UNIVERSIDAD PRIVADA DE TRUJILLO

FACULTAD DE INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA

DE SISTEMAS E INFORMÁTICA

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA BEST CABLE, AÑO 2022

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Bach. SANDHUAS PAREDES, BRYEN RAYKO

Bach. MONTENEGRO PEREZ, MAYKOL MILLER

ASESOR:

ING. FRANKLIN DIAZ DIAZ

TRUJILLO – PERÚ
2023

CERTIFICADO DE ANÁLISIS
magister

ICI-TESIS-MONTENEGRO-SANDHUAS

16% Similitudes

< 1% Texto entre comillas
< 1% similitudes entre comillas

0% Idioma no reconocido

Nombre del documento: ICI-TESIS-MONTENEGRO-SANDHUAS.docx
ID del documento: cf86f5f8da145ea609e043f2cf5c45e039554aab
Tamaño del documento original: 180,05 kB

Depositante: Facultad Ingeniería
Fecha de depósito: 17/7/2023
Tipo de carga: interface
fecha de fin de análisis: 17/7/2023

Número de palabras: 12.249
Número de caracteres: 85.368

Ubicación de las similitudes en el documento:

1	repositorioacademico.upc.edu.pe | Diseño de un Sistema de Gestión de Seguridad https://repositorioacademico.upc.edu.pe/bitstream/10757/652121/3/Monteza_ML.pdf 101 fuentes similares	4%		Palabras idénticas: 4% (530 palabras)
2	normaiso27001.es https://normaiso27001.es/wp-content/uploads/2019/02/Test-cumplimiento-ISO-27001.pdf 76 fuentes similares	4%		Palabras idénticas: 4% (515 palabras)
3	vdocuments.mx | NORMA TÉCNICA NTP ISO/IEC 27001 PERUANA 2014 [PDF Docum... https://vdocuments.mx/norma-tecnica-ntp-isoiec-27001-peruana-2014.html 93 fuentes similares	2%		Palabras idénticas: 2% (306 palabras)
	Documento de otro usuario #a2a4a4 El documento proviene de otro grupo 85 fuentes similares	2%		Palabras idénticas: 2% (310 palabras)
5	hdl.handle.net | Diseño de un sistema de gestión de seguridad de la información ba... https://hdl.handle.net/20.500.14168/504 80 fuentes similares	2%		Palabras idénticas: 2% (302 palabras)

Fuentes principales detectadas

N°	Descripciones Similitudes	Ubicaciones	Datos adicionales

Fuentes con similitudes fortuitas

N°	Descripciones Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario #d1e3ec El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (30 palabras)
2	seguridad-informatica5.webnode.es | Confidencialidad, Integridad y Disponibilidad ... https://seguridad-informatica5.webnode.es/news/confidencialidad-integridad-y-disponibilidad-de-la-inf...	< 1%		Palabras idénticas: < 1% (40 palabras)
3	boletines.exportemos.pe https://boletines.exportemos.pe/wp-content/uploads/2019/07/749.pdf	< 1%		Palabras idénticas: < 1% (30 palabras)
4	hdl.handle.net | Diagnóstico y propuesta de mejora del nivel de gestion de entregar ... https://hdl.handle.net/20.500.13032/2428	< 1%		Palabras idénticas: < 1% (21 palabras)
5	Documento de otro usuario #d1e3ec El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (20 palabras)

Fuentes ignoradas Estas fuentes han sido retiradas del cálculo del porcentaje de similitud por el propietario del documento.

N°	Descripciones Similitudes	Ubicaciones	Datos adicionales

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes

1. https://rincontic.org/2020/04/30/modelo-de-madurez-cobit/
2. https://www.firmae.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-ydisponibilidad/
3. https://www.incibe.es/en/node/2789
4. https://www.coursera.org/learn/information-security-data/lecture/7mqjl/anintroduction-to-knowledge-areas-in-information-security
5. http://repositorio.unp.edu.pe/bitstream/handle/UNP/1165/INDSAN-QUI-17.pdf?sequence=1&isAllowed=y

UPRIT	UNIVERSIDAD PRIVADA DE TRUJILLO DECLARACIÓN DE AUTENTICIDAD Y NO PLAGIO	CODIGO	FR-VI-038
		PAGINA	Página 01 de 01

DECLARACIÓN DE AUTENTICIDAD Y NO PLAGIO

Por el presente documento el(os) alumno(s) :

1.- Sandoval Perez, Bryan Rayko

2.- Montenegro Perez, Maykol Kilder

3.- —

Quien(es) han elaborado la

[X] TESIS [ ] TRABAJO DE SUFICIENCIA [ ] TRABAJO DE INVESTIGACIÓN

Denominada:

Implementación de un Sistema de Gestión de Seguridad de la Información en la Empresa Best Cable - año 2022

Para obtener el Titulo de Ingeniero de Sistemas e Informatica. otorgado por la Universidad Privada de Trujillo – UPRIT.

Declaramos que el presente trabajo ha sido íntegramente elaborado por mi (nosotros) y que en él no existe plagio de ninguna naturaleza, en especial copia de otro trabajo de tesis o similar presentado por cualquier persona ante cualquier instituto educativo o no.

Dejamos expresa constancia que las citas de otros autores, han sido debidamente identificadas en el trabajo, por lo que no hemos asumido como nuestras las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos o de la Internet.

Asimismo, afirmamos que los(el) miembro(s) del grupo hemos leído el documento de investigación en su totalidad y somos plenamente conscientes de todo su contenido. Todos asumimos la responsabilidad de cualquier error u omisión en el documento y somos conscientes que este compromiso de fidelidad de a tesis/trabajo de investigación tiene connotaciones éticas pero también de carácter legal.

En caso de incumplimiento de esta declaración, nos sometemos a lo dispuesto en las normas académicas de la Universidad Privada de Trujillo.

TRUJILLO, 05 / 07 / 2023

Firma Alumno1	Firma Alumno2	Firma Alumno3
DNI. 71559194	DNI. 73231133	DNI. —

HOJA DE FIRMAS

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA BEST CABLE, AÑO 2022

Autores:

Bach. SANDHUAS PAREDES, BRYEN RAYKO

Bach. MONTENEGRO PEREZ, MAYKOL MILLER

Dr. Gómez Avila, José Alberto

PRESIDENTE

Mg. Córdova Otero, Juan

SECRETARIO

Mg. Díaz Díaz, Franklin Alexis

VOCAL

DEDICATORIA

A Dios

Que siempre me ilumina y acompaña guiando mi camino

A mis padres

Por el apoyo constante e incondicional que me han brindado en cada una de mis decisiones, tanto en lo personal, como en lo profesional.

A mis docentes de la universidad

Por inspirarme a ser mejor motivarme a seguir siempre adelante

AGRADECIMIENTO

Deseo expresar mi más profundo y sincero agradecimiento a todas aquellas personas que de alguna manera u otra apoyaron a la realización de este proyecto, sin lo cual, no hubiese sido posible su realización.

Al personal administrativo de la Universidad Privada de Trujillo, por todo el apoyo profesional que nos ha brindado, por su orientación y consejos para la elaboración de este proyecto.

A la carrera profesional de Ingeniería de Sistemas e Informática de la Universidad Privada de Trujillo por la formación profesional de alta calidad brindada durante el periodo del que fui alumno.

ÍNDICE GENERAL

RESUMEN

Este trabajo está basado en la elaboración de un informe de evaluación que permite detectar los errores o falencias que existen en la empresa Best Cable con respecto a la seguridad de la información, por lo cual desarrollaremos un planeamiento de SGSI para dicha empresa.

En la etapa inicial se utilizaron las guías de evaluación de requisitos y la de evaluación de controles del anexo A de la NTP-ISO/IEC 27001:2014, obteniendo como resultado una brecha de cumplimiento del 34% y 41%, respectivamente. Por lo cual, en la siguiente etapa se propone el diseño del SGSI, explicando sus objetivos y políticas generales.

En la tercera etapa se identifican 27 activos dentro de la empresa, las cuales se califican y se hayan 16 amenazas dentro de estos activos; después, continuamos con la evaluación de los riesgos para así diseñar un plan de tratamiento; siguiendo con las referencias de la NTP ISO 27001:2014 (ANEXO A), proponiendo actividades para controlar el riesgo, junto con la fecha de implementación.

Finalmente establecemos las políticas y procedimientos para controlar los riesgos, esperando resultados positivos, para de esa manera reducir o eliminar la brecha de cumplimiento de las guías del anexo A de la NTP-ISO/IEC 27001:2014.

Palabras claves: seguridad de la información, ISO 27001, ISO 31000, NTP-ISO/IEC 27001:2014.

ABSTRACT

This work is based on the elaboration of an evaluation report that allows detecting the errors or shortcomings that exist in the Best Cable company with respect to information security, for which we will develop an ISMS planning for said company.

In the initial stage, the requirements evaluation guides and the control evaluation guides of Annex A of NTP-ISO/IEC 27001:2014 were used, resulting in a compliance gap of 34% and 41%, respectively. Therefore, in the next stage the design of the ISMS is proposed, explaining its objectives and general policies.

In the third stage, 27 assets are identified within the company, which are qualified and there are 16 threats within these assets; then we continue with the risk assessment in order to design a treatment plan; following the references of the NTP ISO 27001:2014 (ANNEX A), proposing activities to control the risk, together with the implementation date.

Finally, we establish the policies and procedures to control the risks, hoping for positive results, in order to reduce or eliminate the compliance gap with the guides of annex A of the NTP-ISO/IEC 27001:2014.Keywords: Administrative management, information systems, strategic planning.

Keywords: information security, ISO 27001, ISO 31000, NTP-ISO/IEC 27001:2014.

CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

En el siguiente informe se presenta a la empresa BEST CABLE, la cual busca en los últimos años ha venido adquiriendo una serie de equipos tecnológicos informáticos para la sistematización de algunos de sus procesos del negocio, agilizando las operaciones y la atención a sus clientes, así también implementar procesos de los que carecían para aumentar los servicios que ofrecen a un mayor alcance de más clientes.

En la actualidad se sabe bien que el contar con recursos informáticos es ventajoso para cualquier negocio y contar con una conexión a internet ya no es un lujo sino una necesidad imperante para cualquier negocio, más ahora con la creciente oferta de servicios en la nube que hace más necesario contar con todo tipo de tecnología al alcance de la organización para obtener ventaja competitiva.

El tener recursos informáticos de acceso local y remoto hace que los activos de la información con que cuenta la empresa, estén constantemente expuestos a diversos tipos de riesgos que aprovechan las vulnerabilidades que tienen estos recursos y que puedan conllevar a riesgos que se materialicen en amenazas y causen un alto impacto de valor negativo en los procesos principales de la organización, pudiendo generar pérdidas irrecuperables pudiendo llevar incluso al cierre del negocio.

Si en grandes empresas, que poseyendo recursos tecnológicos de última generación y recursos económicos para adquirir nuevos y suplantar los obsoletos, son propensos a cualquier ataque interno o externo que puedan poner en riesgo sus activos de información, es comprensiblemente pensar que en una pequeña o mediana empresa con recursos limitados o escasos, estos ataques puedan ser más propensos y fáciles de penetrar la seguridad mínima que tienen los activos de la organización.

Ante ello, la empresa consciente de esta realidad, se ve en la necesidad de salvaguardar sus activos de información con mecanismos especializados,

estandarizados y el personal calificado para un adecuado proceso de control de riesgos que lo evite, acepte, transfiera o reduzca.

1.2. Formulación del problema

¿De qué manera incide la implementación de un sistema de gestión de seguridad de la información en los activos de información de la empresa Best Cable?

1.3. Justificación

1.3.1. Tecnológica

Las empresas utilizan la tecnología para gestionar sus procesos. Hay muchos Las empresas de todo el mundo aún se resisten al cambio a pesar del software y decidieron que las herramientas informáticas habían crecido exponencialmente por su productividad trabajar de manera tradicional con poco o ningún uso de estas herramientas por temor a nuevas formas de hacer las cosas y no saber. Esto se logra de la siguiente manera el nacimiento del sistema informático tuvo un enorme impacto en las familias y sociedades empresariales. A medida que el proceso se gestiona con eficacia, el personal administrativo puede hacer esto desde dispositivos que están conectados a internet las 24 horas del día, sin importar dónde se encuentren.

1.3.2. Teórica

Este estudio se basa en la creencia de que el uso de las tecnologías de la información es fundamental en el mundo actual y con estas tecnologías se puede apoyar cualquier actividad que realiza la sociedad para lograr mejores resultados, ahorrar tiempo y resultados cuando la información relevante se realiza de forma manual y tradicional tendrá que consumir muchos recursos. Ahora es bien sabido que la tecnología en todo el mundo se está desarrollando rápidamente y no es ajena a la ejecución de procesos comerciales, grandes o pequeños, ya que se ha demostrado que la implementación de sistemas

computarizados para gestionar su gestión brinda una serie de ventajas a una empresa y usuarios finales y comunidades afectadas.

1.3.3. Metodológica

El desarrollo de este estudio se llevó a cabo de acuerdo con el método científico mundialmente reconocido, el cual es confiable y válido para determinar los resultados y sacar conclusiones sobre ciertos temas sociales. Siguiendo estos lineamientos, fue posible probar la validez de las hipótesis propuestas sobre las preguntas que inspiraron este estudio y concluir que la herramienta es relevante para el proyecto de investigación. Además, durante la ejecución de los resultados de la búsqueda se utilizó el método RUP para desarrollar software confiable, eficiente y seguro, por lo que podemos concluir que esta investigación se basa en procedimientos científicos reconocidos.

1.3.4. Académica

Este trabajo se justifica profesionalmente, ya que servirá como material de referencia y/o guiará a otros estudiantes en trabajos similares en el tema de sistemas de información basado en la web.

1.4. Objetivos

1.4.1. Objetivo General

Asegurar la información de la empresa Best Cable, a través de la implementación de la seguridad de la información.

1.4.2. Objetivos Específicos

- Implementar la norma ISO 27001 respecto al SGSI.
- Aplicar los dominios, dominios y objetivos de la norma ISO 27002
- Implementar la norma ISO 31000 respecto a Gestión de Riesgos

1.5. Antecedentes

Cortez Parra & Ocares Hermosa (2020), concluyen que el aumento de canales digitales con el fin de difundir la información de adoptar mascotas incrementa la cantidad de contactos que solicitan adoptar mascotas. Además, se tiene la difusión sobre nuevos clientes que tienen mayor interés en adoptar mascotas. Se ha mejorado la administración de información de las mascotas, por lo que se tiene más información con la cual administrar las solicitudes de adopción que se reciben y priorizar la promoción de adoptar mascotas en base al tiempo de estadía en el albergue. Se ha mejorado la distribución de información a las personas interesadas en adoptar, por lo que se ofrecen promociones personalizadas en base a los gustos de los contactos.

(Linares Borjas, 2017), cuyo objetivo general fue la implementación de un sistema de gestión académica vía web para mejorar el seguimiento del rendimiento académico de los alumnos de primaria en una institución educativa. En esta tesis se hace uso de las herramientas tecnológicas necesarias para la implementación de nuestro Sistema de Información, lo que nos permite usar de manera eficiente las fases del Proceso Unificado Racional (RUP).

(Azabache Martinez, 2018) de la Universidad Nacional de Trujillo en la misma ciudad tiene correlación con este proyecto en el objetivo del tiempo promedio en la generación de la planilla mensual , después de implementar el sistema es de 5 minutos y sin el sistema es de 12 minutos, por lo que se representa una mejora del 58.3% y el nivel de satisfacción del usuario del sistema luego de la implementación del sistema alcanza un puntaje de 4.86 en la escala de Likert ,mientras que antes era de 1.78 , lo que representa un incremento 3.08 puntos(61.6%)

1.6. Bases Teóricas

Sistema de Gestión de Seguridad de la Información

"Conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base los riesgos a los que enfrente la organización." (p.13, Gómez & Fernández, 2018)

"Preservar la confidencialidad. Integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos" (p.7, NTP ISO/IEC 27001:2016)

Control

Establecido por la ISO/IEC 27000:2018 como el significado de manejar los riesgos, incluyendo políticas, procedimientos, pautas, estructuras organizacionales o prácticas, que pueden ser de naturaleza administrativas, técnicas, gerenciales o legales.

Ciclo de Deming

El ciclo de Deming es llamado también modelo PDCA, es el sistema más utilizado para la implantación de planes de mejora continua. Está compuesto de 4 etapas de manera que al finalizar la última de ellas se comienza con la primera nuevamente; esto permite que la efectividad sea evaluada de manera continua, incorporando nuevas mejoras. (Deming, 2021)

Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados; es decir, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización. (Firma-e, 2014)

Integridad

Para la seguridad de información, integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas; es decir, que los datos sean

exactamente fueron creados sin alteraciones ni manipulaciones por parte de terceros. (NTP-ISO/IEC27001-2014, 2014)

Disponibilidad

La información puede ser accedida en el momento que sea requerida a través de canales adecuados siguiendo los procesos correctos. (Firma-e, 2014)

Seguridad de la Información

Práctica de defender la información de acceso o uso no autorizado, divulgación, interrupción, modificaciones, inspección, grabaciones o destrucción. Es un término en general que puede ser usado sin importar la forma de la data que tome, ya sea física o en una computadora (Komisarczuk, 2019).

Amenazas

Suceso desfavorable que puede ocurrir teniendo consecuencias negativas sobre los activos informáticos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. (CiberSeguridad, 2014)

Vulnerabilidades

Debilidad que se presenta en los activos que puede ser aprovechado por alguna fuente de amenaza para atentar contra las políticas de seguridad. (NIST800, 2014)

Activos Informáticos

Un activo es algo que tiene valor para la organización, sus operaciones comerciales y continuidad. Por esta razón se necesitan protegerse para asegurar la correcta operación del negocio y continuidad de sus operaciones. (Alexander, 2007)

ISO/IEC 27001

Kosituc (2014) citado en Bermudez y Bailón (2015), informan que una norma internacional que detalla lineamento de seguridad de la información de cualquier empresa controles para mejorar continuamente la seguridad física y lógica de la información de posibles robos o daños. La primera versión se publicó en el año 2005 y fue desarrollada en base a la norma británica BS 7799-2

Oficina Nacional de Gobierno electrónico e Informática ONGEI

Creada en junio del 2003, con el finalidad de liderar los proyectos, la normatividad y las diversas actividades en materia de Gobierno Electrónico que realiza el estado (ONGEI, 2017)

NTP-ISO/IEC 27001:2014. Tecnología de información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información.

Requisitos Norma técnica peruana elaborada con la finalidad de brindar los requisitos necesarios para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de información; así mismo, los requerimientos para la implementación de controles de seguridad para las necesidades de una organización, un sector de la misma, o un proceso, según el alcance del SGSI. De igual forma se establece la documentación exigida para su certificación en el caso del cumplimiento de todos los requisitos. Así mismo, en el Anexo A de la mencionada norma se establece los controles que deben ser implementados en la organización para garantizar la seguridad de información. (NTP-ISO/IEC27001-2014, 2014)

Magerit

SegúnSandoval (2017), Magerit es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Fases de la metodología Magerit

Incibe (2017), es una página titulada "Análisis de riesgos en 6 pasos" y detalla que las fases de análisis de riesgo de la metodología son seis:

Fase 1. Definir el alcance. - es establecer el alcance del estudio.

Fase 2. Identificar los activos. - debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio

Fase 3. Identificar / seleccionar las amenazas. - identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado.

Fase 4. Identificar vulnerabilidades y salvaguardas. - La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades.

Fase 5. Evaluar el riesgo. - Llegado a este punto disponemos de los siguientes elementos:

- Inventario de activos.
- Conjunto de amenazas a las que está expuesta cada activo.
- Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).
- Conjunto de medidas de seguridad implantadas

Fase 6. Tratar el riesgo. - Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido.

1.7. Definición de términos básicos

Seguridad de la información

Es la disciplina que se encarga de proporcionar la evaluación de riesgos y amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo la normativa o las buenas prácticas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información de activos.

Sistema de información

Según Alarcón, 2006, la planificación estratégica de sistemas de información dirige sus esfuerzos a identificar y establecer prioridades sobre las tecnologías y las aplicaciones susceptibles de reportar un máximo beneficio a la empresa.

Un plan estratégico de sistemas de información indica la dirección correcta en el desarrollo de los sistemas de información, el modo de proceder, los criterios de proceder, los criterios de selección, los mecanismos de evaluación, etc.

1.8. Formulación de la hipótesis

La implementación de la seguridad de la información mejora la seguridad de los activos de información de la empresa XXX.

1.9. Propuesta de aplicación profesional

Seguridad de la información

CAPÍTULO II: MATERIALES Y MÉTODOS

2.1. Material

2.1.1. Personal

PERSONAL	UNIDAD	CANTIDAD
INVESTIGADOR	Persona	1
ASESOR	Persona	1

2.1.2. Materiales

DESCRIPCIÓN	UNIDAD	CANTIDAD
PC PERSONAL: CORE I7 + 8GB RAM, 500 GB DISCO DURO	Unidad	1
PC ESCRITORIO: CORE I7 + 8GB RAM, 1TB DISCO DURO	Unidad	1
IMPRESORA EPSON L3110	Unidad	1

2.1.3. Insumos

INSUMOS	UNIDAD	CANTIDAD
CARTUCHOS NEGRO Y DE COLOR	Unidad	4
HOJAS BOND A4	Millar	3
FÓLDER MANILA	Unidad	10
LAPICEROS	Unidad	5
CORRECTOR	Unidad	2

2.1.4. Servicios

DESCRIPCIÓN	UNIDAD	CANTIDAD
PASAJES	Unidad	150
FOTOCOPIAS	Unidad	250

2.2. Material de estudio

2.2.1. Población

El número de trabajadores de la empresa en 15.

2.2.2. Muestra

Al ser la población de 15, por lo tanto la muestra también es de 15.

2.3. Tipo de investigación

2.3.1. De acuerdo a la orientación o finalidad

Investigación aplicada ya que se solucionará problemas utilizando conocimientos adquiridos, procesos y recursos existentes que permitan el desarrollo de la presente investigación.

2.3.2. De acuerdo a la técnica de contrastación

Pre-experimental; debido a que existió una hipótesis que contrastar, tomando como muestra al menos una variable (independiente) para determinar cuál es el efecto que causa y su relación con las demás variables (dependientes)

2.3.3. Nivel de investigación

El nivel de investigación es Descriptivo; debido a que los estudios descriptivos permiten detallar situaciones o eventos, es decir, como es y cómo se manifiesta determinado fenómeno. (Sampieri, R., 1998)

2.3.4. Diseño de investigación

El diseño de investigación consiste en primero realizar una medición previa de la variable dependiente a ser utilizada, previa la aplicación de la variable independiente (Pre-Test).

Posteriormente se realiza la aplicación de la variable independiente, para que finalmente se toma una nueva medición de la variable dependiente después de la aplicación de la variable independiente (Pos-Test).

O_1 → X → O_2

Donde:

O_1: Seguridad de la información en la empresa Best Cable antes de la implementación del SGSI.

X: sistema de información web.

O_2: Seguridad de la información en la empresa Best Cable después de la implementación del SGSI.

2.4. Técnicas, procedimientos e instrumentos

2.4.1. Para recolectar datos

Encuesta: De acuerdo con Trespalacios, Bello y Vásquez (2005), son técnicas de investigación descriptiva que ayudan a reconocer de primera mano, los ítems a desarrollar, las personas escogidas en una muestra que representa a la población, especificar respuestas y establecer la técnica empleada para recopilar información que se pueda ir obteniendo.

TÉCNICA	INSTRUMENTO	FUENTE
ENTREVISTA	Cuestionario	Área administrativa
ENCUESTA	Guía de entrevista	Área administrativa
ANÁLISIS DOCUMENTAL	Ficha de recolección de datos	Área administrativa

2.4.2. Para procesar datos

Se seleccionaron los instrumentos de evaluación debidamente validados y confiables, para seguidamente aplicarlos a la muestra, se analizaron los datos obtenidos utilizando el Excel haciendo las descripciones y haciendo uso del programa estadístico IBM SPSS v26 y Microsoft Excel, para resolver la correlación con la prueba R de Pearson, entre las condiciones y dimensiones; para culminar planteando las conclusiones que dan respuesta a los objetivos.

Para hacer efecto del análisis se han utilizado la estadística descriptiva e inferencial.

2.5. Operacionalización de variables

Variable	Definición conceptual	Definición operacional	Dimensión	Indicador	Escala de medición
Sistema de Gestión de Seguridad de la Información	Es un sistema que se basa en el empleo de la computación y que interrelaciona software, hardware y recursos humanos para el procesamiento y almacenamiento de datos siendo capaz de entregar información relevante y cuyo proceso se realiza a través de internet.	Esta variable será medida a través de tres dimensiones: Controles de seguridad existentes en la institución, Nivel de Riesgo y los activos con los que cuenta la institución.	Controles de seguridad Riesgos Activos	Cantidad de controles existentes Nivel de riesgo Valoración de activos	Escala de razón Ordinal Ordinal

CAPÍTULO III: RESULTADOS

3.1. Desarrollo de la metodología

3.1.1. Etapa I: Diagnóstico inicial

III.1.1.1. Evaluación de los requisitos de la NTP-ISO/IEC 27001:2014

En esta sección se especifican las reglas del negocio a tener en cuenta en la ejecución de los diferentes procesos definidos en la organización.

Para el presente sistema de información web, se basa en las siguientes reglas:

Guía de Evaluación de los Requisitos de la NTP-ISO/IEC 27001:2014				
Objetivo: Obtener la información necesaria sobre los requisitos indicados en la NTP-ISO/IEC 27001:2014 para la implementación del Sistema de Gestión de Seguridad de Información en la empresa BEST CABLE; con la finalidad de determinar el nivel de cumplimiento de los mismos.				
Fecha: 12/10/2022				
Nombre: *CESRA ALCIDES PEREZ QUISPE*		Cargo: *ASISTENTE DE SISTEMAS*		
Criterio NTP-ISO/IEC 27001:2014	Pregunta	Cumple (Sí | No)	Evidencia	Nivel de madurez
4. CONTEXTO DE LA ORGANIZACIÓN				
4.1. Comprender la organización y su contexto	¿Están identificados los objetivos del SGSI?	SI		3
	¿Se han identificado las cuestiones internas y externas relacionadas con la seguridad de la información?	SI		3
	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la información?	SI		3
4.2. Comprender las necesidades y expectativas de las	¿Se han identificado las partes interesadas?	NO		0

partes interesadas				
4.3. Determinar el alcance del SGSI	¿Se ha determinado el alcance del SGSI y se conserva información documentada?	SI		3
4.4. Sistema de Gestión de Seguridad de Información	¿El SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	SI		3
5. LIDERAZGO				
5.1. Liderazgo y Compromiso	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	SI		3
	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	SI		3
	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	NO		0
5.2. Política	¿Se ha definido una Política de la Seguridad de la Información?	SI		3
	¿Se ha comunicado la política de la Seguridad de la información a toda la administración?	SI		4
5.3. Roles,	¿Se han asignado las responsabilidades	SI		4

responsabilidades y Autoridades Organizacionales	autoridades l Seguridad l sobre a de a Información?			
6. PLANIFICACIÓN				
6.1. Acciones para tratar los riesgos y las Oportunidades	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?	SI		3
	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?	SI		3
	¿Se ha definido un proceso de tratamiento de riesgos?	NO		0
6.2. Objetivos de seguridad de la información y planificación para conseguirlos	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?	SI		3
7. SOPORTE				
7.1. Recursos	¿Se identifican y asignan los recursos necesarios para el SGSI?	SI		3

7.2. Competencias	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?	NO		0
	¿Se mantiene información actualizada sobre la competencia del personal?	NO		0
7.3. Concientización	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?	SI		4
	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?	SI		5
7.4. Comunicación	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?	SI		4
	¿Existe un procesopara comunicar las deficiencias o malas prácticas en la seguridad de la Información?	NO		0
7.5. información Documentada	¿Se dispone de la documentación requerida por la norma más la requerida por la Norma ISO 27001 incluyendo registros?	NO		0
8. OPERACIÓN				
8.1. y Planifi cación control operacional	¿Se han definido actividades basadas en un sistema de mejora continua que permita cumplir los objetivos, políticas y requisitos de la seguridad de la información?	SI		3

8.2. Evaluación de riesgos de seguridad de información	¿Realiza la administración la evaluación de riesgos de manera periódica?	NO		0
8.3. Tratamiento de riesgos de seguridad de información	¿La administración cuenta con un plan de tratamiento de riesgos de seguridad de información?	NO		0
9. EVALUACIÓN DEL DESEMPEÑO				
9.1. Monitoreo, medición, análisis y evaluación	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?	NO		0
9.2. Auditoría Interna	¿Se ha establecido una De programación ¿Auditorías Internas y asignado responsables?	SI		3
	¿Se ha definido el alcance y los requisitos para el informe de auditoría?	SI		3
9.3. Revisión la por Gerencia	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?	NO		0
10. MEJORA				
10.1. No conformidades y acción correctiva	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?	NO		0
10.2. Mejora Continua	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?	NO		0

Nivel de Cumplimiento de los Requisito de la NTP-ISO/IEC 27001:2014				
Criterio NTP-ISO/IEC 27001:2014	Nivel de madurez	Nivel de cumplimiento		
		Real	Esperado	Brecha
4. Contexto de la organización	2.25	75%	100%	25%
5. Liderazgo	2.6666667	89%	100%	11%
6. Planificación	3.5	117%	100%	-17%
7. Soporte	3.2	107%	100%	-7%
8. Operación	1	33%	100%	67%
9. Evaluación del desempeño	1.3333333	44%	100%	56%
10. Mejora	0	0%	100%	100%
Nivel de cumplimiento		66%	100%	34%

III.1.1.2. Resultado por los controles del anexo A de la NTP-ISO/IEC 27001:2014

Se describen en la siguiente tabla:

Guía de Evaluación de los controles del anexo A de la NTP-ISO/IEC 27001:2014				
Objetivo: Obtener la información necesaria sobre la aplicación de los controles referidos en el Anexo A de la NTP ISO/IEC 27001:2014 para la implementación del Sistema de Gestión de Seguridad de Información en la empresa *BEST CABLE*; con la finalidad de determinar el nivel de cumplimiento de los mismos.				
Fecha: 12/10/2022				
Nombre: *CESAR ALCIDES PEREZ QUISPE*		Cargo: *ASISTENTE DE SISTEMAS*		
Anexo A NTP-ISO/IEC 27001:2014	Pregunta	Cumple (Sí | No)	Evidencia	Nivel de madurez

A.5. POLÍTICAS DE SEGURIDAD DE INFORMACIÓN				
A.5.1. Dirección de la Gerencia para la Seguridad de la Información				
A.5.1.1. Políticas para la seguridad de información	¿La administración ha publicado y aprobado las políticas sobre la Seguridad de la información?	SÍ		2
A.5.1.2. Revisión de las políticas para la seguridad de la información	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	SÍ		2
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN				
A.6.1. Organización Interna				
A.6.1.1. Roles y Responsabilidades para la seguridad de la información	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?	SI		3
A.6.1.2. Segregación de Funciones	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?	SI		3
A.6.1.3. Contacto con autoridades	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la información?	SI		2
A.6.1.4. Contacto con grupos especiales de interés	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	NO		0

A.6.1.5. Seguridad de la información en la gestión de proyectos	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la administración?	NO		0
A.6.2. Dispositivos Móviles y teletrabajo				
A.6.2.1. Política de dispositivos móviles	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?	SÍ		3
A.6.2.2. Teletrabajo	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?	SÍ		3
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS				
A.7.1. Antes del Empleo				
A.7.1.1. Selección	¿Se investigan los antecedentes de los candidatos?	SÍ		2
A.7.1.2. Términos y condiciones del empleo	¿Se incluyen cláusulas relativas a la seguridad de la información en los contratos de trabajo?	SÍ		3
A.7.2. Durante el Empleo				
A.7.2.1. Responsabilidades de la Gerencia	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?	SÍ		2
A.7.2.2. Conciencia, educación y capacitación sobre la seguridad de la información	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?	SÍ		1
A.7.2.3. Proceso disciplinario	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de	SÍ		2

	los incumplimientos sobre las políticas de la seguridad de la información?			
A.7.3. Terminación y cambio de empleo				
A.7.3.1. Terminación o cambio de responsabilidades del empleo	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?	SÍ		2
A.8. GESTIÓN DE ACTIVOS				
A.8.1. Responsabilidad de los Activos				
A.8.1.1. Inventario de activos	¿Se ha realizado un inventario de activos que dan soporte al negocio y de Información?	SÍ		1
A.8.1.2. Propiedad de los Activos	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?	SÍ		2
A.8.1.3. Uso aceptable de los Activos	¿Se han establecido normas para el uso de activos en relación a su seguridad?	SÍ		1
A.8.1.4. Retorno de activos	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?	NO		0
A.8.2. Clasificación de la Información				
A.8.2.1. Clasificación de la información	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?	SÍ		2

A.8.2.2. Etiquetado de la información	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?	SI		1
A.8.2.3. Manejo de activos	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?	NO		0
A.8.3. Manejo de los Medios				
A.8.3.1. Gestión de medios Removibles	¿Existen controles establecidos para aplicar a soportes extraíbles?	SÍ		2
A.8.3.2. Disposición de Medio	¿Existen procedimientos establecidos para la eliminación de soportes?	SÍ		1
A.8.3.3. Transferencia de los medios	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad?	SÍ		2
A.9. CONTROL DE ACCESOS				
A.9.1. Requisitos de la Empresa para el Control de Accesos				
A.9.1.1. Política de control de accesos	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?	SÍ		3
A.9.1.2. Accesos a redes y servicios de red	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?	SÍ		4
A.9.2. Gestión de Accesos de usuario				

A.9.2.1. Registro y baja de Usuarios	¿Existen procesos formales de registros de usuarios?	SÍ		4
A.9.2.2. Aprovisionamiento de acceso de usuario	¿Existen procesos formales para asignación de perfiles de acceso?	SÍ		3
A.9.2.3. Gestión de derechos de acceso Privilegiado	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?	SÍ		4
A.9.2.4. Gestión de información de autenticación secreta de Usuario	¿Se ha establecido una política específica para el manejo de información clasificada como secreta?	SÍ		3
A.9.2.5. Revisión de derechos de acceso de Usuario	¿Se establecen periodos concretos para renovación de permisos de acceso?	NO		0
A.9.2.6. Remoción o ajustes de derechos de acceso	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?	NO		0
A.9.3. Responsabilidad de los Usuarios				
A.9.3.1. Uso de Información de autenticación secreta	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?	SÍ		3
A.9.4. Control de Acceso a Sistema y aplicación				

A.9.4.1. Restricción de acceso a la información	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?	SÍ		3
A.9.4.2. Procedimientos de acceso seguro	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?	SÍ		4
A.9.4.3. Sistema de gestión de contraseñas	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?	SÍ		3
A.9.4.4. Uso de programas utilitarios privilegiados	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de seguridad?	SÍ		4
A.9.4.5. Control de acceso al código fuente de los programas	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?	SÍ		3
A.10. CRIPTOGRAFÍA				
A.10. Controles Criptográficos				
A.10.1.1. Política sobre el uso de controles criptográficos	¿Existe una política para el establecimiento de controles criptográficos?	SÍ		2
A.10.1.2. Gestión de Claves	¿Existe un control del ciclo de vida de las claves criptográficas?	SÍ		2
A.11. SEGURIDAD FÍSICA Y DEL AMBIENTE				
A.11.1. Áreas Seguras				

A.11.1.1. Perímetro de Seguridad física	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?	SÍ		3
A.11.1.2. Controles de acceso físico	¿Existen controles de acceso a personas autorizadas en áreas restringidas?	SÍ		3
A.11.1.3. Asegurar oficinas, áreas e instalaciones	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo?	SÍ		4
.11.1.4. Protección contra amenazas externas y ambientales	¿Se establecen medidas de protección contra amenazas externas y ambientales?	SÍ		3
A.11.1.5. Trabajo en áreas seguras	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?	SÍ		3
A.11.2. Equipos				
A.11.2.1. Emplazamiento y protección de equipos	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?	SÍ		4
A.11.2.2. Servicio de suministro	¿Se protegen los equipos contra fallos de suministro de energía?	SÍ		3
A.11.2.3. Seguridad en el cableado	¿Existen protecciones para los cableados de energía y de datos?	SÍ		2
A.11.2.4. Mantenimiento de equipos	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?	SÍ		3

A.11.2.5. Remoción de activos	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. que puedan contener información?	SÍ		4
A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?	SÍ		3
A.11.2.7. Disposición o reutilización segura de equipos	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?	SÍ		2
A.11.2.8. Equipos de usuarios desatendidos	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?	SÍ		3
A.11.2.9. Política de escritorio limpio y pantalla limpia	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?	SÍ		2
A.12. SEGURIDAD DE LAS OPERACIONES				
A.12.1. Procedimientos y responsabilidades operativas				
A.12.1.1. Procedimientos operativos documentados	¿Se documentan los procedimientos y se establecen responsabilidades?	SÍ		2
A.12.1.2. Gestión de cambio	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?	SÍ		3

A.12.1.3. Gestión de la capacidad	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?	SÍ		2
A.12.1.4. Separación de los entornos de desarrollo, pruebas y operaciones	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?	SÍ		3
A.12.2. Controles contra código malicioso				
A.12.2.1. Controles contra código malicioso	¿Existen sistemas de detección para software malicioso o malware?	NO		0
A.12.3. Respaldo				
A.12.3.1. Respaldo de la información	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?	SÍ		3
A.12.4. Registro y monitoreo				
A.12.4.1. Registro de eventos	¿Se realiza un registro de eventos?	SÍ		2
A.12.4.2. Protección de información de registro	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?	SÍ		2
A.12.4.3 Registro del administrador y del operador	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?	SÍ		3
A.12.4.4. Sincronización de reloj	¿Existe un control de sincronización de los distintos sistemas?	SÍ		3
A.12.5. Control de Software en la Producción				

A.12.5.1. Instalaciones de software en sistemas operacionales	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?	SÍ		2
A.12.6. Gestión de vulnerabilidad técnica				
A.12.6.1. Gestión de Vulnerabilidades técnicas	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?	NO		0
A.12.6.2. Restricciones de instalación de software	¿Se establecen medidas restrictivas para la instalación de software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?	SÍ		3
A.12.7. Consideraciones para la auditoria de los sistemas de información				
A.12.7.1. Controles de auditoría de información	¿Existen mecanismos de auditorías de medidas de seguridad de los sistemas?	SÍ		2
A.13. SEGURIDAD DE LAS COMUNICACIONES				
A.13.1. Gestión de la Seguridad de la Red				
A.13.1.1. Controles de la red	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?	SÍ		2
A.13.1.2. Seguridad de los servicios de red	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?	SÍ		2
A.13.1.3. Segregación en redes	¿Existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos?	NO		0

A.13.2. Transferencia de información				
A.13.2.1. Políticas o procedimientos para la transferencia de información	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?	SÍ		3
A.13.2.2. Acuerdos de transferencia de información	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?	SÍ		2
A.13.2.3. Mensajes electrónicos	¿Se establecen normas o criterios de seguridad en mensajería electrónica?	NO		0
A.13.2.4. Acuerdos de confidencialidad o no divulgación	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades?	SÍ		2
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A.14.1. Requisitos de Seguridad en los Sistemas de Información				
A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información?	SÍ		3
A.14.1.2. Aseguramiento de servicios de aplicaciones sobre redes públicas	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?	SÍ		2
A.14.2. Seguridad en los procesos de desarrollo y soporte				

A.14.2.1. Política de desarrollo seguro	¿Se establecen procedimientos que garanticen el desarrollo seguro del software?	SÍ		3
A.14.2.2. Procedimientos de control de cambios del sistema	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?	SÍ		2
A.14.2.3. Revisión técnica de aplicaciones después de cambios a la plataforma operativa	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?	SÍ		2
A.14.2.4. Restricciones sobre cambios a los paquetes de software	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?	SÍ		2
A.14.2.5. Principios de ingeniería de sistemas seguros	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de sistemas?	SÍ		2
A.14.2.6. Ambiente de desarrollo seguro	¿Se cuenta con un entorno de desarrollo aislado de los analistas?	NO		0
A.14.2.7. Desarrollo de contratado externamente	¿Se realizan desarrollo de software por parte de terceros?	SÍ		1

A.14.2.8. Pruebas de seguridad del sistema	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?	SÍ		2
A.14.2.9. Pruebas de aceptación del sistema	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?	SÍ		2
A.14.3. Datos de Prueba				
A.14.3.1. Protección de datos de prueba	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?	SÍ		2
A.15. RELACIONES CON LOS PROVEEDORES				
A.15.1. Seguridad de la Información en las relaciones con los proveedores				
A.15.1.1. Política de seguridad de la información para las relaciones con los proveedores	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?	SÍ		2
A.15.1.2. Abordar la seguridad dentro de los acuerdos con proveedores	¿Se han establecido requisitos de seguridad de la información en contratos con terceros?	SÍ		2
A.16. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN				
A.16.1. Gestión de incidentes de la Seguridad de la Información y mejoras				
A.16.1.1. Responsabilidades y procedimientos	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?	SÍ		1
A.16.1.2. Reporte de eventos de seguridad de la información	¿Se han implementado canales adecuados para la comunicación de	SÍ		2

	incidentes en la seguridad de la Información?			
A.16.1.3. Reporte de debilidades de seguridad de la información	¿Se promueve y se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?	SÍ		2
¿Se promueve y se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?	SÍ		1
A.16.1.5. Respuesta de incidentes de seguridad de la información	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?	SÍ		2
A.16.1.6. Aprendizaje de los incidentes de la seguridad de información	¿La información que proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?	SÍ		2
A.16.1.7. Recolección de evidencias	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?	SÍ		1
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO				
A.1.7.1. Continuidad de Seguridad de la información				
A.17.1.1. Planificación de continuidad de seguridad de la información	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?	SÍ		2
A.17.1.2. Implementación de continuidad de seguridad de la información	¿Se ha implementado las medidas de recuperaciones previstas en el plan de Continuidad del Negocio?	SÍ		1

A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información	¿Se han verificado o probado las acciones previstas en el plan de continuidad del negocio?	NO		0
A.17.2. Redundancias				
A.17.2.1. Instalaciones de procesamiento de la información	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?	SÍ		3
A.18. CUMPLIMIENTO				
A.18.1. Cumplimiento con los Requisitos Legales y Contractuales				
A.18.1.1. Identificación de los requisitos contractuales y legislación aplicables	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento?	SÍ		3
A.18.1.2. Derechos de propiedad intelectual	¿Existen procedimientos implementados sobre la propiedad intelectual?	NO		0
A.18.1.3. Protección de registros	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?	SÍ		3
A.18.1.4. Privacidad y protección de datos personales	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	SÍ		2
A.18.1.5. Regulación de controles criptográficos	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?	SÍ		1
A.18.2.1. Revisión independiente de la Seguridad de la Información	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?	NO		0

A.18.2. Revisiones de seguridad de la información				
A.18.2.2. Cumplimiento de políticas y normas de seguridad	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?	SÍ		2
A.18.2.2. Cumplimiento de políticas y normas de seguridad	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?	SÍ		1

Nivel de Cumplimiento - Resultado por los Controles del anexo A de la NTP-ISO/IEC 27001:2014				
Anexo A NTP-ISO/IEC 27001:2014	Nivel de madurez	Nivel de cumplimiento		
		Real	Esperado	Brecha
A.5. Políticas de seguridad de información	2	67%	100%	33%
A.6. Organización de la seguridad de información	1.86	62%	100%	38%
A.7. Seguridad de los recursos humanos	2	67%	100%	33%
A.8. Gestión de activos	1.7	57%	100%	43%
A.9. Control de accesos	2.85714286	95%	100%	5%
A.10. Criptografía	1.5	50%	100%	50%
A.11. Seguridad física y del ambiente	3	100%	100%	0%
A.12. Seguridad de las operaciones	1.64285714	55%	100%	45%
A.13. Seguridad de las comunicaciones	1.42857143	48%	100%	52%
A.14. Adquisición, desarrollo y mantenimiento de sistemas	1.83333333	61%	100%	39%
A.15. Relaciones con los proveedores	1.5	50%	100%	50%

A.16. Gestión de incidentes de la seguridad de información	1.57142857	52%	100%	48%
A.17. Aspectos de seguridad de la información en la gestión de continuidad del negocio	1	33%	100%	67%
A.18. Cumplimiento	1	33%	100%	67%
Nivel de cumplimiento		59%	100%	41%

3.1.2. Etapa II: Propuesta del diseño de sistema de gestión de seguridad de la información

III.1.2.1. Objetivos del SGSI

- Dar protección a los sistemas de información a través de medidas de seguridad.
- Establecer políticas de respuestas frente a incidentes de seguridad de la información.
- Gestionar los recursos de seguridad de la información para que se use de manera adecuada los sistemas de información.
- Optimizar los procesos de los sistemas de información, respetando la seguridad de la misma.
- Controlar y gestionar el uso de usuarios para la NO vulneración de información.

III.1.2.2. Política general del sistema de gestión de seguridad de la información

III.1.2.2.1. Resumen

En la presente política se describe de forma general los estándares de seguridad mediante los cuales se deben manejar en la institución, tratamiento de los activos de información, roles y responsabilidades de la seguridad de información y las posibles sanciones a las que están expuestos por incumplimiento de las políticas de seguridad.

III.1.2.2.2. Objetivos

Establecer los roles adecuados para la gestión de la seguridad de información que permita proteger los activos de información de la organización y la tecnología utilizada para el procesamiento de la misma, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

III.1.2.2.3. Alcance

La siguiente política de seguridad de la información es aplicable a todos los trabajadores de la organización, este documento debe ser revisado y actualizado de manera periódica según se manifiesten cambios de infraestructura, nuevas tecnologías, nuevos servicios, entre otros.

- Compromiso Institucional

  Es compromiso de las Gerencias y Jefaturas establecer de manera clara el apoyo de la dirección, funcionamiento y cumplimiento de las Políticas de Seguridad de Información.

- Límites

  Las Políticas de Seguridad de Información, involucra a todos los sistemas y personas que tratan información de la organización. En general, se suele traducir en la implementación de políticas en la Oficina de Tecnología de Información, por ser uno de los principales responsables del tratamiento y conservación de la información.

III.1.2.2.4. Generalidades

- La Institución, reconoce que la seguridad de la información es un compromiso esencial en todos los procesos y colaboradores; por ello es necesario implementar mecanismos que permitan proteger los activos de información con la finalidad de gestionar eficientemente la

información asegurando la confidencialidad, disponibilidad e integridad.

- Los accesos y uso de información estarán alineadas a las normativas internas de la Organización.
- Las políticas deben ser difundidas a todos los colaboradores de la institución.
- Se promoverá la cultura de seguridad de la información en todos los colaboradores de la Organización.
- Los perfiles y roles de usuario deben ser autorizados.
- La información será clasificada según los siguientes niveles:

TIPO	GLOSA	DESCRIPCIÓN
C	Confidencial	Información de gran relevancia para la administración, se restringe el acceso a la misma.
R	Restringido	Accesible para determinados colaboradores según el desempeño de las funciones
UI	Uso interno	Accesible para todos los colaboradores de la administración
P	Público	Información de dominio público como la publicada en la página web

III.1.2.2.5. Responsabilidades

Las Políticas de Seguridad de Información son de aplicación para todo el personal de la organización.

III.1.2.2.6. Sanciones

La violación o incumplimiento de un control o política de seguridad de información justifica la aplicación de las sanciones comprendidas en el reglamento interno de la organización, las cuales serán aplicadas teniendo en consideración lo siguiente: gravedad de la falta, antecedentes

del colaborador, reincidencia y circunstancias en las que se cometió la falta u omisión de las políticas.

III.1.2.2.7. Políticas específicas

Las políticas específicas de seguridad de la información deben estar alineadas y soportadas bajo la política general del Sistema de Gestión de seguridad de Información, las cuales son las siguientes:

- Política para la gestión de usuarios.
- Política para el control de acceso físico.
- Política para la limpieza del puesto de trabajo.
- Política para la copia de seguridad.
- Política para el uso del servicio de Call Center y Mensajería.

III.1.2.2.8. Roles y responsabilidades para la Seguridad de la Información

Área / Dpto: Área Sistemas

Cargo: Asistente de Sistemas

Responsabilidades organizacionales:

- Coordinar y apoyar en las labores de auditoría y consultoría, administración de la información, diseño y desarrollo de software y mantenimiento e implementación de infraestructura tecnológica.
- Gestionar el diseño e implementación de proyectos correspondientes a la oficina de Sistemas.
- Responsable por la disponibilidad, desempeño, crecimiento y operación del hardware, software, acceso a recursos tecnológicos de toda la organización.

Área / Dpto: Telecomunicaciones

Cargo: Jefe de Telecomunicación

Responsabilidades organizacionales:

- Coordinar y apoyar en las labores de auditoría y consultoría, mantenimiento e implementación de infraestructura tecnológica tanto en uso y cambios de IP.
- Gestionar el diseño e implementación de proyectos correspondientes al Área de Telecomunicaciones.
- Responsable por la modificación, mantenimiento y operatividad de los IP que nos brindan para el uso correcto del sistema de la organización.

Área / Dpto: Call Center y Mensajería

Cargo: Jefe De Call Center

Responsabilidades organizacionales:

- Capacitar, coordinar y apoyar constantemente al personal del Área de call center para una atención adecuado a los clientes.
- Informar algún proyecto de implementación que se requiere en el Área.
- Responsable por la falta de capacitación a la persona y mal atención al cliente de toda la organización.

Área / Dpto: Limpieza

Cargo: Asistentes de aseo

Responsabilidades organizacionales:

- Limpiar y ordenar todas las instalaciones de la organización.
- Informar al área administrativa los requerimientos de aseo que se necesita para un mejor desempeño.

- Responsable por el desorden y algún accidente ocasionado por la falta de limpieza en los ambientes de la organización.

Área / Dpto: Administración

Cargo: Administradora

Responsabilidades organizacionales:

- Administrar, Capacitar, Coordinar y Supervisar a todo el personal que labora en la empresa.
- Informar a gerencia los problemas y las posibles soluciones por el bienestar de la organización.
- Responsable de cambios en el personal que administra.

3.1.3. Etapa III: Planificación del sistema de gestión de seguridad de la información

III.1.3.1. Identificación de activos

Los activos de información es todo aquello físico o virtual que genera valor para la organización, los cuales se detalla en la siguiente tabla:

TIPO DE ACTIVO		NOMBRE DEL ACTIVO	PROPIETARIO	USUARIO	VULNERABILIDAD	AMENAZA	CÓDIGO
PRIMARIOS	Procesos del negocio	Proceso de compras a proveedor	Administrador	Administrador Asistente administrativo	Procesos desactualizados desde 2020	Auditorías con resultados negativos	AM1
		Proceso facturación interna y externa	Jefe de Contabilidad	Asistentes contables			
		Proceso de instalaciones de cable e internet	Jefe de personal Técnico	Técnico	Reglamento de calidad de servicios de Telecomunicaciones desactualizado.	Sanciones impuestas por Osiptel	AM2
	Información	Documentos institucionales (PEI, RIT, MOF, ROF, otros)	Gerente General	Todos los empleados	Documentos expuestos sin seguridad física	Alteración de la información	AM3
		Documentos de gestión (Gestión de procesos, contratos, otros)	Gerente General	Personal nivel táctico	Falta de copias de respaldo	Procesos y procedimientos no claros	AM4
		Comprobantes, recibos	Gerente General	Asistentes contables	Perdida de comprobantes electrónicos	Sanciones impuestas por SUNAT	AM5

SOPORTE		Manuales de sistemas	Responsable de TI	Todos los empleados	Información descubierta	Difusión de información delicada o confidencial.	AM6
		Data de clientes, otros	Responsable de TI	Asistente de Sistemas			
	Hardware	Servidor	Responsable de TI	Personal de TI	Errores de configuración	Interrupción de los procesos del negocio	AM7
		Computadoras	Responsable de TI	Personal de oficinas	Falta de políticas de mantenimiento de escritorio	Mal funcionamiento de los ordenadores	AM8
		UPS	Responsable de TI	Personal de oficinas	Ninguno	Ninguno	
	Software	Firewall	Responsable de TI	Personal de Ti	Errores en los sistemas de autenticación	Acceso a redes internas de la empresa a conexiones IP que no son de confianza	AM9
		Base de datos	Responsable de TI	Asistente de Sistemas	Control inadecuado sobre los datos de entrada y salida	Revelación de Información, sobrecarga de datos.	AM10
		Antivirus	Responsable de TI	Personal de TI	No cuenta con parches de seguridad	Sistema expuesto a ataques, bloqueos de archivos e instalar malware	AM11

	Red	Sistema de cobros	Responsable de TI	Asistente de Sistemas	Manuales y antivirus desactualizados	Robo, alteración, destrucción de información,	AM12
		Router	Responsable de TI	Personal de TI	Contraseñas y credenciales de acceso deficientes - Tráfico de red y patrones de acceso no encriptado.	Robo de contraseñas, acceso a archivos restringidos o confidenciales	AM13
		Switch	Responsable de TI	Personal de TI			
		VPN	Responsable de TI	Personal de TI			
		Cableado	Responsable de TI	Personal de TI			
	Personal	Personal de Administrativo de la empresa	Jefe de Administración	Asistente administrativo	Falta de capacitación para actuar frente a situaciones de amenaza o sufrir daños	Interrupción de los procesos del negocio con poca capacidad de respuesta y solución.	AM14
		Personal de seguridad	Jefe de Administración	Personal de seguridad			
		Personal de mantenimiento	Jefe de Administración	Personal de mantenimiento			
		Personal de servicio técnico	Jefe de Administración	Personal técnico			

	Ambiente físico	Datacenter	Responsable de TI	Personal de TI	Falta de Capacitación al Personal	Información confidencial expuesta a terceros	AM15
		Callcenter	Responsable de TI	Personal de TI			
		Oficina de personal Contable	Jefe de Contabilidad	Asistentes contables	Pésimo control del acceso físico	Sabotaje en archivos y reportes, desastres naturales	AM16
		Oficinas de personal de administrativo	Jefe de Administración	Asistentes administrativos			

III.1.3.2. Clasificación de activos

TIPO DE ACTIVO		CÓDIGO	NOMBRE ACTIVO	CRITERIO DE CLASIFICACIÓN	DIMENSIÓN DEL ACTIVO			VALOR DEL ACTIVO	MAGNITUD DEL DAÑO	PROPIETARIO DEL ACTIVO		VALOR	MAGNITUD
					C	I	D			PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO		
PRIMARIOS	Procesos del negocio	A1	Proceso de compras a proveedor	R	5	5	5	5	4	Administrador	Administrador Asistente administrativo		
		A2	Proceso facturación interna y externa	R	5	5	5	5	3	Jefe de Contabilidad	Asistentes contables	5	4
		A3	Proceso de instalaciones de cable e internet	R	5	4	4	4	4	Jefe de personal Técnico	Técnico		
	Información	A4	Documentos institucionales (PEI, RIT, MOF, ROF , otros)	C	5	4	5	5	3	Gerente General	Todos los empleados	4	3

		A5	Documentos de gestión (Gestión de procesos, contratos, otros)	C	4	3	3	3	3	Gerente General	Personal nivel táctico		
		A6	Comprobantes, recibos	R	4	4	3	4	4	Gerente General	Asistentes contables		
		A7	Manuales de sistemas	R	3	5	3	4	2	Responsable de TI	Todos los empleados		
		A8	Data de clientes, otros	R	5	5	5	5	3	Responsable de TI	Asistente de Sistemas		
	Hardware	A9	Servidor	R	5	4	5	5	4	Responsable de TI	Personal de TI		
		A10	Computadoras	UI	3	4	4	4	3	Responsable de TI	Personal de oficinas	4	3
		A11	UPS	UI	4	4	4	4	2	Responsable de TI	Personal de oficinas		
	Software	A12	Firewall	R	4	4	4	4	3	Responsable de TI	Personal de Ti		
		A13	Base de datos	R	5	5	5	5	4	Responsable de TI	Asistente de Sistemas		
SOPORTE		A14	Antivirus	UI	4	4	3	4	3	Responsable de TI	Personal de TI	4	3.50
		A15	Sistema de cobros	R	5	4	4	4	4	Responsable de TI	Asistente de Sistemas		
	Red	A16	Router	UI	4	4	4	4	3	Responsable de TI	Personal de TI	4	3.2

Personal	A17	Switch	UI	4	3	4	4	3	Responsable de TI	Personal de TI		
	A18	VPN	UI	3	3	3	3	4	Responsable de TI	Personal de TI		
	A19	Cableado	P	4	4	4	4	3	Responsable de TI	Personal de TI		
	A20	Personal de Administrativo de la empresa	P	5	4	4	4	3	Jefe de Administración	Asistente administrativo		
	A21	Personal de seguridad	UI	4	5	5	5	3	Jefe de Administración	Personal de seguridad	5	3.333333333
	A22	Personal de mantenimiento	P	4	5	4	4	3	Jefe de Administración	Personal de mantenimiento		
	A23	Personal de servicio técnico	P	5	4	5	5	4	Jefe de Administración	Personal técnico		
Ambiente físico	A24	Datacenter	R	5	5	5	5	3	Responsable de TI	Personal de TI	5	3.5
	A25	Callcenter	R	5	5	4	5	3	Responsable de TI	Personal de TI		
	A26	Oficina de personal Contable	R	4	5	4	4	4	Jefe de Contabilidad	Asistentes contables		
	A27	Oficinas de personal de administrativo	R	5	4	4	4	4	Jefe de Administración	Asistentes administrativos		

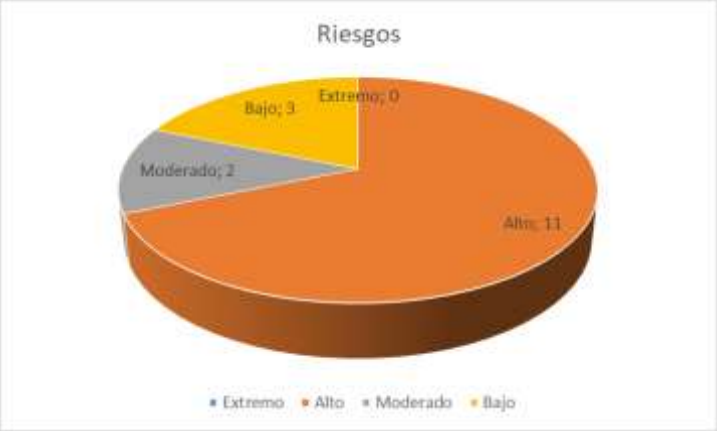
III.1.3.3. Gestión de riesgos

III.1.3.3.1. Evaluación de riesgos

RIESGO Y AMENAZA			IMPACTO DEL RIESGO																										Valorización del riesgo	Nivel de Riesgo
			Procesos del Negocio			Información					Hardware			Software				Red				Personal				Ambiente físico					
			A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27		
Riesgos	Amenaza	Probabilidad	4	4	5	3	3	5	3	3	4	3	2	1	4	2	4	2	2	3	2	3	3	3	2	4	3	4	4		
Pérdida de la información de la entidad	AM1	2	8	8	10	6	6	10	6	6	8	6	4	2	8	4	8	4	4	6	4	6	6	6	4	8	6	8	8	6.30	Moderado
	AM2	1	4	4	5	3	3	5	3	3	4	3	2	1	4	2	4	2	2	3	2	3	3	3	2	4	3	4	4	3.15	Bajo
	AM3	3	12	12	15	9	9	15	9	9	12	9	6	3	12	6	12	6	6	9	6	9	9	9	6	12	9	12	12	9.44	Alto
	AM4	3	12	12	15	9	9	15	9	9	12	9	6	3	12	6	12	6	6	9	6	9	9	9	6	12	9	12	12	9.44	Alto
	AM5	1	4	4	5	3	3	5	3	3	4	3	2	1	4	2	4	2	2	3	2	3	3	3	2	4	3	4	4	3.15	Bajo
	AM6	3	12	12	15	9	9	15	9	9	12	9	6	3	12	6	12	6	6	9	6	9	9	9	6	12	9	12	12	9.44	Alto
Indisponibilidad de la información	AM7	3	12	12	15	9	9	15	9	9	12	9	6	3	12	6	12	6	6	9	6	9	9	9	6	12	9	12	12	9.44	Alto
	AM8	4	16	16	20	12	12	20	12	12	16	12	8	4	16	8	16	8	8	12	8	12	12	12	8	16	12	16	16	12.59	Alto
	AM9	4	16	16	20	12	12	20	12	12	16	12	8	4	16	8	16	8	8	12	8	12	12	12	8	16	12	16	16	12.59	Alto
	AM10	4	16	16	20	12	12	20	12	12	16	12	8	4	16	8	16	8	8	12	8	12	12	12	8	16	12	16	16	12.59	Alto
	AM11	2	8	8	10	6	6	10	6	6	8	6	4	2	8	4	8	4	4	6	4	6	6	6	4	8	6	8	8	6.30	Moderado
	AM12	3	12	12	15	9	9	15	9	9	12	9	6	3	12	6	12	6	6	9	6	9	9	9	6	12	9	12	12	9.44	Alto
Fallas de seguridad por personal humano	AM13	3	12	12	15	9	9	15	9	9	12	9	6	3	12	6	12	6	6	9	6	9	9	9	6	12	9	12	12	9.44	Alto
	AM14	4	16	16	20	12	12	20	12	12	16	12	8	4	16	8	16	8	8	12	8	12	12	12	8	16	12	16	16	12.59	Alto
	AM15	3	12	12	15	9	9	15	9	9	12	9	6	3	12	6	12	6	6	9	6	9	9	9	6	12	9	12	12	9.44	Alto
	AM16	1	4	4	5	3	3	5	3	3	4	3	2	1	4	2	4	2	2	3	2	3	3	3	2	4	3	4	4	3.15	Bajo

Resumen

Nivel de riesgo	Riesgos
Extremo	0
Alto	11
Moderado	2
Bajo	3



III.1.3.3.2. Plan de tratamiento de riesgos

RIESGO	CODIGO AMENAZA	AMENAZA	NIVEL RIESGO	TRATAMIENTO	REFERENCIA NTP ISO 27001:2014 ANEXO A	ACTIVIDADES	RECURSO	RESPONSABLE	FECHA DE IMPLEMENTACIÓN
PÉRDIDA DE LA INFORMACIÓN DE LA ENTIDAD	AM1	Auditorías con resultados negativos	Moderado	Evitar riesgo	12.1.1 Documentación de procedimientos de operación	Revisar y realizar actualizaciones periódicas (1 ó 2 años) de los documentos de procesos	Gestión de los procesos	Gerente General	6/01/2023
	AM2	Sanciones impuestas por DIGESA	Bajo	Evitar riesgo	18.1.1 Identificación de la legislación aplicable	Revisar los cambios en las legislaciones para su posterior aplicación	Informes, documentos legales	Administrador	3/01/2023
	AM3	Alteración de la información	Alto	Evitar riesgo	8.2.1. Clasificación de la Información	Realizar clasificación de información según el valor para la institución	Documentos de clasificación de Información	Gerente General	10/02/2023
						Realizar procedimientos de seguridad de información	Charlas y cursos orientados a la seguridad		

						según cada grupo de clasificación	de la información		
					7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	Brindar capacitación y educación sobre la conciencia de la seguridad de la información			
					9.4.1. Restricción de acceso a la información	Establecer una política de acceso a la información que se determine por grados y responsabilidades			
	AM4	Procesos y procedimientos no claros	Alto	Mitigar riesgo	12.1.1 Documentación de procedimientos de operación	Realizar y salvaguardar copias de seguridad en entornos confiables			3/01/2023
	AM5	Sanciones impuestas por SUNAT	Bajo	Mitigar riesgo	18.1.1 Identificación de la legislación aplicable	Verificar los cambios en las legislaciones para su posterior aplicación	Documentos legales, documentación de la gestión de sanciones		

	AM6	Difusión de información delicada o confidencial.	Alto	Evitar riesgo	9.4.1. Restricción de acceso a la información	Realizar acuerdos de confidencialidad de información de la Empresa	Políticas de confidencialidad		10/01/2023
INDISPONIBILIDAD DE LA INFORMACIÓN	AM7	Interrupción de los procesos del negocio	Alto	Mitigar riesgo	12.1.1 Documentación de procedimientos de operación	Revisar y realizar actualizaciones periódicas (1 o 2 años) de los documentos de procesos	Documentación de la gestión de los procesos	Responsable de TI	18-01-20203
	AM8	Mal funcionamiento de los ordenadores	Alto	Evitar riesgo	11.2.4 Mantenimiento de Equipos	Inspeccionar el estado de cada equipo para poder analizar su tiempo de vida	Normas de limpieza, utensilios de limpieza, regular temperatura ambiente		
					11.2.9 Políticas de escritorio limpio	Establecer una política del cuidado del equipo y su entorno			
	AM9	Acceso a redes internas de la empresa a conexiones IP que no son de confianza	Alto	Mitigar riesgo	9.1.2 Acceso a Rede y servicios de Red	Verificar el acceso a la Red interna con direcciones ip de confianza	Listas de Ip seguras		
					13.1.2 Seguridad de Servicios de Red	Identificar acuerdos de servicios de red,	Acuerdos y contratos de acuerdo a los		13/01/2023

						ya sean internas o sean tercerizadas	servicios de red	
	AM10	Revelación de Información, sobrecarga de datos.	Alto	Mitigar riesgo	13.2.2 Acuerdo sobre transferencia de información	Verificar que la transferencia de información entre la organización y partes externas sea segura	Guías de las transferencias de información realizadas	
	AM11	Sistema expuesto a ataques, bloqueos de archivos e instalar malware	Moderado	Evitar riesgo	12.2.1 Controles contra códigos maliciosos	Implementar controles de detección, prevención y recuperación contra códigos maliciosos	Documentos de Gestión de controles	10/01/2023
	AM12	Robo, alteración, destrucción de información,	Alto	Evitar riesgo	9.2.3 Gestión de derechos de acceso privilegiado	Restringir y controlar el uso de derechos de acceso privilegiado		
FALLAS DE SEGURIDAD POR PERSONAL HUMANO	AM13	Robo de contraseñas, acceso a archivos restringidos o confidenciales	Alto	Evitar riesgo	9.2.4 Gestión de información de autenticación secreta de usuarios	Controlar la asignación de información de autentificación	Documentos de gestión de la entrega de autentificación y roles de usuario	3/01/2023

		Interrupción de los procesos del negocio con poca capacidad de respuesta y solución.	Alto	Mitigar riesgo	16.1.1 Responsabilidades y procedimientos	Establecer las responsabilidades y los procedimientos para asegurar respuesta rápida, efectiva y ordenada	Guía de responsabilidades y procedimientos asignados		6/01/2023
	AM14				12.1.1 Documentación de procedimientos de operación	Revisar y realizar actualizaciones periódicas (1 ó 2 años) de los documentos de procesos	Documentos de gestión de Procesos	Gerente General	10/01/2023
	AM15	Información confidencial expuesta a terceros	Alto	Evitar riesgo	13.2.4 Acuerdos de confidencialidad o no divulgación	Documentar los acuerdos de confidencialidad para la protección de la información	Políticas de confidencialidad		
	AM16	Sabotaje en archivos y reportes, desastres naturales	Bajo	Mitigar riesgo	11.1.3 Asegurar oficinas, áreas e instalaciones	Implementar un diseño de seguridad física para las oficinas	Utilizar candados, implementar zonas seguras	Jefe de Seguridad	2/01/2023
					11.1.4 Protección contra amenazas externas y ambientales	Diseñar protección física para desastres naturales, accidente o			

	ataques maliciosos

III.1.3.4. Establecer políticas y procedimientos para controlar riesgos

III.1.3.4.1. Política para la gestión de usuarios

Objetivo

Establecer estándares para la gestión de cuentas de usuarios que involucra la creación, modificación y bajas de cuentas de usuarios de acuerdo al nivel de acceso de cada usuario.

Alcance

Esta política abarca a todos los usuarios que necesiten tener acceso al Sistema de la organización.

Política

Creación de cuentas de usuario

- El área administrativa deberá informar al Área de sistemas los nuevos ingresos del personal nuevo que tendrá acceso a algún sistema informático de acuerdo al perfil de sus respectivas funciones.
- El área de Sistemas deberá confirmar al área Administrativa la creación exitosa del nuevo usuario.

Modificación de cuentas de usuario

- El área administrativa deberá informar al Área de sistemas las modificaciones del usuario y brindarle perfiles de acuerdo a las funciones que necesita el usuario dentro del sistema.
- El área de Sistemas deberá confirmar al área Administrativa la realización exitosa de la operación.

Bajas de cuentas de usuario

- El área administrativa deberá informar al Área de sistemas la no continuidad de un personal que tenga acceso al sistema de la organización, para así proceder a bloquear o eliminar sus cuentas de los usuarios

- El área de Sistemas deberá confirmar al área Administrativa la realización exitosa de la operación.

Sanciones

Cada usuario es responsable de la administración de la cuenta asignada, ya sea el cambio de contraseña o la divulgación de la misma, bajo responsabilidad de acuerdo a la confidencialidad de la organización, esto requiere una suspensión o bloqueo del usuario para no ingresar al sistema.

III.1.3.4.2. Política de control de acceso físico

Objetivo

Prevenir e impedir accesos no autorizados a los ambientes de vulnerabilidad de la organización.

Con ello buscamos proteger los equipos o documentos importantes de la organización para reducir los riesgos ocasionados por amenazas y vulnerabilidades de acceso no autorizado.

Alcance

Esta política abarca a todo el personal de la organización.

Política

Perímetro de seguridad física

- Verificar accesos del personal al Edificio. Para ello se utiliza el reconocimiento Facial y huella dactilar.
- Verificar accesos al Data Center y ambientes vulnerables.
- Mantener al personal de seguridad y personal de aseo actualizado sobre las normativas de seguridad, las políticas de control de acceso y las personas que puedan acceder.

Control de acceso físico

- Supervisar o inspeccionar a los visitantes a áreas protegidas, registrar el motivo de la visita, también la fecha y hora de su ingreso y salida.
- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas NO autorizadas.

Respecto al cableado:

- Proteger el cableado de red contra daño.
- Separar los cables de energía de los cables de comunicaciones para evitar interferencias y así evitar una caída o corte en nuestro Data Center.

Sanciones

- Suspender el acceso durante una semana.
- De ser reincidente se procederá a realizar el descuento según el daño ocasionado, caso contrario se despedirá de la persona.

III.1.3.4.3. Política de limpieza del puesto de trabajo

Objetivo

Para poder realizar alguna actividad laboral debemos garantizar, mantener el orden, la limpieza y el acondicionamiento de todas las instalaciones y ambientes para evitar cualquier daño y accidentes dentro de la organización.

Alcance

Esta política abarca a todas las oficinas y ambientes de trabajo de la organización.

Política

Orden

Tiene como finalidad mantener ordenado los ambientes de todas las áreas de la organización, para evitar cualquier daño o accidente.

Limpieza

Tiene como finalidad mantener limpio todo el edificio de la organización, ello nos mantendrá seguros y Así evitamos golpes y accidentes.

Acondicionamiento

Tiene como finalidad mantener acondicionado todos los ambientes para así poder desempeñarnos de una mejor manera en el trabajo.

Sanciones

- Llamada de atención por parte Administrativa.
- De suceder reiteradas veces, despido del personal de limpieza.

III.1.3.4.4. Política de copia de seguridad

Objetivo

Realizar y verificar las copias de seguridad (Backup) que garantizan la continuidad del proceso de negocio de la organización.

Alcance

Esta política abarca a todo el Área de Sistemas.

Política

Resguardo de la información:

- Almacenar en una ubicación remota y en un disco extraíble las copias de seguridad que se realizan diariamente.

- Verificar y probar periódicamente la restauración de las copias de seguridad garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.
- Cifrado de la información con la finalidad de proteger los datos en caso de robo de información o acceso no autorizado.

Sanciones

Amonestación a la persona encargada de realizar el backup de la BD de la organización.

III.1.3.4.5. Política de uso de servicio de Call center y mensajería

Objetivo

Establecer estándares para la gestión de uso correcto de Call center y Mensajería masiva a los abonados de la organización.

Alcance

Esta política abarca al Área de Sistemas y Área de Call Center.

Política

Capacitación al personal de Call center

- El área administrativa y el área de sistemas capacita periódicamente a las personas de Call center para atender y brindar una mejor atención a los abonados.
- Informar al gerente la realización con éxito de la capacitación.

Mensajería Masiva

- El área administrativa debe informar al área de sistemas el día y el contendido que se envía en los mensajes masivos a los abonados.

- El área de sistemas informa al área administrativa la realización con éxito del envío masivo de los mensajes.

Sanciones

- Amonestación a las personas que brinden un servicio pésimo en el área de calla center.
- Si el problema permanece reiteradas veces, se despide al personal.

CAPÍTULO IV: DISCUSIÓN

- En base al análisis realizado de la situación actual de la organización realizado el análisis de brechas de los 7 requisitos de la NTP-ISO/IEC 27001:2014 se ha obtenido el nivel de cumplimiento de 1 que corresponde al nivel inicial en donde el control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe; es decir solo se cumple con el 19% de los requisitos mínimos necesarios para llevar a cabo el desarrollo del Sistema de Gestión de Seguridad de Información, mientras que la brecha existente del 81% correspondes a procesos inexistentes o aquellos procesos que no se encuentran documentados.
- También se realizó el análisis de los 14 dominios, 35 objetivos de control y 114 controles establecidos en el anexo A de la misma norma se ha obtenido el nivel de cumplimiento del 0.78 que corresponde al nivel inicial en donde el control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe; es decir solo el 41% de los controles se están ejecutando sin embargo no se encuentran documentados o no se soportan en una política documentada, aprobada y de conocimiento a los colaboradores de la institución; mientras que la brecha existente del 59% corresponden a aquellos controles que no se evidencian en la institución además de, aquellos que por la naturaleza de la misma no se aplican.
- El análisis de brechas ha logrado determinar que la situación actual de la institución en cuanto a los temas de seguridad de la información se encuentra en nivel inicial en donde el control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe; con respecto al nivel mínimo aceptable el 3 definido, en donde los procedimientos se han estandarizado y documentado, y se han difundido a través del entrenamiento.

CAPÍTULO V: CONCLUSIONES

- Se evaluó el proceso de gestión de riesgos de la organización donde se identificaron los activos, vulnerabilidades y amenazas que ayudaron a determinar el nivel de riesgo a los que se encuentran expuestos demostrando que existe un 27% de nivel de riesgo extremo, 51% de nivel de riesgo alto y el 22% de nivel de riesgo moderado; riesgos de seguridad de información que afectan los activos de información de la institución.
- Se realizó la selección de objetivos y objetivos de control de la seguridad de información establecidos en el Anexo A de la NTP-ISO/IEC 27001:2014, mediante la declaración de aplicabilidad.

CAPÍTULO V: RECOMENDACIONES

- Implementar un Sistema de Gestión de Seguridad de la Información para proteger los activos de información de la organización, teniendo y coordinando un control adecuado con la planificación de los incidentes que puedan amenazar la seguridad de información, y con esto preservar la confidencialidad, integridad y disponibilidad de la misma.
- Contar con un proceso que gestione los riesgos asociados a las amenazas que se presentan en la organización para determinar la acción sobre los riesgos que serán tratados mediante la aplicación de controles con la finalidad de evitar y mitigar la ocurrencia de los mismos.

IV. REFERENCIAS BIBLIOGRÁFICAS

Bermudez, K.;Bailón, E. (2015). Analisis De Seguridad Informática Y Seguridad De La Información Basado En La Norma ISO/IEC 27001 - Sistema De Gestión De Seguridad De Seguridad De La Información Dirigido A Una Empresa De Servicios Financieros.

COBIT, M. d. (2021). Modelo de Madurez COBIT. Obtenido de COBIT: https://rincontic.org/2020/04/30/modelo-de-madurez-cobit/

Firma-e. (Octubre de 2014). Pilares de la Seguridad de Información. (F.-e. C. TI, Editor) Recuperado el de de 2017, de Seguridad de Informacion: https://www.firmae.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-ydisponibilidad/

Fonseca Herrera, O. (2019). “Modelo de un Sistema de Gestión de Seguridad de la Información en la organización GEOCONSULT cs”. Bogota.

Incibe. (2017). Incibe. Obtenido de Incibe: https://www.incibe.es/en/node/2789

Komisarczuk, P. (2020). An introduction to knowledge areas in Information Security - Introduction to Information Security. Retrieved June 04, 2020, from https://www.coursera.org/learn/information-security-data/lecture/7mqjI/anintroduction-to-knowledge-areas-in-information-security

NTP-ISO/IEC27001:2014. (2014). Information technology - Security techniques – Information security management systems - Requirements. Lima.

NTP-ISO/IEC27001-2014. (2014). TECNOLOGIA DE INFORMACION. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Lima.

ONGEI. (2017). UN GOBIERNO ELECTRONICO. Obtenido de UN GOBIERNO ELECTRONICO: http://gobiernoelectronicope.blogspot.com/2013/07/que-es-el-ongei.html

Sandoval, J. (2017). Diseño de un Plan De Seguridad de la Informacion para el Centro De Informatica Y Telecomunicaciones de la Universidad Nacional De Piura, periodo 2015-

2018. (Para optar el Título de Ingeniero Informático). Universidad Nacional de Piura, Piura. Obtenido de http://repositorio.unp.edu.pe/bitstream/handle/UNP/1165/INDSAN-QUI-17.pdf?sequence=1&isAllowed=y

Sampieri, R. H. (1998). Metodologia de la Invesitgación - Cuarta Edición

Trespalacios, J., Bello, L. y Vásquez, R. (1994). Investigación de mercados: métodos de recogida y análisis de la información para la toma de decisiones. Paraninfo.