus (monitorización)	Oficial de seguridad/ Administrador de Servidores de BD
	Acceso no autorizado	Falta de monitoreo del estado y reglas del firewall, antivirus, configuración incorrecta de las cuentas de usuario.	alto	alto	bajo	Mitigar	**A.14.2.8** Pruebas de seguridad del sistema	Rediseñar esquemas de seguridad basado en roles y permisos Diseñar un esquema de privilegios sobre el servidor (fileserver). Plataforma de seguridad perimetral.	Oficial de seguridad/ Administrador de Servidores de BD
	Caída del sistema por agotamiento de recursos	No existe un monitoreo de consumo de recursos hardware de los sistemas, falta de mantenimiento de equipos.	bajo	bajo	Medio	Mitigar	**A.11.2.3** Seguridad del cableado. **A.13.1.3** Segregación en redes	Plataforma de seguridad perimetral. Elaboración de un plan de contingencia – monitoreo preventivo de consumo de recursos Hardware de los sistemas.	Oficial de seguridad/ Administrador de Servidores de BD

	Corte del suministro eléctrico	Probabilidad a las variaciones de tensión. Mantenimiento inopinado	Bajo	Bajo	alto	Mitigar	**A.11.2.2** Servicios de suministro	Contra con sistema de alimentación ininterrumpida, Mantenimiento de sistema de alimentación ininterrumpida	Oficial de seguridad/ Administrador de Servidores de BD
	Condiciones inadecuadas de temperatura o humedad	Susceptibilidad a humedad, recalentamiento, polvo y suciedad	Bajo	Bajo	Medio	Mitigar	**A.11.2.1** Emplazamiento y protección de los equipos. **A.11.2.4** Mantenimiento de equipos	Ubicación adecuad de equipos según estándares internacionales. Plan de mantenimiento de equipos. Acondicionamiento adecuado del área.	Oficial de seguridad/ Administrador de Servidores de BD
	Degradación de los soportes de almacenamiento de la información	Equipo / dispositivos susceptibles a cambios de temperatura y humedad, falta de esquema de reemplazo	bajo	Bajo	Medio	Mitigar	**A.11.2.4** Mantenimiento de equipos	Plan de manteamiento de soportes de informático. Inventario de activos y monitoreo del funcionamiento y tiempo vida	Oficial de seguridad/ Administrador de Servidores de BD
	Inestabilidad de la línea de internet	Un solo proveedor de servicios de comunicaciones (para el servidor terminal), gestión inadecuada de la red	Bajo	Medio	alto	Mitigar	**A.13.1.2** Seguridad de servicios de red.	Plan de contingencia - Uso de varias líneas dedicadas y redundancia de servicios con diversos proveedores del servicio. – balanceo de carga. Acuerdos de nivel de servicio con el(los) proveedor(es) de comunicaciones	Oficial de seguridad/ Administrador de Servidores de BD
	fallo de servicios de comunicación	Desconfiguración de accesos remotos	Bajo	Bajo	alto	Mitigar	**A.11.2.2** Servicios de suministro	Elaboración de políticas de acceso. Plan de configuración de acceso	Oficial de seguridad/ Administrador de Servidores de BD
Local sede central de ITS Business SAC	Fuego	Extintores vencidos. Falta de capacitaciones en uso de extintores	Bajo	Bajo	Medio	Mitigar	**A.11.1.4** Protección contra amenazas externas y ambientales.	Compra de extintores y capacitación al personal	Administrador/ Gerencia
	desastres naturales(sismo)	Falta de señalización de Zonas seguras, así como un sistema eléctrico estable.	Bajo	Bajo	Alto	Mitigar	**A.11.1.4** Protección contra amenazas externas y ambientales.	Implementación de poso a tierra. Adquisición de equipos de alimentación ininterrumpida	Administrador/ Gerencia

Local sede central de ITS Business SAC	Acceso no autorizado	Inadecuado control de seguridad.	Medio	bajo	bajo	Mitigar	**A.11.1.1** Perímetro de seguridad física. **A.11.1.2** Controles de ingreso físico.	Establecer controles para indicar las áreas accesibles por los visitantes, implementar control de acceso restringido y controlar el acceso(Sistema de gestión de visitas).	Administrador/ Gerencia
	Robo de Equipos	No existe inventario de activos, inadecuada plataforma de vigilancia.	Medio	Bajo	Medio	Mitigar	**A.11.1.3** Asegurar oficinas, áreas e instalaciones. **A.11.2.5** Remoción de activos	Establecer controles de acceso restringido. Inventario de activos. Controles de remoción de activos.	Administrador/ Gerencia
	Corte del suministro eléctrico	Falta de algunos UPS, inestabilidad del sistema eléctrico.	bajo	bajo	alto	Mitigar	**A.11.1.4** Protección contra amenazas externas y ambientales.	Adquisición de equipos alimentación ininterrumpida. Mantenimiento equipos alimentación ininterrumpida. Acuerdos de niveles de servicio con Electrocentro.	Administrador/ Gerencia
	Condiciones inadecuadas de temperatura o humedad	inadecuada ubicación de equipos y ventilación del local	bajo	Bajo	alto	Mitigar	**A.11.1.4** Protección contra amenazas externas y ambientales.	Establecer controles de seguridad y salud en las oficinas.	Administrador/ Gerencia
Copias de Respaldo	Errores de administrador	Falta de plan de gestión de sistemas y políticas de respaldo, entrenamiento insuficiente en temas de seguridad	bajo	Bajo	alto	Mitigar	**A.8.2** Clasificación de la información **A.12.3.1** Respaldo de la información	Clasificación de la información, etiquetado y manejo. Establecer políticas de respaldo. Establecer un plan o cronograma de prueba de backups Almacenamiento de backups fuera de Data Center.	Oficial de seguridad/ Administrador de Servidores de BD

Fuente: *Elaboración Propia* ()

Finalmente, se ha creado el documento que cumple con los requisitos 6.1.3 (item d) de la norma NTP ISO/IEC 27001:2014, este documento, conocido como “Declaración de Aplicabilidad” contiene todos los controles necesarios identificados, si como la justificación de la inclusión o exclusión de los controles del **Anexo A**.

Este documento se adjunta como **Anexo I** de la tesis actual.

La declaración de aplicabilidad proporciona la siguiente información:

- **Sección:** contiene el identificador de sección de los controles propuestos en el anexo A de la norma NTP ISO/IEC 27001:2014
- **Objetivos:** es el objetivo de control.
- **Control:** es el nombre de control propuesto por la norma, el cual esta diseña para cumplir el objetivo establecido y está relacionado con un tema específico al que un riesgo puede estar relacionado.
- **Estado:** indica el estado actual del control en contexto de la empresa ITS Business SAC. Puede indicar si el control se está aplicando, se tiene previsto aplicar en el futuro o si no se aplica
- **Justificación:** proporciona una explicación o razón para determinar el control es aplicable no a la situación específica. Esta justificación puede basarse en la evaluación de riesgos, recursos disponibles u otros factores relevantes.

CAPITULO VI

CONCLUCIONES Y RECOMENDACIONES

6.1 Conclusiones

Habiendo concluido el análisis y diseño del SGSI, se llegó a las siguientes conclusiones:

- ✓ Se ha logrado crear el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo en el esfoque establecido por Norma Técnica Peruana (NTP) ISO/IEC 27001 para la empresa ITS Business SAC.

- ✓ Se logró definir el alcance del diseño del Sistema de Gestión de Seguridad de la Información para la empresa ITS BUSINESS S.A.C. *Siendo el alcance el proceso de gestión de la infraestructura tecnológica de la sede central de la empresa ubicado en Zarate San juan Lurigancho - Lima*.

- ✓ Se logró realizar la evaluación de los riesgos de seguridad de información para a empresa ITS BUSINESS S.A.C. *Para ello se adoptó la metodología MAGERIT V3 el cual permitió realizar la evaluación de riesgos de seguridad de información, así como también permitió identificar y valorar los activos y las amenazas*

- ✓ Se logró elaborar la lista de controles de seguridad para mitigar los riesgos identificados en el diseño del SGSI para la empresa ITS BUSINESS S.A.C. *Basándose en la NTP ISO/IEC 27001:2014 el cual permitirá establecer las métricas que ayudaran a medir la eficacia y eficiencia del SGSI una vez que este haya sido implementado.*

- ✓ Se logró obtener la certificación IEC/ISO 27001 de forma parcial para la empresa ITS Business SAC. requisito indispensable para proveedores de PSE (Proveedores de Servicios Electrónicos).

6.2 Recomendaciones

- ✓ La empresa necesita establecer una serie de medidas de seguridad con el fin de mejorar su protección y cumplir con los requisitos establecidos en la NT ISO/IEC 27001:2014.

- ✓ Durante el trabajo de investigación de identificó que la empresa ITS Business SAC necesita implementar un sistema de Gestión de Seguridad de la Información y contar con la documentación correspondiente relacionada con la seguridad de la información. Se sugiere contratar los servicios de una consultoría que brinde la orientación y apoyo en la implementación exitosa de la norma.

- ✓ La falta de controles orientados a proteger la información que se intercambia con terceros, se puede generar consecuencias graves para la empresa y afectar de manera negativa su imagen ante sus pares interesados, por tales motivos, se sugiere que la empresa implemente sistemas de cifrado para garantizar que la información se mantenga integra, confidencial y autentica.

- ✓ Dentro de la entidad se ha notado que un personal cumple el rol de oficial de seguridad de la información, pero también tiene otras responsabilidades y tareas adicionales. Se sugiere que la entidad defina de manera claras las funciones y responsabilidad específicas del oficial de seguridad de la información. Esto ayudara que la persona encargada tenga un enfoque más claro del área y pueda llevar a cabo sus tareas de manera efectiva.

- ✓ Se recomienda genera conciencia de seguridad de la información en los trabajadores de toda la entidad, mediante capacitaciones y charlas informativas. Además, es necesario que la empresa ITS Business SAC asigne presupuesto para la implementación del SGS (establecimiento de controles, capacitaciones, mantenimiento, mejorar continua).

6.3 Referencia Bibliográfica

R. Peltier, T., Peltier, J., & Blackley, J. (2005). Information Security Fundamentals. USA: Auerbach Publications. Obtenido de http://index-of.co.uk/Hacking-Coleccion/95%20-%20Information.Security.Fundamentals.Ebook%20Een%20%5B-PUNISHER-%5D.pdf

Aguirre Mollehuanca, D. (2014). Diseño De Un Sistema De Gestión De Seguridad De Información Para Servicios Postales Del Perú S.A. Lima, Peru.

ATENCIO BAZAN, E. L. (2019). *Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión.* Obtenido de http://repositorio.undac.edu.pe/bitstream/undac/1474/4/T026_10133566_M.pdf

Ccesa Quincho, M. (2016). Diseño De Un Sistema De Gestión De Seguridad De La Información Bajo La NTP ISO/IEC 27001:2014 Para La Municipalidad Provincial De Huamanga. Huamanga, Peru.

Chiavenato, I. (2006). Introducción a la Teoría General de la Administración. En *Introducción a la Teoría General de la Administración* (pág. 110). Mexico: McGraw-Hill Interamericana.

Diario el Peruano. (22 de Marzo de 2013). *Normas Legales.* Obtenido de https://diariooficial.elperuano.pe/pdf/0036/ley-proteccion-datos-personales.pdf

Escalante Coronel, D. M. (2019). Diseño De Un Sistema De Gestión De Seguridad De La Información Bajo El Enfoque De La NTP ISO/IEC 27001 Para La Dirección De Salud Virgen De Cocharcas – Chincheros. Andahuaylas, Peru: jose maria arguedas.

Excellence-ISOTools. (2015). *ISOTools Excellence*. Obtenido de https://www.isotools.pe/normas/ntp-iso-27001/

Fernandez Rivero, P., & Gómez Fernández , L. (2015). Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. Madrid, España: Primera Edicion.

Gomez. (2015). Cómo implementar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.

Goméz Fernández , L., & Fernández Rivero , P. P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.* Madrid, España: AENOR.

Gomez Vieites, A. (2011). *Enciclopedia de la Seguridad Informatica* (Segunda Edicion ed.). (R.-M. S. Publicaciones, Ed.) Madrid, España: RA-MA. Obtenido de https://books.google.com.pe/books?id=Bq8-DwAAQBAJ&printsec=frontcover&dq=alvaro+gomez+2011&hl=es&sa=X&ved=2ahUKEwjWj6qN4o_rAhVEdt8KHbzEB0sQ6AEwAHoECAMQAg#v=onepage&q=alvaro%20gomez%202011&f=false

Guanoluisa Huertas, J. E., & Maldonado Soliz , I. F. (2015). *Analisis de Riesgos y Diseño de un Plan de Seguridad de la Informacion para el Consejo Nacional de Igualdad de Discapacidades "CONADIS".* Quito.

Gutiérrez Amaya, C. (1 de Myo de 2013). *MAGERIT: metodología práctica para gestionar riesgos*. Obtenido de https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Guzman Silva, C. (2015). *Diseño De Un Sistema De Gestión De Seguridad De La Información Para Una Entidad Financiera De Segundo Piso.* Obtenido de https://alejandria.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y

Harán , J. (5 de setiembre de 2019). *welivesecurity by eset.* Obtenido de Eset Latinoamerica: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

Hirt, G., & Ferrell, O. (2004). Introducción a los Negocios en un Mundo Cambiante. Mexico: McGraw-Hill Interamericana.

INDECOPI. (2014). Norma Técnica Peruana “NTP-ISO/ IEC 27001:2014. Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Lima, Peru.

ISO 27000. (2018). *ISO 27000.ES*. Obtenido de https://www.iso27000.es/glosario.html

ISO/IEC 27001. (2013). *Normais27001.es*. Obtenido de https://normaiso27001.es/#h1

Justino Salinas, I. I. (2015). Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001: 2013. *Tesis*, 50.

López Jaramillo, D. M., & Vásquez Mejía, S. A. (2016). *Tabajo de Graduacion Previo a la Obtención del Titulo de Ingeniero en Sistemas y Telematica.* Obtenido de http://dspace.uazuay.edu.ec/handle/datos/5391

López Neira, A., & Ruiz Spohr, J. (2005). *ISO27000.ES*. Obtenido de https://www.iso27000.es/sgsi.html

LRQA Entidad ceriticadora ISO 27001. (s.f.). *LRQA*. Obtenido de https://www.lrqa.com/es-es/iso-27001/#accordion-%C2%BFqu%C3%A9eslanormaiso27001?

M. Farias-Elinos. (Mayo de 2004). *Perfil del Oficial de Seguridad Informática.* Obtenido de http://www.cudi.edu.mx/rfc/drafts/draft4.pdf

MAGERIT. (2012). *MAGERIT- V.3 Metodologia de Analisis y Gestion de Riegos de los sistema de Informacion.* (M. d. Técnica, Ed.) Obtenido de http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

MAGERIT V3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (2016). *Portal de Administración Electrónica*. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

NTP ISO/IEC-17799. (18 de Marzo de 2015). *Blog especializado en Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com/2015/03/ntp-isoiec-17799-norma-tecnica-peruana/

Peruano, D. e. (22 de Octubre de 2013). *Ley de Delitos Informaticos.* Obtenido de https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Peruano, D. e. (10 de Marzo de 2014). *Ley de Delitos Informacticos .* Obtenido de https://leyes.congreso.gob.pe/Documentos/Leyes/Textos/30171.pdf

Quero, O. (10 de Julio de 2019). *OBS Business School*. Obtenido de https://obsbusiness.school/int/maestria-en-ciberseguridad

SUNAT. (23 de Diciembre de 2020). *RESOLUCIÓN DE SUPERINTENDENCIA N.º 000221-2020/SUNAT.* Obtenido de https://www.sunat.gob.pe/legislacion/superin/2020/221-2020.pdf

SUNAT. (2021). *Padrón de Proveedores de Servicios Electrónicos – PSE.* Obtenido de https://www.sunat.gob.pe/orientacion/padrones/pse/ProveedoresServiciosElectronicos-PSE.pdf

UNE-ISO/IEC 27000:2014. (2014). *Normaiso27001.es.* Obtenido de https://normaiso27001.es/referencias-normativas-iso-27000/

ANEXOS

Anexo A

Evaluación completa del estado inicial de la Empresa ITS BUSINESS S.A.C respecto a la NTP ISO/IEC 27001: 2014

SECCIÓN	REQUERIMIENTO DE LA ISO/IEC 27001	ESTADO	EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? / ¿QUÉ SE TENDRÍA QUE HACER?)	VALORACIÓN
4	**CONTEXTO DE LA ORGANIZACIÓN**	**No diseñado**	Se recomienda realizar un análisis exhaustivo del entorno de la empresa ITS Business SAC. Esto implica comprender tanto los factores internos y externos que puedan influir en su SGSI, así como identificar las partes interesadas, y los requisitos y la documentación del alcance del SGSI.	**10%**
4.1	**Comprender la Organización y contexto.** La organización **debe** determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI	**Parcialmente diseñado**	La empresa ITS Business SAC tiene documentos que describen su Misión, Visión, matriz FODA y estrategias, pero no aborda de manera clara los aspectos de seguridad, se recomienda realizar objetivos de seguridad que estén en línea con los objetivos estratégicos de la empresa.	**25%**
4.2	**Comprender las necesidades y expectativas de las partes interesadas.** La organización **debe** determinar las partes interesadas y los requisitos de las mismas.	**No diseñado**	**Sugerencia:** identificar a las partes interesadas y comprender las necesidades y expectativas de estas partes con relación a la seguridad de la información.	**5%**
4.3	**Determinar el alcance del SGSI.**	**No diseñado**	**Sugerencia.** Definir y establecer el alcance SGSI, teniendo en cuenta los aspectos en la referencia 4.1 y 4.2, una vez definido el alcance documentarlo de forma clara para que las partes interesadas pueden entenderlo.	**0%**
4.4	**Sistema de Gestión de Seguridad de la información.** La organización **debe** establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta Norma Técnica Peruana	**No diseñado**	**Sugerencia.** implementar una estrategia que el SGSI tena una mejora continua según manifiesta la NTP actual. **Establecer el alcance de los límites del SGSI.**	**15%**
5	**LIDERAZGO**	**Parcialmente diseñado**	**El Titular de la entidad tiene la responsabilidad de liderar y asegurar que se asignen roles y responsabilidades, se establezca una política de seguridad de la información y se fije objetivos para la seguridad de la información, todo ello con el fin de mostrar compromiso y liderazgo en materia de SGSI en la institución.**	**25%**

5.1	Liderazgo y compromiso. La alta dirección debe demostrar liderazgo y compromiso respecto al SGSI.	**No diseñado**	El titular (máxima autoridad de la organización) de la entidad debe mostrar liderazgo y compromiso	**20%**
5.2	Política.	**No diseñado**	Es necesario establecer la Política de Seguridad que estén alineados con los objetivos y propósitos de la organización como lo manifiesta en la (Sección 6.2), luego definir las reglas y directrices para proteger la información. Asegurando que todos los empleados tengan conocimiento de ello.	**15%**
5.3	Roles, responsabilidades y autoridades organizacionales.	**No diseñado**	La alta dirección debe garantizar que se asignes y comuniquen las responsabilidades y la autoridad para los roles relacionados con la seguridad de la información. Esto ar que los miembros de la organización sepan los términos de protección de la de información.	**20%**
	a) asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de esta Norma Técnica Peruana	**No diseñado**	Designar un responsable auditor que compruebe que el SGSI está conforme al NTP vigente.	**0%**
	b) reportar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.	**No diseñado**	Asignar un responsable que reporte a la alta dirección sobre el desempeño del SGSI.	**0%**
SECCIÓN	**REQUERIMIENTO DE LA ISO/IEC 27001**	**ESTADO**	**EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? / ¿QUÉ SE TENDRÍA QUE HACER?)**	**VALORACIÓN**
6	**PLANIFICACIÓN**	**No diseñado**	Adoptar, planificar y documentar el procedimiento de valoración y tratamiento de riesgos de la seguridad de la información. Establecer y documentar los objetivos de seguridad de la información conforme a los propósitos de la organización y elaborar un plan para lograr estos objetivos de seguridad de la información.	**10%**
6.1	**Acciones para tratar los riesgos y oportunidades**	**No diseñado**	Adoptar, planificar y documentar el procedimiento la valoración y tratamiento de riesgos de la seguridad de la información.	**15%**
6.2	Objetivos de seguridad de la información y planificación para conseguirlos	**No diseñado**	Establecer los objetivos de seguridad de la información alineados a los objetivos estratégicos de la organización y elaborar un plan para lograr estos objetivos de seguridad.	**0%**
7	**SOPORTE**	**No diseñado**		**20%**
7.1	**Recursos** La organización **debe** determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.	**No diseñado**	Asignar presupuesto para la implementación, mantenimiento y mejora continua del SGSI.	**20%**

7.2	**Competencia**	**No diseñado**	Determinar las competencias del personal a su cargo para un correcto desempeño del SGSI, cuando sea necesario tomar acciones para adquirir las competencias necesarias sobre la seguridad de la información, documentar las competencias como evidencia.	**10%**
7.3	**Concientización** Las personas que trabajan bajo el control de la organización **deben** ser conscientes de la política de seguridad, su contribución a la efectividad del SGSI y las implicancias de no tener la conformidad de los requisitos del SGSI.	**No diseñado**	Concientizar al personal que trabaja en la organización sobre la importancia de la seguridad de la información, la política de seguridad y el papel crucial que cumple cada uno de ellos en el correcto desempeño de SGSI, asimismo concientizarlos sobre las consecuencias de no cumplir con los requisitos del SGSI	**10%**
7.4	**Comunicación** La organización debe determinar la necesidad de comunicaciones internas y externas relevantes al sistema de gestión de seguridad de la información incluyendo:	**No diseñado**	Se recomienda tener comunicación con entidades dedicadas a la seguridad de la información para obtener estrategias y/o capacitaciones para el personal. Se recomienda documentar los procedimientos de comunicación para tenerlos como evidencia e incluir en el mismo la comunicación interna.	**20%**
7.5	Información documentada	**Parcialmente diseñado**	Existe documentación de origen externo (Resoluciones, leyes, Ejem. "LEY DE PROTECCIÓN DE DATOS PERSONALES LEY N° 29733" etc.) Identificados que serán usados en la planificación y posterior implementación del SGSI en la empresa ITS BUSINESS S.A.C. Se sugiere empezar a elaborar la documentación necesaria exigida por la NTP vigente para lograr la efectividad del SGSI asimismo determinar los procedimientos de creación, actualización y control de la documentación.	**20%**
8	**OPERACIÓN**	**No diseñado**		**0%**
8.1	Planificación y control operacional	**No diseñado**	Planificar, controlar y documentar los procesos necesarios para cumplir con los requisitos de seguridad de la información y estar seguros de que los procesos se llevan a cabo acorde a lo planeado.	**0%**
8.2	Evaluación de riesgos de seguridad de la información	**No diseñado**	Planificar los intervalos de tiempo en los que se llevarán a cabo las evaluaciones de riesgos de seguridad de la información, documentar los resultados de éstas evaluaciones.	**0%**
9	**EVALUACIÓN DEL DESEMPEÑO**	**No diseñado**	Implementar el SGSI y elaborar un plan para evaluar periódicamente su funcionamiento y garantizar que el sistema se mantiene eficaz a lo largo del tiempo. Asimismo documentar dichas evaluaciones.	**0%**
9.1	Monitoreo, medición, análisis y evaluación	**No diseñado**	Establecer procedimientos para realizar el monitoreo, medición, análisis y evaluar el desempeño de la seguridad de la información y la efectividad del SGSI. Documentar los resultados del monitoreo, medición, análisis y evaluación del SGSI.	**0%**

9.2	Auditoría interna	**No diseñado**	No existen documentos de resultados de auditorías que se hayan realizado por la gerencia en el que se contempla la no conformidad de seguridad de la información. Se recomienda planificar auditorías internas y levantar la no conformidad de la auditoría interna para el cumplimento legal.	**0%**
9.3	Revisión por la gerencia	**No diseñado**	No existe documentación (resultado de auditoría) que dan a conocer el estado actual de la organización respecto al SGSI (no implementado) y la orden de implementación de las funciones de seguridad.	**0%**
10	**MEJORAS**	**No diseñado**	Implantar el SGSI y elaborar un plan de mejora continua para actualizar el SGSI de acuerdo a los cambios y novedades de la organización, las tecnologías, las amenazas, etc., tratando de mantener los riesgos controlados en todo momento.	**0%**
10.1	No conformidades y acción correctiva	**No diseñado**		**0%**
10.2	Mejora Continua La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información.	**No diseñado**		**0%**
	PUNTAJE TOTAL DE LA EVALUACION DE REQUISITOS DE LA NTP ISO/IEC 27001:2014			**14%**

Anexo B

Cuestionario de aceptación del sistema de gestión de seguridad de la información y diagnóstico inicial de la seguridad de la información

Nombre: …….

1. ¿Tiene conocimiento de la existencia de un sistema de gestión de seguridad de la información dentro de la empresa ITS Business SAC?
   Sí ◯ **No** ◯
2. ¿indique si cree que el diseño de un sistema de gestión de la seguridad de la Información (SGSI) ayudara con mejorar la seguridad de información de su área de trabajo?
   Sí◯ **No** ◯
3. ¿Indique si con el uso del sistema de gestión de seguridad de la información se logrará un cambio positivo en su área de trabajo?
   Sí ◯ **No** ◯
4. ¿Usted estaría de acuerdo con la implementación del sistema de gestión de la seguridad de la información en su área de trabajo?
   Sí ◯ **No** ◯
5. Dentro de su área de trabajo, ¿estaría de acuerdo con programas y capacitaciones dirigidos a todos los trabajadores con el propósito de concientizar sobre la seguridad de la Información?
   Sí ◯ **No** ◯
6. ¿Estarías dispuesto a trabajar en colaboración para diseñar e implementar un sistema de gestión de seguridad de la información en tu puesto de trabajo?
   Sí ◯ **No** ◯
7. ¿Considera usted que existe información que debe ser resguarda debidamente en su área de trabajo?
   Sí ◯ **No** ◯
8. ¿considera que en su área de trabajo se ha clasificado la información de acuerdo a la importancia que tienen para la empresa ITS Business SAC?
   Sí ◯ **No** ◯
9. ¿Recibió capacitaciones en su área laboral en referencia a la seguridad de la información?

Sí ◯ **No** ◯

10. ¿En su área de trabajo ¿se consideran la seguridad de información cuando se gestiona un proyecto?

    Sí ◯ **No** ◯

11. Dentro de su área laboral ¿se considera la seguridad de información cuando se gestiona un proyecto?

    Sí ◯ **No** ◯

12. ¿Cuándo ingresa a su computador y/o laptop cuenta con una clave de acceso?

    Sí ◯ **No** ◯

13. Cuando su laptop o computador no está en uso ¿Se activa de forma automática el bloqueo de pantalla con contraseña para proteger la información?

    Sí ◯ **No** ◯

14. ¿Durante este año ha sufrido alguna modificación o pérdida de información sin autorización (virus, acceso de personas no autorizadas, deterioro, tras papeleo, etc.)?

    Sí ◯ **No** ◯

15. ¿Durante el año se ha filtrado o divulgado información sensible para la empresa ITS Business SAC sin su autorización o conocimiento?

    Sí ◯ **No** ◯

16. ¿Se ha llevado a cabo una evaluación de los riesgos asociados a la información en tu puesto de trabajo?

    Sí ◯ **No** ◯

17. ¿Se ha llevado a cabo análisis de seguridad de la red en su área de trabajo?

    Sí ◯ **No** ◯

18. ¿Cuenta con software antivirus actualizado en su puesto de trabajo?

    Sí ◯ **No** ◯

19. ¿genera copias de seguridad (backups) para proteger su información?

    Sí ◯ **No** ◯

20. ¿cree usted que su oficina está protegida contra amenazas externas o ambientales que puedan generar pérdidas de información?

    Sí ◯ **No** ◯

Anexo C

Imágenes de los servidores de la ITS Business

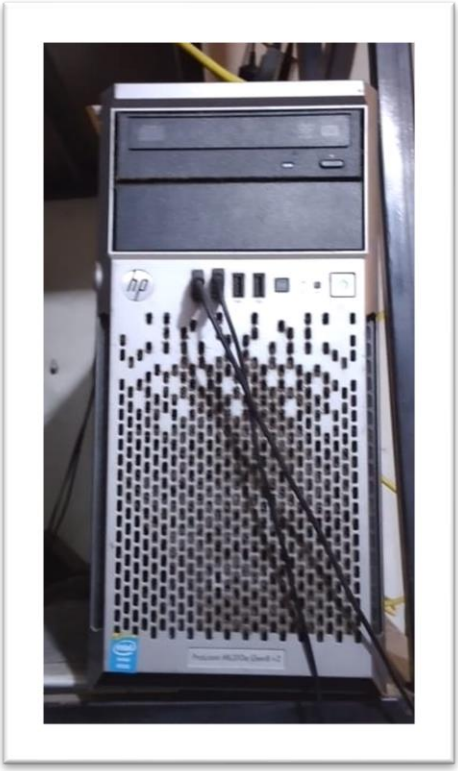


Figura 29: Servidor Local

Figura 30: Servidor Terminal

Figura 31: Cableado Switch y Teléfonos

Figura 32: Switch y Router

INTERCERT®

CERTIFICADO DE REGISTRO

INTERCERT certifica por la presente que el Sistema de Gestión de Seguridad de la Información

ITS BUSINESS SOCIEDAD ANONIMA CERRADA

JR. COYLLUR NRO. 280 URB. ZARATE (CDRA 18 AV GRAN CHIMU) LIMA - LIMA - SAN JUAN DE LURIGANCHO, PERÚ.

Ha sido evaluado con éxito según los requisitos de

ISO 27001:2013

Para el alcance de

ACTIVIDADES DE TECNOLOGÍA DE LA INFORMACIÓN Y DE SERVICIOS INFORMÁTICOS; ACTIVIDADES DE CONTABILIDAD, TENEDURÍA DE LIBROS, AUDITORÍA Y CONSULTORÍA FISCAL, EN EMPRESAS PÚBLICAS Y PRIVADAS A NIVEL NACIONAL.
SOA Version-1.0

Fecha de Certificación Inicial : Septiembre 24, 2021
Fecha de Emisión del Certificado : Septiembre 24, 2021
Fecha de Validez del Certificado : Septiembre 23, 2022
Fecha de Recertificación : Septiembre 23, 2024

Número de Registro: IC-IS-2109135

Emitido en nombre de InterCert
Jefe- Certificaciones

INTERCERT REGISTERED

La validez de este certificado se puede verificar en **www.intercert.com** o por correo electrónico en **info@intercert.com**, este certificado es propiedad de **INTERCERT INC.** 2001 Timberloch Place - Suite 500, The Woodlands, Texas 77380, United States y debe ser devuelto a pedido.

Figura 33: Certificado De Registro de ISO 27001

Anexo D

Alcance del sistema de gestión de seguridad de la información

1. Propósito, alcance y usuarios

El propósito de la elaboración de este documento es definir claramente cuáles son los límites del sistema de gestión de seguridad de la información (SGSI) de la empresa ITS Business y es aplicable a toda la documentación perteneciente al SGSI.

Los únicos usuarios autorizados a este documento son los miembros del comité de seguridad de la información y el personal autorizado de la empresa ITS Business SAC.

2. Alcance del SGSI

En la empresa ITS BUSINESS S.A.C el alcance definido del sistema de seguridad de la información (SGSI), abarca todos los sistemas de información, procesos, tecnología y personas. Ya que se ha identificado que todos sus procesos de negocio son claves en el SGSI.

La aplicabilidad de este sistema de gestión de seguridad de la información (SGSI) es solo para la sede principal de la empresa que se encuentra ubicada en Zarate, San Juan de Lurigancho, Lima. Esto Limitando las actividades y los procesos que se ejercen en esta sede.

Anexo E

Cuestionario para identificar activos

Relación de activos - en cada tabla marque (x) los activos con los que cuenta la empresa ITS Business SAC

TABLA DE RELACION DE ACTIVOS DE TIPO DATO/INFORMACION

( ) Fichero o base de datos

( ) Capias de respaldo

( ) Datos de configuración de los sistemas de información

( ) Datos de gestión interna

( ) Credenciales (ejemplo contraseñas)

( ) Datos de control de acceso

( ) Registro de actividad o de los sistema de información

( ) Código fuente de los sistema de información

( ) Datos de prueba para la implementación de los sistema de información

TABLA DE RELACION DE ACTIVOS DE TIPO SERVICIO

( ) Anónimo (sin requerir identificación de usuario)

( ) Al público en general (sin relación contractual)

( ) A usuarios externos (bajo una relación contractual)

( ) Interno (a usuarios de la propia organización)

( ) Internet

( ) Acceso remoto a cuenta local

( ) Correo electrónico

( ) Almacenamiento de fichero(File server)

() Transferencia de fichero (FTP)

( ) Intercambio electrónico de datos (EDI)

( ) Servicios de directorio

( ) Gestión de identidades (servicios que permiten altas y bajas de usuarios de los sistema)

TABLA DE RELACION DE ACTIVOS DE TIPO SOFTWARE/APLICACIÓN INFORMATICAS

( ) Software de desarrollo propio

( ) Software a medida(subcontratado)

( ) Página web

( ) Internet

( ) Servicio de aplicaciones

( ) ERP (Enterprise Resource Planning- Planificación de recursos empresariales)

( ) Correo electrónico

( ) Sistema de gestión de base de datos

( ) Ofimática

( ) Antivirus

( ) Sistema operativo

( ) Gestor de máquinas virtuales

( ) Servidor de terminales

( ) Sistema de backup

TABLA DE RELACION DE ACTIVOS DE TIPO EQUIPOS INFORMATICOS

( ) PCs

( ) Servidor

( ) Equipamiento de respaldo

( ) Medios de impresión(impresoras y servidores de impresión)

( ) Escáneres

( ) Módems

( ) Comunicadores (Switch)

( ) Encaminadores (Router)

( ) Cortafuego (Firewall)

( ) Punto de Acceso inalámbrico

( ) Telefonía IP

( ) Otros: ……

TABLA DE RELACION DE ACTIVOS DE TIPO REDES DE COMUNICACIONES

( ) Red telefónica

( ) Comunicación radio

( ) Red inalámbrica

( ) Telefonía móvil

( ) Red local

( ) internet

TABLA DE RELACION DE ACTIVOS DE TIPO SOPORTE DE INFORMACION

( ) Discos duros

( ) Discos virtuales

( ) Almacenamiento en red

( ) Disquetes

( ) Cederrón (CD-ROM)

( ) Memorias USB

( ) DVD

( ) Cinta magnética

( ) Tarjetas de memoria

( ) Tarjetas inteligentes

( ) Material impreso

( ) Cinta de papel

( ) Otros: ……

TABLA DE RELACION DE ACTIVOS DE EQUIPAMIENTO AUXILIAR

( ) Fuente de alimentación

( ) Generadores eléctricos

( ) Cable eléctrico

( ) Fibra óptica

( ) Equipos de destrucción de soporte de información

( ) Suministros esenciales

( ) Mobiliario, armarios, etc.

( ) Otros:……..

Anexo F

Inventario de activos del proceso gestión de la infraestructura tecnológica

N°	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO	UBICACIÓN
1	Datos vitales	Datos de almacenamiento los diferentes sistemas de información esenciales para el funcionamiento de la ITS BUSINESS SAC	Dato/Información	Servidor
2	Archivos personales	Documentos personales de los trabajadores de la ITS BUSINESS SAC	Dato/Información	Computadores personales
3	Copias de respaldo (backup)	Copias de respaldo de datos/información que manejas los distintos sistemas de la IST BUSINESS SAC	Dato/Información	Servidos y PCs personales
4	Datos de configuración de los SI	Corresponde a los documentos, manuales y procedimientos relacionados con la administración de los diferentes SI	Dato/Información	Archivo físico (estantería)
5	Datos de gestión interna	Corresponde a los documentos de la ITS BUSINESS SAC	Dato/Información	Archivo físico (estantería)
6	Credenciales (contraseñas)	Usuario y contraseña que utilizan los usuarios para ingresar a los recursos tecnológicos	Dato/Información	C/ usuario guarda sus contraseñas
7	Datos de control de acceso	Corresponde a los datos de los usuarios internos que utilizan los sistemas de información y/o aplicaciones	Dato/Información	BD/Usuarios internos
8	Log de los sistemas de información	Log que contiene los registros de los eventos e seguridad y de los eventos de administración sobre aplicaciones	Dato/Información	Servidor
9	Correo electrónico	Correo electrónico corporativo	Servicio	Correo electrónico GMAIL
10	Gestión de privilegios	Corresponde al mecanismo para la administración y asignación de privilegios de acceso a los recursos tecnológicos y aplicaciones	Servicio	Sistemas de información
11	Base de datos	BD de los diferentes sistemas que almacenan la información de la entidad	Servicio	Servidor terminal
12	Base de datos clientes	BD almacenados de los clientes del facturador	Servicio	Servidor AWS
13	Página web principal	Página web Principal de la entidad	Software	VPS
14	Página web revista de consultoría	Página web Revista de consultoría	Software	VPS
15	Página web instituto de cont. electrónica	Página web instituto de contabilidad electrónica	Software	VPS
16	Facturador Electrónico	Sistema de facturación electrónica	Software/aplicación informática	Servidor AWS
17	Sistema VISUAL FACT	Sistema de gestión empresarial	Sistema Informático	Servidor terminal
18	Sistema VISUAL CONT	Sistema contable	Sistema Informático	Servidor terminal
19	Sistema VISUAL PLAN	Sistema de planillas	Sistema Informático	Servidor terminal
20	Computador de los trabajadores	Computadores que utilizar los trabajadores de la entidad	Equipos informáticos	Oficinas
21	Impresoras	Impresoras de la entidad	Equipos informáticos	Oficinas
22	Escáner	Escáner de oficina de sistemas	Equipos informáticos	Oficina de informática

23	Firewall	Equipos informáticos destinados a proteger la seguridad perimetral de la entidad	Equipos informáticos	Oficina de informática
24	Soporte de red	Equipamiento necesario para transmitir datos: Reuters, swicth	Equipos informáticos	servidor
25	Red local	Red de comunicaciones cableada	Redes de comunicación	Red local
26	Red inalámbrica	Red de comunicaciones inalámbricas	Redes de comunicación	Área de ventas
27	Internet	Red de redes	Redes de comunicación	Red local
28	Equipos de comunicación de datos (teléfonos, celulares, mensajería)	Red de comunicación analógicas	Redes de comunicación	Oficinas de la ITS BUSINESS SAC
29	Disco duro externo	Disco duro externo	Soporte de información	Oficina de informática
30	Dispositivos de almacenamientos externos	CDs DVDs, etc	Soporte de información	Archivos físicos o estantes
31	Soporte no electrónico	Dispositivos físicos de almacenamiento no electrónico como material impreso	Soporte de información	Archivos físicos o estantes
32	Sistema de alimentación interrumpida	UPS	Equipamiento auxiliar	Oficinas de la ITS BUSINESS SAC
33	Gabinetes/ estantes	Armarios de soporte a los sistemas de información	Equipamiento auxiliar	Oficinas de la ITS BUSINESS SAC
34	Servidor interno	Centro de almacenamiento donde reside la infraestructura para soportar la operación de la empresa	Instalación	Oficina de la ITS BUSINESS SAC
35	Servidor terminal	Centro de almacenamiento donde reside la infraestructura de los clientes que usan los servicios de softwares (VC, VF, VP)	Instalación	Oficina de la ITS BUSINESS SAC
36	Servidor AWS	Centro de almacenamiento donde reside la infraestructura de los clientes que usan el sistema facturador	Servicio	Externo
37	Usuarios externos	Usuarios externos a la ITS BUSINESS SAC que usan los servicios atreves de páginas web, accesos remotos	Personal	Usuarios externos
38	Usuarios internos	Personal propio de ITS BUSINESS SAC	Personal	Oficina de sistemas de la ITS BUSINESS SAC
39	Personal de soporte técnico	Personal encargado del soporte de la ITS BUSINESS SAC	Personal	Oficina de sistemas de la ITS BUSINESS SAC
40	Personal desarrollo software (analista)	Personal encargado realizar (testeo previo) los diferentes sistemas informáticos de la ITS BUSINESS SAC	Personal	Oficina de sistemas de la ITS BUSINESS SAC
41	Personal de desarrollo de software (programadores)	Personal encargado desarrollar los diferentes sistemas informáticos de la ITS BUSINESS SAC	Personal	Oficina de sistemas de la ITS BUSINESS SAC
42	Personal de servicio soporte de ventas	Personal encargado brindar servicio de ventas de los software o servicios brindados por de la ITS BUSINESS SAC	Personal	Oficina de sistemas de la ITS BUSINESS SAC
43	Proveedores	Proveedores de tecnología y comunicaciones	Personal	Oficina de sistemas de la ITS BUSINESS SAC

Anexo G

Cuestionario para identificar amenazas y establecer probabilidad de materialización

N°	AMENAZAS	PROBABILDIAD DE OCURRENCIA				
		1	2	3	4	5
1	fuego					
2	desastres naturales(sismo)					
3	corte del suministro eléctrico					
4	condiciones inadecuadas de temperatura o humedad					
5	degradación de soportes de almacenamiento de la información					
6	fallo de servicios de comunicación					
7	error de usuario					
8	errores de configuración					
9	error del administrador					
10	alteración accidental de la información					
11	destrucción de la información					
12	caída del sistema por agotamiento de recursos					
13	difusión de software dañino					
14	fugas de información					
15	vulnerabilidades de los programas(software)					
16	errores de mantenimiento actualización de programas (software)					
17	error de mantenimiento actualización de equipos (hardware)					
18	Indisponibilidad del personal					
19	suplantación de identidad del usuario					
20	abuso de privilegios de acceso					
21	acceso no autorizado					
22	análisis de trafico					
23	modificación deliberada de información					
24	divulgación de información					
25	robo de quipos					
26	inestabilidad de la línea de internet					
27	manipulación de quipos					
28	instalación de software no autorizado					

PROBABILIDAD DE QUE SE MATERIALICE LA AMENAZA		
criterio	**valor**	**puntuación**
más de 2 años	imposible	1
anual	poco probable	2
mensual	posible	3
semanal	probable	4
diario	muy probable	5

Anexo H

Tabla de descripción de amenazas, riesgos y consecuencias.

AMENAZAS							RIESGOS	
N°	AMENAZAS	DESCRIPCION	TIPOS DE ACTIVO AFECTADOS	DIMENCIONES			RIESGO	CONSECUENCIA
				C	I	D		
1	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema	Equipos informáticos, soportes de información, equipamiento auxiliar, instalaciones			1	Incendio	Pérdida de los activos de información, daños materiales
2	Desastres naturales(sismo)	Incidentes que se producen sin intervención humana	Equipos informáticos, soportes de información, equipamiento auxiliar, instalaciones			1	Destrucción	No disponibilidad de los ambientes de trabajo de la empresa
3	Corte del suministro eléctrico	Cese de la alimentación de potencia	Equipos informáticos, soportes de información, equipamiento auxiliar			1	Malogren los equipos, pérdida de la información	Dejen de funcionar los servicios, insatisfacción del cliente, quejas de clientes
4	Condiciones adecuadas de temperatura o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	Equipos informáticos, soportes de información, equipamiento auxiliar			1	Malogren los equipos, pérdida de la información, pedidas económicas	No disponibilidad de los equipo y servicios prestados a través de ellos
5	Degradación de soportes de almacenamiento de la información	Degradación como consecuencia del paso del tiempo	Soportes de información			1	Pérdida de información	No disponibilidad de la información
6	Fallo de servicios de comunicación	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	Datos/información, servicios, aplicaciones (software), redes de comunicaciones			1	Perdida de información, desconfiguraciones	No disponibilidad de los servicios prestados, insatisfacción de los clientes, pérdidas económicas
7	Error de usuario	Equivocaciones de las personas cuando usan los servicios, datos, etc.	Datos/información, servicios, aplicaciones (software), soportes de información	2	1	3	Equivocaciones de los usuarios	No disponibilidad, de los datos/información, soportes de información, etc.
8	Errores de configuración	Introducción de datos de configuración erróneos.	Datos de configuración		1		Introducción de datos de configuración erróneos.	Pérdida de la integridad de los datos, errores en los sistemas

	Error del administrador	Equivocaciones de personas con responsabilidades de instalación y operación de los sistemas de información	Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones, soportes de información	3	2	1	Equivocaciones de los administradores	Mal funcionamiento de los servicios/SI
10	Alteración accidental de la información	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Datos/información, servicios, aplicaciones (SW) comunicaciones (tránsito), soportes de información, instalaciones		1		Alteración de los datos	Pérdida de la disponibilidad, molestia en los clientes
11	Destrucción de la información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	Datos/información, servicios, aplicaciones (SW), comunicaciones (tránsito), soportes de información, instalaciones			1	Eliminación de la Información	Pérdida total de información.
12	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	Servicios, equipos informáticos, redes de comunicaciones			1	No disponibilidad de los sistemas	Insatisfacción de los clientes, llamadas de atención, sanciones graves, pérdida de imagen, pérdida económica
13	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	Aplicaciones (software)	3	2	1	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	Pérdida de dato/información, perdida de la disponibilidad de los sistemas
14	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	Datos/información, servicios, aplicaciones (SW), comunicaciones (tránsito), soportes de información, instalaciones, personal (revelación)	1			Mal uso de la información, falta de controles	Pérdida de la confidencialidad, genera desconfianza en los clientes
15	Vulnerabilidades de los programas(software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	Aplicaciones (software)	3	1	2	Defectos en el código de los sistemas (programación)	Pérdida de la integridad de los datos o la capacidad de operar de los sistemas y/o aplicaciones, malestar en los usuarios que usan los sistemas.
16	Errores de mantenimiento actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	Aplicaciones (software)		1	2	Defectos en los procedimientos o controles de actualización del código.	Pérdida de la disponibilidad de los sistemas y/o aplicaciones, insatisfacción de los clientes
17	error de mantenimiento actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	Equipos informáticos, soportes electrónicos, equipamiento auxiliar			1	Defectos en los procedimientos o controles de actualización de los equipos.	Mal funcionamiento de los equipos, demoras al brindar soportes a los clientes
18	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, accidente, etc.	Personal interno			1	Insatisfacción de los clientes	No se atiendan los servicios adecuadamente

19	suplantación de identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	Datos/información, servicios, aplicaciones (software), redes de comunicaciones	1	2		Mal uso intencionado de la infraestructura tecnológica	Modificación de la información, malestar en los clientes
20	abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones	1	2	3	Abuso de privilegios para realizar tareas que no son de su competencia.	Modificación a los accesos o información, sanciones
21	acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones	1	2		Ataque a los recursos del sistema	Hackeo, modificación y perdida de información
22	Análisis de trafico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.	Datos/información, servicios, aplicaciones (SW), equipos informáticos, redes de comunicaciones	1			Alteración de los datos, perdida de información	Pérdida de la confidencialidad, modificación de los datos
23	Modificación deliberada de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	Datos/información, servicios (acceso), aplicaciones (SW), soportes de información.		1		Eliminación intencional de información	Pérdida de la confidencialidad y integridad de la información, malestar en los clientes
24	Divulgación de información	Revelación de información.	Datos/información, servicios, aplicaciones (software).			1	con ánimo de obtener un beneficio o causar un perjuicio,	Revelación de información privilegiada a terceros
25	Robo de quipos	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.	Equipos informáticos, soportes de información, equipamiento auxiliar	2		1	Carencia de un medio para prestar los servicios, es decir una indisponibilidad.	Pérdida económica, Insatisfacción de los clientes, sanciones graves, pérdida de imagen de la empresa
26	inestabilidad de la línea de internet	Fallo en el servicio prestado por un tercero	Servicios			1	No disponibilidad de los servicios, fallas en el servicio	Insatisfacción de los clientes, desconfiguraciones, pérdidas económicas
27	manipulación de quipos	Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	Aplicaciones (hardware)	1		2	Alteración intencionada del funcionamiento de los equipos	Mal funcionamiento de los equipos, desconfiguraciones
28	instalación de software no autorizado	Instalación de software no autorizado por parte del personal interno.	Aplicaciones (software)	1			Infectar/dañar el sistema	sanciones por uso de software no autorizado, funcionamiento incorrecto

Anexo I

Declaración de aplicabilidad

SECCIÓN	OBJETIVOS	CONTROL	ESTADOS	JUSTIFICACIÓN
A. 5	**Políticas de seguridad de la información**			
A.5.1	Proporcionar directrices de gestión de seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones	5.1.1 Políticas para la seguridad de la Información	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
		5.1.2 Revisión de las políticas para la seguridad de la información	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
A.6	**Organización de la seguridad de la información**			
A.6.1	Organización interna	6.1.1 Roles y responsabilidades en seguridad de la información	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
		6.1.2 Segregación de funciones	Aplicar	Se deben segregar las funciones para la realización de actividades, para evitar usos indebidos y el impacto de los incidentes de seguridad. Documentar
		6.1.3 Contacto con autoridades	Aplicar	Será necesario mantener contacto con foros especializados, revistas, etc. en temas de seguridad para estar alertas a la aparición de nuevas amenazas
		6.1.4 Contacto con grupos especiales de interés	Aplicar	Será necesario mantener contacto con foros especializados, revistas, etc. en temas de seguridad para estar alertas a la aparición de nuevas amenazas
		6.1.5 Seguridad de información en la gestión de proyectos	Aplicar	Será necesario identificar riesgos derivados de los proyectos
A.6.2	**Dispositivos móviles y teletrabajo:** Asegurar la seguridad del teletrabajo y el uso de dispositivos móviles	6.2.1 Política de dispositivos móviles	Aplicar	Los dispositivos móviles de la empresa tienen que ser de uso exclusivo para el contacto con los clientes y/o proveedores

				y la información obtenida tiene que estar debidamente organizada y archivada
		6.2.2 Teletrabajo	Aplicar	Sera necesario tener identificado cada puesto de trabajo, para tener un control adecuado de las conexiones remotas. Cada Pc tiene que estar protegida con un antivirus operativo y actualizado.
A.7	**Seguridad de los recursos humanos**			
A.7.1	Antes del empleo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera	7.1.1 Investigación de antecedentes	Aplicando	Se controla la selección del personal y se solicitan referencias.
		7.1.2 Términos y condiciones del empleo	Aplicando	Están establecidos en el contrato. Aunque se recomienda revisar para asegurar que no se excluyen responsabilidades de seguridad de la información relevantes
A.7.2	Durante el empleo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.	7.2.1 Responsabilidades de la gerencia	Aplicar	Es necesario documentar y comunicar las responsabilidades antes de capacitar al personal para que cumpla con las políticas de seguridad.
		7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	Aplicar	Según el análisis de riesgos, una amenaza habitual es la falta de formación en materia de seguridad.
		7.2.3 Proceso disciplinario	Aplicar	En la comunicación de responsabilidades y políticas se informará de las consecuencias de su incumplimiento.
A.7.3	Terminación y cambio de empleo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	7.3.1 Responsabilidades ante la finalización o cambio de empleo	Aplicar	Es necesario definir y contemplar en los contratos las responsabilidades ante la finalización del empleo, especialmente en relación a la confidencialidad de la información.
A.8	**Gestión de activos**			

A.8.1	Responsabilidad sobre los activos: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.	8.1.1 Inventario de activos	Aplicar	Necesario para llevar a cabo el proceso de evaluación de riesgos según la metodología adoptada.
		8.1.2 Propiedad de los activos	Aplicar	Es necesario identificar a los responsables de la seguridad de los activos.
		8.1.3 Uso aceptable de los activos	Aplicar	Se marcarán pautas de utilización de los activos.
		8.1.4 Retorno de activos	Aplicar	Cuando el contrato del empleado termina, éste devuelve todos los activos que poseía.
A.8.2	Clasificación de la información: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.	8.2.1 Clasificación de la información	Aplicar	Es necesario identificar la información acorde a los requisitos legales, valor, criticidad dentro de la empresa para aplicar medidas adecuadas.
		8.2.2 Etiquetado de la información	Aplicar	Necesario para que los usuarios de la información identifiquen las protecciones a aplicar.
		8.2.3 Manejo de activos	Aplicar	Para adoptar medidas de seguridad en función a la clasificación establecida.
A.8.3	Manejo de los medios: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.	8.3.1 Gestión de medios removibles	Aplicar	Necesario dada la proliferación de soportes USB
		8.3.2 Disposición de medios	Aplicar	Es necesario poner a disposición los medios de manera segura cuando ya no se requieran, sobre todo en los backups, formalizar el procedimiento.
		8.3.3 Transferencia de medios físicos	No aplica	No se extraerían soportes con información relevante fuera de la oficina.
A.9	**Control de acceso**			
A.9.1	Requisitos de la empresa para el control de acceso: Limitar el acceso a la información y a las	9.1.1 Política de control de acceso	Aplicando	Los usuarios cuentan con la información pertinente respecto a los permisos de acceso que poseen.

	instalaciones de procesamiento de la información.	9.1.2 Acceso a redes y servicios de red	Aplicando	Se controla el acceso a los servicios de red en función de la necesidad de uso.
A.9.2	Gestión de acceso de usuario: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.	9.2.1 Registro y baja de usuarios	Aplicar	El movimiento de alta y baja de usuarios en los sistemas haría indispensable este control. Contar con documentos formales autorizado por el jefe del proceso sobre la creación o baja de usuario.
		9.2.2 Aprovisionamiento de acceso a usuario	Aplicar	Se conceden o retiran los permisos, en función de las necesidades de acceso de los usuarios.
		9.2.3 Gestión de derechos de acceso privilegiados	Aplicando	Se restringe y controla la asignación y uso de acceso privilegiado.
		9.2.4 Gestión de información de autentificación secreta de usuarios	Aplicar	Dado el resultado del análisis de riesgo, se cree conveniente aplicar este tipo de control. Es decir, establecer un proceso de gestión controlado para la asignación de información confidencial de autenticación.
		9.2.5 Revisión de los derechos de acceso de usuarios.	Aplicando	Se realizan revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los usuarios manteniendo los registros de las revisiones y hallazgos.
		9.2.6 Remoción o ajuste de derechos de acceso	Aplicando	Se hace bajo petición del responsable directo del usuario.
A.9.3	Responsabilidades de los usuarios: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación	9.3.1 Uso de información de autentificación secreta	Aplicar	Buenas prácticas de seguridad serían necesario para proteger el acceso a la información.
A.9.4	Control de acceso a sistemas y aplicaciones: Prevenir el acceso no autorizado a los sistemas y aplicaciones	9.4.1 Restricción de acceso a la información	Aplicando	Los usuarios acceden únicamente a la información que requieren para desarrollar su trabajo.
		9.4.2 Procedimientos de ingreso seguro	Aplicando	Se requiere usuario y contraseña para el acceso a sistemas y aplicaciones.

		9.4.3 Sistema de gestión de contraseñas	Aplicar	Se requiere reforzar la gestión de contraseñas implantada actualmente al identificarse riesgos en este sentido.
		9.4.4 Uso de programas utilitarios privilegiados	Aplicar	Controlar el uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas para evitar incidentes de seguridad.
		9.4.5 Control de acceso de código fuente de los programas	Aplicar	Se reforzará el control de acceso al código fuente dado los riesgos identificados.
A.10	**Criptografía**			
A.10.1	Controles criptográficos: Asegurar el uso apropiado y efectivo de la criptografía para proteger la información	10.1.1 Política sobre el uso de controles criptográficos	Aplicar	Establecer políticas para determinar el uso de técnicas criptográficas que ayuden a proteger la información de la organización.
		10.1.2 Gestión de claves	No aplica	No se gestionan claves criptográficas en la entidad.
A.11	**Seguridad física y ambiental**			
A.11.1	Áreas seguras: impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización	11.1.1 Perímetro de seguridad física	Aplicar	Exigido por la NTP ISO/IEC 27001:2014
		11.1.2 Controles de ingreso físico	Aplicar	Establecer controles para indicar las áreas accesibles por los visitantes, implementar control de acceso restringido y controlar el acceso.
		11.1.3 Asegurar oficinas, áreas e instalaciones	Aplicar	En circunstancias aconsejables los equipos e información de encuentran aislados.
		11.1.4 Protección contra amenazas externas y ambientales	Aplicando	Se cuenta con lo básico para hacer frente a amenazas ambientales externas y ambientales (equipo contra incendios, otros)

		11.1.5 Trabajo en áreas seguras	Aplicando	Los servidores se encuentran en una zona segura dentro de la oficina, pero se debe mejorar este control.
		11.1.6 Áreas de despacho y carga	Aplicando	Se establece una zona en recepción para carga y descarga.
A.11.2	Equipos: Prevenir la pérdida, daño, robo o compromiso de activos o interrupción de las operaciones de la organización	11.2.1 Emplazamiento y protección de los equipos	Aplicando	Los equipos están en áreas controladas por personal autorizado.
		11.2.2 Servicios de suministro	Aplicando	Se dispone de un sistema de alimentación ininterrumpida.
		11.2.3 Seguridad del cableado	Aplicando	La instalación del cableado es segura.
		11.2.4 Mantenimiento de equipos	Aplicando	Existe personal de soporte técnico que da mantenimiento a los equipos. Mejorar el control manteniendo registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo
		11.2.5 Remoción de activos	No aplica	No salen equipos con información sensible de la entidad.
		11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Aplicar	Controlar el uso de los equipos que se prestan y supervisar el estado de salida y retorno.
		11.2.7 Disposición y reutilización segura de equipos	Aplicando	Los equipos descartados se formatean e instalan de nuevo para ponerlos en servicio nuevamente.
		11.2.8 Equipos de usuarios desatendidos	Aplicando	Los equipos cuentan con una clave de protección en caso estén desatendidos.
		11.2.9 Política de escritorio limpio y pantalla limpia	Aplicar	Se evitará así filtraciones de información indeseadas.
A.12	**Seguridad de las operaciones**			

A.12.1	Procedimientos y responsabilidades operativas: asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.	12.1.1 Procedimientos operativos documentados	Aplicar	Será necesario documentar algunos de los procedimientos de seguridad, especialmente los de requisito más técnico (copias de seguridad, mantenimiento del equipo, manejo de medios, manejo del correo y seguridad, recuperación del sistema)
		12.1.2 Gestión del cambio	Aplicando	Los cambios se realizarán de manera controlada.
		12.1.3 Gestión de la capacidad	Aplicar	Se implementará, por ejemplo, un rubro dedicado para los sistemas más críticos.
		12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones	Aplicando	Los entornos de desarrollo, prueba y operación serán separados para reducir los riesgos de acceso no-autorizado o cambios en los sistemas operacionales.
A.12.2	Protección contra códigos maliciosos	12.2.1 Controles contra códigos maliciosos	Aplicando	Se dispone de antivirus, aunque es necesario complementar este control con capacitación y concienciación de los usuarios.
A.12.3	Respaldo: Proteger contra la pérdida de datos	12.3.1 Respaldo de la información	Aplicando	Se realizan copias de seguridad diarias. Mejorar este control estableciendo periodos de prueba de recuperación de backup, almacenamiento fuera de daños y desastres del local principal.
A.12.4	Registros y monitoreos: Registrar eventos y generar evidencias	12.4.1 Registro de eventos	Aplicar	El registro de los operadores y el registro de fallas deberían ser usados para garantizar la identificación de los problemas del sistema de información.
		12.4.2 Protección de información de registros	Aplicar	Es necesario proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
		12.4.3 Registro del administrador y del operador	Aplicar	Necesario para revisar y proteger los registros asociados a las actividades del administrador y del operador del sistema.

		12.4.4 Sincronización del reloj	Aplicando	Para evitar fallas en las comunicaciones y asegurar la integridad de registro de eventos.
A.12.5	Control de software operacional: Asegurar la integridad de los sistemas operacionales	12.5.1 Instalación de software en sistemas operacionales	Aplicando	Se realizan instalaciones con el conocimiento del área de sistemas y con personal autorizado.
A.12.6	Gestión de vulnerabilidad técnica: Prevenir la explotación de vulnerabilidades técnicas	16.6.1 Gestión de vulnerabilidades técnicas	Aplicando	Se instalan las actualizaciones de seguridad en los puestos de los usuarios y los servidores.
		16.6.2 Restricción sobre la instalación de software	Aplicar	Restringir los permisos de instalación a los usuarios.
A.12.7	Consideraciones para la auditoría de sistemas de información: Minimizar el impacto de las actividades de auditoría en sistemas operacionales	12.7.1 Controles de auditoría de sistemas de información	Aplicar	Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.
A.13	**Seguridad de las comunicaciones**			
A.13.1	Gestión de seguridad de la red	13.1.1 Controles en la red	Aplicando	Se dispone de un firewall.
		13.1.2 Seguridad de servicios de red	Aplicar	Verificar los acuerdos de nivel de servicio con el proveedor y que estén estipulados en el contrato
		13.1.3 Segregación en redes	Aplicando	Las redes se encuentran separadas para prevenir accesos no autorizados.
A.13.2	Transferencia de información: Mantener la seguridad de la información transferida dentro de una organización y cualquier entidad externa	13.2.1 Políticas y procedimientos de transferencia de la información	Aplicando	Se realizan configuraciones para proteger la transferencia de información por las redes.
		13.2.2 Acuerdo sobre transferencia de información	Aplicando	Se realizan acuerdos de intercambio con los Clientes.
		13.2.3 Mensajes electrónicos	Aplicando	Los sistemas antivirus, el firewall disponen de medidas de protección.

		13.2.4 Acuerdos de confidencialidad o no divulgación	Aplicando	Los contratos con los clientes y personal incluyen acuerdos de confidencialidad.
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**			
A.14.1	Requisitos de seguridad de los SI: Garantizar que la seguridad de información es una parte integral de los SI a través del ciclo de vida completo. Esto también incluye los requisitos para SI que proporcionen servicios sobre redes públicas	14.1.1 Análisis y especificación de requisitos de seguridad de la información	Aplicar	Se exigirá a los analistas programadores y documentar el establecimiento de medidas de seguridad en el desarrollo de software.
		14.1.2 Aseguramiento de servicios de aplicaciones sobre redes públicas	Aplicar	Utilizar sistema de cifrado para la información, exigir al proveedor donde se aloja la PW acuerdos de seguridad. Nivel de confianza de la dirección.
		14.1.3 Protección de transacciones en servicios de aplicación	Aplicar	Realizar informe sobre el nivel global de confianza de la dirección, basado en el análisis de los últimos test de penetración, incidentes actuales o recientes, vulnerabilidades actuales conocidas para prevenir ataques web.
A.14.2	Seguridad en los procesos de desarrollo y soporte: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	14.2.1 Política de desarrollo seguro	Aplicar	Se establecerá una política para contemplar los requisitos de seguridad al desarrollar SI.
		14.2.2 Procedimiento de control de cambio del sistema	Aplicar	Cada cambio debe ser controlado y documentado.
		14.2.3 Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Aplicando	Se realizan pruebas al realizar cambios para comprobar que funcionen correctamente. Verificar también funciones de seguridad.
		14.2.4 Restricciones sobre cambios a los paquetes de software	No aplicar	No se realizan cambios en los paquetes de software de terceros.

		14.2.5 Principios de ingeniería de sistemas seguros	Aplicar	Se deberá establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.
		14.2.6 Ambiente de desarrollo seguro	Aplicar	Proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
		14.2.7 Desarrollo contratado externamente	No aplicar	No se contrata desarrollo externo
		14.2.8 Pruebas de seguridad del sistema	Aplicar	Realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
		14.2.9 Pruebas de aceptación del sistema	Aplicando	Se comprueba el cumplimiento de los requisitos especificados
A.14.3	Datos de prueba: Asegurar la protección de datos utilizados para las pruebas	14.3.1 Protección de datos de prueba	Aplicando	Se selecciona cuidadosamente, protege y controla los datos de prueba. Tener autorización de uso de datos reales.
A.15	**Relaciones con proveedores**			
A.15.1	Seguridad de la información en las relaciones con los proveedores: Asegurar protección a los activos de la organización que son accesibles por los proveedores.	15.1.1 Política de seguridad de la información para las relaciones con los proveedores	No aplicar	Se considera que el coste de implementación de este control superaría el beneficio que se obtendría.
		15.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores	Aplicando	En los contratos con los proveedores se incluyen acuerdos de confidencialidad. Verificar otros temas relacionados a la seguridad.
		15.1.3 Cadena de suministro de tecnología de información y comunicaciones	Aplicar	Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

A.15.2	Gestión de entrega de servicios del proveedor	15.2.1 Monitoreo y revisión de servicios de los proveedores	Aplicar	Monitorear y revisar la prestación de servicios de tercero para saber si ¿Lo que se recibe vale lo que se paga por ello?
		15.2.2 Gestión de cambios a los servicios de proveedores	Aplicando	Se firman nuevos contratos con los proveedores ante un cambio en las condiciones, revisar implicaciones en temas de seguridad.
A.16	**Gestión de incidentes de seguridad de la información**			
A.16.1	Gestión de incidentes de seguridad de la información y mejoras: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades	16.1.1 Responsabilidades y procedimientos	Aplicar	Necesario para implicar al personal en la gestión de incidencias.
		16.1.2 Reporte de eventos de seguridad de la información	Aplicar	La organización debe generar un procedimiento para gestionar adecuadamente cada uno de los eventos de seguridad de la información reportados por el personal o detectados por cada uno de los controles implementados, además se debe realizar charlas de capacitación con el personal para explicarles cuáles son sus roles y responsabilidades dentro del sistema de gestión.
		16.1.3 Reporte de debilidades de seguridad de la información	Aplicar	La organización debe capacitar adecuadamente a todo el personal de la organización para que sea capaz de detectar debilidades en el sistema de gestión de seguridad de información y puedan reportarlas adecuadamente, asimismo, se debe recalcar las sanciones que podrían recibir si es que deciden probar las debilidades encontradas
		16.1.4 Evaluación y decisión sobre eventos de seguridad de la información.	Aplicar	Es necesario identificar a una persona responsable de evaluar las incidencias y determine las acciones que se deben tomar.

		16.1.5 Respuestas a incidentes de seguridad de la información	Aplicar	Para solucionar las incidencias y documentarlos.
		16.1.6 Aprendizaje de los incidentes de seguridad de la información	Aplicar	Tener para esto un registro de incidencias y revisarlas periódicamente para prevenir incidencias.
		16.1.7 Recolección de evidencias	Aplicar	Mantener un registro de incidencias y de las operaciones realizadas.
A.17	**Aspectos de seguridad de la información en la gestión de continuidad del negocio**			
A.17.1	Continuidad de seguridad de la información: La seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio.	17.1.1 Planificación de continuidad de seguridad de la información	Aplicar	Necesario para identificar puntos débiles en cuanto a la continuidad de las operaciones.
		17.1.2 Implementación de continuidad de seguridad de la información	Aplicar	Necesario para garantizar la continuidad de los servicios.
		17.1.3 Verificación, revisión y evaluación de continuidad de seguridad de la información	Aplicar	Necesario para verificar la adecuación a los planes y de mejora continua
A.17.2	Redundancias: Asegurar la disponibilidad de las instalaciones y procesamiento de la información	17.2.1 Instalaciones de procesamiento de la información	No aplicar	Por el momento se considera que no es necesario debido a que el coste supera los beneficios obtenidos.
A.18	**Cumplimiento**			
A.18.1	Cumplimiento con requisitos legales y contractuales: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.	18.1.1 Identificación de requisitos contractuales y de legislaciones aplicables	Aplicar	Se debe identificar las leyes aplicables a la organización
		18.1.2 Derechos de propiedad intelectual	Aplicando	Se contempla como propiedad de la ITS Business los desarrollos realizados en la entidad. Disponer de los derechos de propiedad de software originales.

		18.1.3 Protección de registros	Aplicar	Se deben proteger los registros mediante medidas de seguridad física y lógica. Se debe establecer guías y procedimiento que especifiquen por cuanto tiempo la organización está dispuesta a almacenar la información.
		18.1.4 Privacidad y protección de datos personales	Aplicar	Se debe establecer un procedimiento para el adecuado manejo de la información personal almacenada dentro de la organización, en conformidad con la ley de protección de datos personales.
		18.1.5 Regulación de controles criptográficos	Aplicar	A nivel nacional existe una directiva que indica que la información sensible debe ser encriptado para asegurar su integridad y confidencialidad, esta directiva es la 007-95-INEI-SJI.
A.18.2	A.18.2 Revisiones de seguridad de la información: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.	18.2.1 Revisión independiente de la seguridad de la información	Aplicar	Se debe revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información, planificar las revisiones.
		18.2.2 Cumplimiento de políticas y normas de seguridad	Aplicar	En las auditorias se verificará el cumplimiento de políticas, procedimientos y normas.
		18.2.3 Revisión del cumplimiento técnico	Aplicar	Establecer un plan de revisión de los SI y verificar si cumplen con las políticas y normas de seguridad dispuesta por la organización.