UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

FACULTAD DE INGENIERÍA

ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

T E S I S

Diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021

Para optar el título profesional de:

Ingeniero de sistemas y Computación

Autor:

Bach. Joel Jaime RAMIREZ PARRA

Asesor:

Ing. Melquiades Arturo TRINIDAD MALPARTIDA

Cerro de Pasco – Perú – 2022

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

FACULTAD DE INGENIERÍA

ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

T E S I S

Diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021

Sustentada y aprobada ante los miembros del jurado:

Mg. Teodoro ALVARADO RIVERA	**Mg. Oscar CAMPOS SALVATIERRA**
PRESIDENTE	**MIEMBRO**

Mg. Pit Frank ALANIA RICALDI
MIEMBRO

Universidad Nacional Daniel Alcides Carrión

Facultad de Ingeniería

Unidad de Investigación

INFORME DE ORIGINALIDAD N° 160-2023-UNDAC/UIFI

La Unidad de Investigación de la Facultad de Ingeniería de la Universidad Nacional Daniel Alcides Carrión en mérito al artículo 23° del Reglamento General de Grados Académicos y Títulos Profesionales aprobado en Consejo Universitario del 21 de abril del 2022, La Tesis ha sido evaluado por el software antiplagio Turnitin Similarity, que a continuación se detalla:

Tesis:

Diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021

Apellidos y nombres del tesista

Bach. RAMIREZ PARRA, Joel Jaime

Escuela de Formación Profesional

Ingeniería de Sistemas y Computación

Apellidos y nombres del Asesor

Ing. TRINIDAD MALPARTIDA, Melquiades Arturo

Indice de Similitud

8 %

APROBADO

Se informa el Reporte de evaluación del software similitud para los fines pertinentes:

Cerro de Pasco, 8 de noviembre del 2023

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN
FACULTAD DE INGENIERÍA
UNIDAD DE INVESTIGACIÓN

Luis Vilar Requis Carbajal
DOCTOR EN CIENCIAS - DIRECTOR

DEDICATORIA

El presente trabajo de investigación está dedicada a mi familia, quienes me apoyan en cada decisión, objetivo y paso de mi vida.

AGRADECIMIENTO

A los diversos repositorios institucionales nacional e internacionales que aportaron intelectualmente a la presente investigación.

Al Gobierno Regional Pasco, por abrirme las puertas de su institución y recibir el apoyo para que la presente investigación se haga realidad.

A mi alma mater, por todos los conocimientos impartidos en el trayecto de mi vida universitaria; a mis docentes por cada una de sus enseñanzas, a mi asesor por encaminar teórica y metodológicamente la presente investigación.

RESUMEN

El Gobierno Regional Pasco tiene la determinación de proteger la seguridad de la información de sus activos de información, es por ello que determino como objetivo principal a “Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco – 2021”. Con la finalidad de llegar al objetivo se realizó la implementación del SGSI basada en la metodología PHVA, dentro de ellas y como mención de las principales actividades se realizó el análisis de brechas, gestión de riesgos y medición del SGSI. Es por ello que la presente investigación es de tipo aplicada con el nivel de investigación descriptivo, del mismo modo también se basó en el método de investigación inductivo – deductivo y el diseño corresponde al cuasi experimento; la población está conformada por todos los funcionarios públicos que laboran en la SG de racionalización y sistemas TIC del Gobierno Regional Pasco y como muestra fueron considerado la totalidad de la población los cuales son 12 funcionario optando por un muestreo de tipo censal. Y como conclusión podemos resaltar que el SGSI permitió la mejora de la seguridad de la información debido a que se alcanzaron los niveles esperados para cada control de la NTP ISO/IEC 27001:2014.

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

ABSTRACT

The Pasco Regional Government is determined to protect the information security of its information assets, which is why it determined as its main objective to "Design an information security management system based on the NTP ISO / IEC 27001: 2014 to mitigate the risks of the pillars of information security in the Deputy Management of Rationalization and ICT Systems of the Pasco Regional Government - 2021". In order to reach the objective, the implementation of the ISMS was carried out based on the PHVA methodology, within them and as a mention of the main activities, the analysis of gaps, risk management and measurement of the ISMS was carried out. That is why the present investigation is of an applied type with the level of descriptive investigation, in the same way it was also based on the inductive - deductive research method and the design corresponds to the quasi-experiment; The population is made up of all public officials who work in the SG for rationalization and ICT systems of the Pasco Regional Government and as a sample the entire population was considered, which are 12 officials, opting for a census-type sampling. And in conclusion, we can highlight that the ISMS allowed the improvement of information security because the expected levels were reached for each control of the NTP ISO/IEC 27001:2014.

Keywords: NTP ISO/IEC 27001:2014, Information Security Management System.

INTRODUCCIÓN

En la actualidad las organizaciones vienen siendo participes de la transformación digital la misma que ayuda a tener ventajas competitivas con respecto a las demás. Las organizaciones apoyan gran parte de sus procesos en tecnologías de información y comunicación; pero estas oportunidades vienen acompañadas de amenazas que pueden presentar riesgos contra los activos de información de las organizaciones. Con la finalidad de contrarrestar a los problemas que atentan con los activos de seguridad de la información de las organizaciones se han creado distintos estándares, normas y regulación con respecto a la seguridad de la información una de ellas es el ISO 27001 el mismo que establece buenas prácticas, una estructura consistente y controles con la finalidad de tener una organización más segura.

El Gobierno Regional Pasco, con la finalidad de asegurar sus activos de información se plantea como objetivo “Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco – 2021” con la finalidad de asegurar la confidencialidad, disponibilidad e integridad de sus activos de información, es por ello la razón de ser de la presente investigación.

La presente investigación conta de 4 capítulos los mismos que se estructuran de la siguiente manera:

Capítulo I, en el mismo que se presenta el problema de investigación con los siguientes apartados: identificación y determinación, delimitación de la investigación, formulación del problema, formulación de objetivos, justificación de la investigación y limitaciones.

Capitulo II, El mismo que presenta el marco teórico con los siguientes apartados: antecedentes de estudio, bases teóricas – científicas, definición de términos básicos, formulación de hipótesis, identificación de variables y definición operacional de las variables e indicadores.

Capitulo III, el mismo que presenta la metodología y técnicas de investigación contando con los siguientes apartados: tipo de investigación; nivel de investigación; métodos de investigación; diseño de investigación; población y muestra; técnicas e instrumentos de recolección de datos; selección, validación, y confiabilidad de los instrumentos de investigación; tratamiento estadístico; orientación ética, filosófica y epistémica.

Capitulo IV, en el mismo que se presenta los resultados y discusión el mismo que consta de: descripción del trabajo de campo; presentación, análisis e interpretación de resultados; prueba de hipótesis; y discusión de resultados.

Por último, se presentan las conclusiones, recomendaciones, referencias bibliográficas y anexos.

El Autor.

ÍNDICE

CAPÍTULO III

METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

ÍNDICE DE TABLAS

ÍNDICE DE FÍGURAS

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. Identificación y determinación del problema

En la actualidad se vive una nueva era considerada como la cuarta revolución industrial la cual hace su enfoque al desarrollo tecnológico y su capacidad de integrar a las sociedades superando todo tipo de barreras y haciendo con el objetivo de formar sociedades justas e inclusivas; esta revolución incluye dentro de sus beneficios el uso de tecnología, el uso de los datos, internet de las cosas, computación en la nube, entre otras. Es por ello que toda organización no es ajena a este desarrollo o revolución y también vienen apoyando sus actividades, procesos internos y externos con el uso de tecnologías innovadoras tales como: sistemas de información, aplicaciones móviles, aplicaciones web, entre otros. Los cuales les permiten a las organizaciones a agilizar sus procesos con la finalidad de obtener mejores resultados en cuestión de los beneficios a los cuales están enfocados.

El sector público tiene como objetivo principal que todos sus procesos estén enfocados al desarrollo de la sociedad, búsqueda de mejorar la calidad de vida en bien de su población, es por ello que la gran mayoría de las instituciones

públicas vienen haciendo uso de herramientas tecnológicas para lograr sus objetivos. Estos procesos conllevan a una gran generación de datos los cuales son de vital importancia para el desarrollo sin interrupciones de sus actividades.

El Gobierno Regional Pasco, dentro de sus instalaciones cuenta con sistemas de información los cuales ayudan a la institución a encaminar con mayor eficiencia sus procesos, los sistemas pueden estar enfocados para la gestión documentaria o gestión económica, es por ello que la institución depende en gran medida de ellos para el correcto funcionamiento de sus procesos. Es por ello que nace la necesidad de gestionar la seguridad de la información debido a la valía de los datos generados a partir de todos los procesos y sean manuales o apoyadas en el uso de tecnología. Todo ello con la finalidad de mitigar posibles incidencias de seguridad informática, esto visto con el incremento sustancial de atacantes, software malicioso, técnicas y otros que vulneran la información dentro de las entidades. También es conocido que el Gobierno Central, mediante la Presidencia de Consejo de ministros obliga a toda entidad pública a diseñar su sistema de gestión de seguridad de la información mediante el uso de la NTP ISO/IEC 27001:2014.

1.2. Delimitación de la investigación

1.2.1. Delimitación espacial

Se tomó como delimitación espacial a la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco, el mismo que se ubica en la sede central de la institución en mención; distrito Yanacancha, provincia y departamento Pasco.

1.2.2. Delimitación temporal

La presente investigación tiene como delimitación temporal a todos los procesos y requerimientos funcionales para la implementación del SGSI los cuales fueron tomados en el año 2021.

1.2.3. Delimitación de universo

La presente tiene como universo a todos los procesos relacionados con la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco.

1.2.4. Delimitación de contenido

La investigación presente tiene como contenido al diseño de un sistema de gestión de seguridad de la información la misma que está basada en la NTP ISO/IEC 27001:2014.

1.3. Formulación del problema

1.3.1. Problema general

¿De qué manera el diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021?

1.3.2. Problemas específicos

- ¿De qué manera el diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la confidencialidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021?
- ¿De qué manera el diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la integridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021?
- ¿De qué manera el diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los

riesgos de la disponibilidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021?

1.4. Formulación de objetivos

1.4.1. Objetivo general

Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.

1.4.2. Objetivos específicos

- Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de la confidencialidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.
- Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de la integridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.
- Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar de la disponibilidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.

1.5. Justificación de la investigación

1.5.1. Justificación científica

La presente influye en gran medida en demostrar la valía de la protección de la información debido a que ella tiene un gran valor dentro de las organizaciones; una organización que no hace uso de sus datos, es una organización que no tiene rumbo; sin embargo, una organización que hace uso de la información generada por sus procesos internos, conlleva a una ventaja competitiva sobre sus competidores. Es por ello que al saber de la importancia de los datos se pretende mitigar posibles riesgos con el uso de la NTP ISO/IEC 27001:2014 con la finalidad de dar a conocer a la comunidad científica la importancia del uso de la mencionada Norma Técnica Peruana.

1.5.2. Justificación económica.

Día a día grandes organizaciones vienen siendo objetivos de personas maliciosas que atacan mediante el uso de técnicas, herramientas, software, entre otros con la finalidad de perjudicar a una organización y posteriormente pedir recompensas económicas para poder ser liberados de los ataques cibernéticos, es por ello que la presente pretende la prevención de estos posibles ataques haciendo uso de la NTP ISO/IEC 27001:2014 con la finalidad de que la organización ante cualquier posible ataque siga en funcionamiento sin detener los procesos internos de la organización.

1.6. Limitaciones de la investigación.

- Recursos económicos insuficientes para la recopilación de requerimientos, información y validación de la investigación.
- El cambio drástico del modo de trabajo dentro de la institución debido a la pandemia a causa del COVID-19.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de estudio

2.1.1. Antecedentes internacionales

- En la investigación denominada “Diseño del sistema de gestión de seguridad de la información para los procesos de gestión de información, gestión de recursos físicos y gestión humana de la empresa acceso directo asociados limitada, basado en la norma ISO 27001:2014” Giraldo & Villalobos (2017) nos mencionan que:

  El diseño de un sistema de gestión de seguridad de la información permitió a los autores del proyecto identificar los riesgos existentes en la empresa Acceso Directo Asociados Limitada, los cuales exponen los activos de información a algún tipo de vulnerabilidad o exposición a algún agente interno o externo que afecte su integridad, disponibilidad y confidencialidad; y realizar una clasificación de estos de acuerdo a valores dados a los riesgos, estableciendo así que los riesgos potencialmente peligrosos están clasificados como extremos, altos y moderados, los cuales deben ser analizados, evaluados y controlados hasta llevarlos a un nivel aceptable donde se vea una relación coherente costo-beneficio (pág.128).

- En la investigación denominada “Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2014” Nieves (2017) nos menciona que:

  El diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), permitirá identificar amenazas y vulnerabilidades de los activos de información, para posteriormente elaborar plan de tratamientos con la finalidad de mitigar los riesgos (pág.34).

- En la investigación denominada “Diseño de un sistema de gestión de seguridad de la información ajustado a las necesidades de la corporación médica Clínica Vida de Quibdó” Guardia (2017) nos menciona que:

  Se logró Identificar el estado actual de la Clínica Vida en materia de Gestión de Seguridad de la Información, permitiendo diseñar una propuesta de implementación del Sistema de Gestión de Seguridad de la Información ajustada a los hallazgos detectadas en el diagnóstico previamente realizado, obteniendo todos los pormenores necesarios del área de infraestructura de la Clínica para ubicar y valorar los riesgos y vulnerabilidades, construyendo un modelo basado en las necesidades reales (pág.52)

2.1.2. Antecedentes nacionales

- En la investigación denominada “Diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2013 para una empresa de producción y comercialización de productos de consumo masivo” Cajusol (2020) nos menciona que:

  Se determinó durante el desarrollo del análisis de riesgos, que el 31% de activos de información tienen un Nivel de Riesgo Crítico, lo que induce que existe un alto déficit de implementación de directivas en

aseguramiento en la empresa. Se definió en la Declaración de Aplicabilidad (SoA), el empleo de 46 controles para el aseguramiento de la información. De estos 46 controles, 13 ya se están implementando en la empresa (pág.74).

- En la investigación denominada “Evaluación del sistema de seguridad de la información en la organización DISAV SAC aplicando lineamientos ISO 27001” Rivas (2019) nos menciona que:

  Se evaluó la gestión de la seguridad de la información basada en el estándar ISO 27001 en la Organización DISAV SAC, obteniendo como resultado la minimización en un 63,33%. Por lo tanto, se concluye que hay una minimización de la vulnerabilidad de la información de manera significativa (pág.45).

- En la investigación denominada “Sistema de gestión de seguridad de la información en la Municipalidad Distrital de Pira aplicando la norma ISO/IEC 27001:2013” Rivas (2019) nos menciona que:

  En base a la norma ISO/IEC 27001:2013, apoyado de la metodología MAGERIT versión 3.0 el estándar que permitió evaluar los riesgos de la seguridad de información, con el objetivo de determinar en qué condiciones se encuentran y si están alineadas con los objetivos del negocio garantizando la integridad de su información para el beneficio de la municipalidad (pág.130)

- En la investigación denominada “Diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2013 para una empresa de producción y comercialización de productos de consumo masivo” Cruz & Fukusaki (2017) nos menciona que:

  La implementación del Sistema de Gestión de Seguridad de la Información fue la base para lograr el cumplimiento del objetivo principal. La

implementación se logró a través del diseño e implementación de políticas para gestionar eficientemente el acceso a la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información logrando minimizar los riesgos de seguridad de la información (pág.131).

2.1.3. Antecedentes locales

- En la investigación denominada “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 Pasco Perú” Atencio (2019) nos menciona que:

  El eslabón más débil de la cadena son las personas, por lo tanto, dentro del análisis y evaluación del riesgo del SGSI se debe dar el énfasis necesario para considerar este tipo de amenazas. Siempre aplicando en los perfiles el principio del mínimo conocimiento. Dentro del análisis se pudo evidenciar que uno de los factores que afectan la disponibilidad e integridad de la información son por fallas del personal, ya que en gran parte la manipulación de la información no está dada por sistemas operativos óptimos, lo cual genera errores de configuración, de transaccionalidades mal ejecutadas y saltos de información (pág. 212).

2.2. Bases teóricas – científicas

2.2.1. Información

Uno de los activos más importantes dentro de las organizaciones es el activo intangible de la información, esto debido a que las organizaciones día a día generan grandes volúmenes de datos los cuales posteriormente se transforman en información las mismas que ayudan a tomar mejores decisiones a la organización, las mismas que son de mayor relevancia de acuerdo al sector de negocio, los cuales son:

- **En el ámbito sanitario.** Como menciona INCIBE (2019) que “se maneja un gran volumen de información personal de pacientes, a la que se deben aplicar todas las medidas de seguridad para evitar que se pierda, modifique o se acceda a ella sin autorización” (p.9).
- **En el sector financiero.** Como menciona INCIBE (2019) que “se maneja in- formación confidencial tanto de clientes como de operaciones financieras de compras y ventas de activos cuya difusión puede suponer una importante pérdida económica o un perjuicio para nuestros clientes” (p.9).
- **En el sector industrial o desarrollo de productos.** Como menciona INCIBE (2019) que “es importante velar por la confidencialidad de los procesos y procedimientos que nos pueden aportar una mejora de productividad sobre la competencia” (p.9).
- **En hotelería y restauración.** Como menciona INCIBE (2019) que “se maneja, además de un volumen de datos de carácter personal muy significativo, información sobre reservas, cuya pérdida nos podría poner en una situación muy complicada con nuestros clientes” (p.9).

2.2.2. Seguridad de la información.

Hoy en día la información tiene una gran relevancia en los aspectos de la búsqueda de la ventaja competitiva, la mejor toma de decisiones y el desarrollo institucional, es por ello que la información se debe de proteger. Vega (2021) menciona que “la seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada” (p.9). Esto debido a la gran evolución tecnológica que se vive a nivel general, debido a que muchos aspectos, actividades y procesos están cada vez más automatizados y apoyados en tecnologías de información y comunicación. De la misma manera

INCIBE (2019) menciona que “la información de nuestra empresa y constituyen uno de los activos más importantes de nuestra organización” (p.3)

Calderon (2018) menciona que “la seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden estar involucradas otras propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio” (p.1).

2.2.2.1. Dimensiones de la seguridad de la información.

La seguridad de la información está compuesta por tres dimensiones las mismas que también son conocidas como pilares o la triada de la seguridad de la información, los cuales se pueden observar en la siguiente figura:

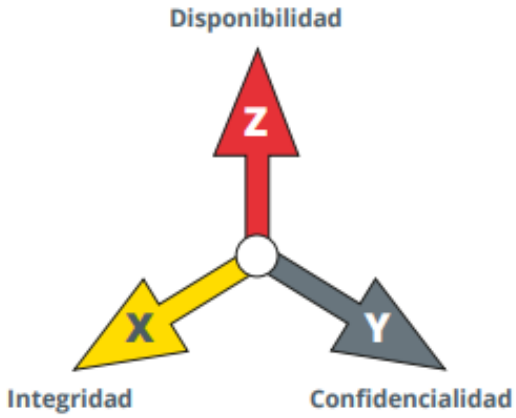


Figura 1. *Dimensiones de la seguridad de la información.* ***Fuente:*** *INCIBE (2019)*

- **Confidencialidad.** Como menciona Vega (2021) la confidencialidad “es un componente necesario de la privacidad y se refiere a nuestra capacidad de proteger nuestros datos de aquellos que no están autorizados para verlos” (p.12). De la misma manera INCIBE (2019) menciona que “es lo que se conoce como *need-to-know*. Con este término se hace referencia a que la información solo debe ponerse

en conocimiento de las personas, entidades o sistemas autorizados para su acceso” (p.6)

- **Integridad.** Como menciona Vega (2021) refiere que es “la capacidad de evitar que nuestros datos se modifiquen de manera no autorizada o indeseable. Esto podría significar el cambio o la eliminación no autorizada de nuestros datos o partes de nuestros datos” (p.13). De la misma manera INCIBE (2019) menciona que “hace referencia a que la información sea correcta y esté libre de modificaciones y errores” (p.6).
- **Disponibilidad.** Como menciona Vega (2021) refiere que “se refiere a la capacidad de acceder a nuestros datos cuando los necesitamos. La pérdida de disponibilidad puede referirse a una amplia variedad de interrupciones en cualquier parte de la cadena de comunicaciones que nos permite acceder a nuestros datos” (p.13). De la misma manera INCIBE (2019) menciona que “la disponibilidad de la información hace referencia a que la información esté accesible cuando la necesitemos” (p.6)

2.2.3. Sistema de gestión de seguridad de la información.

La organización indistintamente al sector productivo de cualquier tipo sea privado o público para adoptar un sistema de gestión de seguridad de la información (SGSI) deberá de tomar una decisión en base a sus necesidades, objetivos y procesos. Para conocer a fondo se explica según Estélia et al. (2014) menciona que “El SGSI en inglés Information Security Management System, ISMS, es un proceso estructurado de tratamiento de seguridad de la información en los diversos sectores” (pág. 75). El SGSI basa su implementación en el modelo PHVA, el cual está formado por una serie de pasos establecidos, el cual está definido a en siguiente apartado.

2.2.3.1. Modelo PHVA.

El modelo PHVA como ya se adelantó en el apartado anterior está formado por una serie de pasos, la cual está reflejada en el nombre por cada una de las siglas las cuales son explicadas a continuación:

- **Planear.** Según Estélia et al. (2014) hace referencia a: “establecer las políticas, objetivos, procesos y procedimientos del SGSI, relevantes para la gestión del riesgo y la mejora de la seguridad de información, para conseguir resultados de acuerdo con las políticas y objetivos generales de una organización” (pág. 74).
- **Hacer.** El termino hacer hace referencia a la implementación de SGSI y lo propuesto en el punto anterior (planear).
- **Verificar.** Según Estélia et al. (2014) menciona que: “(comprobar: monitorear y analizar críticamente el SGSI): evaluar y, si es el caso, medir el desempeño de un proceso con base en la política, los objetivos y la experiencia práctica del SGSI y presentar los resultados para la revisión” (pág. 74)
- **Actuar.** Según Estélia et al. (2014) menciona que: “(mantener y mejorar el SGSI): llevar a cabo las acciones correctivas y preventivas, basadas en los resultados de la auditoría interna del SGSI y el análisis crítico realizado por la dirección u otra información pertinente, para lograr la mejora continua del SGSI” (pág. 75).

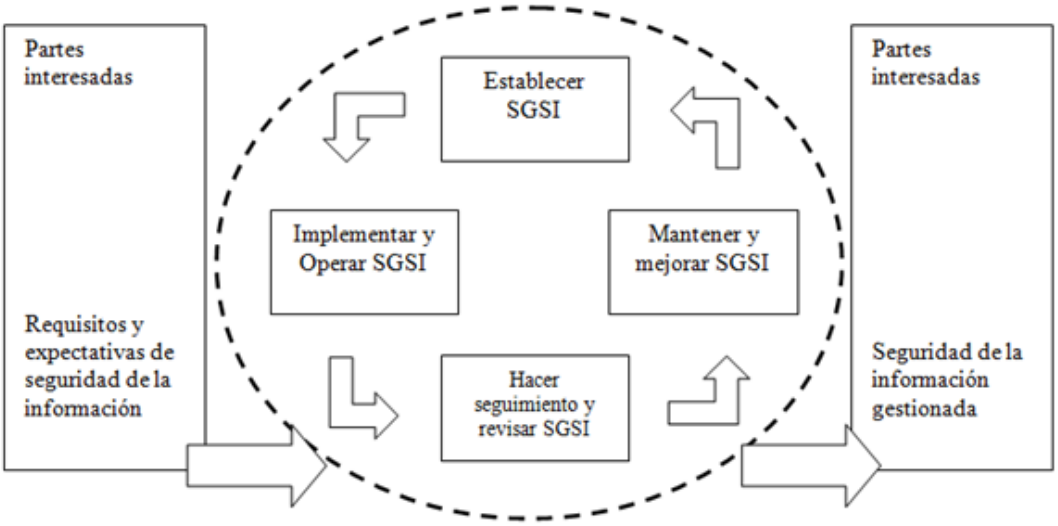


Figura 2. *Modelo PHVA aplicado a los procesos de SGSI.* ***Fuente:*** (Solarte, 2016)

2.2.3.2. Establecer el SGSI.

Para establecer un Sistema de Gestión de Seguridad de la Información se deben de tener en cuenta que los procesos internos, actividades, objetivos y otros deben de estar alineados a la propuesta del SGSI es por ello que se realiza un estudio previo a la organización para poder realizar la propuesta del SGSI.

Para ello se siguen el cumplimiento de los siguientes requisitos dentro de la organización:

- Definir el alcance.
- Definir la política de seguridad. Las políticas de seguridad deberán de estar alineadas con el contexto de la gestión de riesgos de la organización.
- Estrategia de evaluación de riesgos.
- Identificación, análisis y evaluación de riesgos.
- Seleccionar los controles y los objetivos para el tratamiento de riesgo.

- Obtener aprobación para los riesgos residuales.
- Obtener el consentimiento para la implementación.
- Preparar la declaración de aplicabilidad

2.2.3.3. Implementar el SGSI.

Posteriormente al cumplimiento de los requerimientos, se procede al análisis del contexto organizacional para ello se cumplen los siguientes puntos:

- Formulación e implementación del tratamiento de riesgos es como continuidad del análisis de los riesgos, la organización diseña, plantea e implementa un plan para el tratamiento de los riesgos.
- Implementar controles que permitan medir los indicadores principales para evaluar la eficacia y eficiencia.
- Implementación de un programa de entrenamiento para la capacitación.
- Gestionar las operaciones del sistema de gestión de seguridad de la información.
- Gestionar los recursos para el sistema de gestión de seguridad de la información.
- Implementación de procedimientos para la detección y respuesta a los incidentes de seguridad de la información.

2.2.3.4. Monitoreo y análisis de SGSI.

Los procesos de monitoreo y análisis son fundamentales para el éxito de cualquier sistema de gestión de seguridad de la información, es por ello que para la presente fase se tienen que cumplir los siguientes requerimientos:

- Realizar la ejecución de procedimientos de monitoreo y análisis crítico con la finalidad de la detección de errores de procesamiento, identificación de fallas, brechas de seguridad e incidentes para realizar el control de cada una de ellas.
- Realizar revisiones programadas de los resultados del sistema de gestión de seguridad de la información.
- Revisar los riesgos y basado en ello evaluar la posibilidad de realizar cambios con respecto a los bienes o procesos del negocio.
- Actualizar el plan de seguridad.
- Llevar un registro de las acciones, evento u otros que hayan afectado a la eficacia del sistema de gestión de seguridad de la información.

2.2.3.5. Documentación.

La documentación es un factor importante para el éxito de un sistema de gestión de seguridad de la información; es por ello que se enumeran a continuación los documentos que según Estélia et al. (2014) menciona que son necesario para la auditoria del SGSI:

- Declaración de la política de seguridad y los objetivos del SGSI;
- Alcance;
- Procedimientos y controles;
- Descripción de la metodología de análisis / evaluación de riesgos;
- Informe de análisis / evaluación de riesgos;
- Plan de tratamiento de riesgos;
- Procedimientos necesarios para garantizar la eficacia, la operación y los controles;
- Descripción de la medición de la eficacia de los controles;

- Registros requeridos.

2.2.3.6. Mejora del SGSI.

Para aplicar las mejoras del sistema de gestión de seguridad de la información se debe mejorar continuamente las políticas de seguridad, los objetivos, resultados de las auditorias, el análisis de los eventos monitoreados, acciones correctivas (para eliminar las causas de los requerimientos del SGSI para evitar el suceso por segunda vez) y preventivas (se debe de eliminar las potenciales amenazas para prevenir su ocurrencia).

2.2.4. NTP ISO/IEC 27001:2014.

La Presidencia de Consejo de Ministros (2016) aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" para todas las entidades integrantes del Sistemas Nacional de Informática. Mediante la Resolución Ministerial N°004-2016-PCM. El cual especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. El documento también establece procedimientos para la evaluación y tratamiento de los riesgos de seguridad a los que pueden estar expuestos los diversos activos informáticos.

La misma que reemplaza y cancela a la NTP ISO/IEC 27001:2008 con la finalidad de mantener actualizado la norma relacionada a la gestión de seguridad de la información.

2.2.4.1. NTP "Norma Técnica Peruana".

Las Normas Técnicas Peruana según el Ministerio de Desarrollo Agrario y Riego (2015) son "documentos que establecen las

especificaciones de calidad de los productos, procesos y servicios. Existen también NTP's sobre terminología, métodos de ensayo, muestreo, envase y rotulado que se complementan entre sí". De la misma manera se menciona que las Normas Técnicas Peruanas son elaborados por profesionales técnicos y expertos en el área o tema de la misma manera menciona que sigue el proceso donde "participan representantes de todos los sectores involucrados en la actividad a normalizar; estos son: productores, comercializadores, consumidores y técnicos calificados. Los Comités Técnicos de Normalización elaboran los proyectos de NTP's, los cuales son alcanzados a INDECOPI para su aprobación".

También cabe recalcar que según Instituto Nacional de Calidad (2022) menciona que "no se distribuyen de forma gratuita ya que están amparados en Ley N° 30224, Ley que crea el Sistema Nacional para la Calidad y el Instituto Nacional de Calidad, publicada el 11 de julio de 2014" (p.2), de la misma manera menciona que "cuyo artículo 39 señala que son recursos del INACAL, entre otros, los ingresos provenientes de los derechos de propiedad intelectual" (p.2).

2.2.4.2. ISO "Organización Internacional para la Normalización".

ISO o International Organization for Standardization que traducido al español es la Organización Internacional de Normalización la misma que define y establece normas técnicas con validez internacional.

Fundación Iberoamericana para la Gestión de la Calidad (2012) menciona que "contribuyen a que el desarrollo, la producción y el suministro de bienes y servicios sean más eficaces, seguros y transparentes. Gracias a estas normas, los intercambios comerciales entre países son más fáciles y justos".

2.2.4.3. IEC “Comisión Electrotécnica Internacional”

La IEC o Comisión Electrotécnica Internacional (International Electrotechnical Commission) la misma que tiene funcionamiento desde 1906 y con sede oficial en Ginebra, Suiza. La mencionada organización cuenta como principal función a la elaboración y publicación de normas internacionales relacionadas con los campos de electrónica, eléctrica y relacionadas. La organización tiene como ingresos la venta de las normas mencionadas.

De Buen (2017) menciona que “la IEC colabora con la ISO (Organización Internacional de Normalización) o con la UIT (Unión Internacional de Telecomunicaciones) para garantizar que las normas internacionales se ajusten de manera adecuada y se complementen entre sí”. De la misma manera menciona que las normas elaboradas por las IEC son de suma importancia debido a que permiten el comercio internacional de productos y servicios que tienen relación con las tecnologías; permitiendo la negociación entre cliente proveedor al establecer un parámetro o norma para los productos o servicios.

2.2.4.4. ISO/IEC 27000

El ISO/IEC 27001 es una familia de normas que establecen parámetros de calidad con la finalidad de asegurar la información de las organizaciones ISO (2013) menciona que “ISO/IEC 27001 es ampliamente conocido y proporciona requisitos para un sistema de gestión de seguridad de la información (ISMS), aunque hay más de una docena de estándares en la familia ISO/IEC 27000”. Los mismos que proporcionan a las organizaciones indistintamente a sus actividades gestionar la seguridad de sus activos e información.

La familia ISO 27000 contiene diversas normas entre las más representativas son:

- **ISO 27000.** ISO Tools Excellence (2004) menciona que “Está en fase de desarrollo. Contiene definiciones y términos empleados en toda la serie 27000. La aplicación de toda norma necesita un vocabulario definido claramente, que rehúya de diferentes interpretaciones de los conceptos de gestión y técnicos”.
- **ISO 27001.** ISO Tools Excellence (2004) menciona que “Es la principal norma de la serie. Contiene los requerimientos del SGS (Sistema de Gestión de Seguridad) de la información”.
- **ISO 27002.** ISO Tools Excellence (2004) menciona que “Es una especie de guía de buenas prácticas que delinean los objetivos de control recomendables en la seguridad de la información. No es certificable. Contiene un anexo en el que se resume todos los controles”.
- **ISO 27003.** ISO Tools Excellence (2004) menciona que “Está en fase de desarrollo. Consiste en una guía de implantación de SGSI del empleo del modelo PDCA y los requisitos de sus etapas”.
- **ISO 27004.** ISO Tools Excellence (2004) menciona que “Está en fase de desarrollo. Establece las técnicas aplicables para la determinación de la eficiencia de un SGSI y sus controles. Se utilizan fundamentalmente en el ciclo PDCA”.
- **ISO 27005.** ISO Tools Excellence (2004) menciona que “Establece los principios para la gestión del riesgo en la seguridad de la información. Diseñada para ayudar a la aplicación de la seguridad de la información en el enfoque de gestión de riesgos”.
- **ISO 27006.** ISO Tools Excellence (2004) menciona que “Establece los requerimientos de la acreditación de entidades auditoras y certificación de SGSI”.

- **ISO 27007.** ISO Tools Excellence (2004) menciona que “Establece los requerimientos de la acreditación de entidades auditoras y certificación de SGSI”.
- **ISO 27011.** ISO Tools Excellence (2004) menciona que “Está en fase de desarrollo. Consiste en una guía para la auditoria de un SGSI”.
- **ISO 27031.** ISO Tools Excellence (2004) menciona que “Está en fase de desarrollo. Es una guía de gestión de la seguridad de la información para las telecomunicaciones junto con ITU”.
- **ISO 27032.** ISO Tools Excellence (2004) menciona que “En fase de desarrollo. Guía vinculada a la ciber seguridad”.
- **ISO 27033.** Hace referencia a la fase de desarrollo. La misma que contiene 7 partes.
- **ISO 27034.** Hace referencia a la fase de desarrollo con la muestra de una guía para el desarrollo de aplicaciones.

2.2.4.5. Componentes de la NTP ISO/IEC 27001.

Con la finalidad de asegurar la información basada en los pilares principales de la seguridad de la información los mismo que son la confidencialidad, integridad y disponibilidad de los principales activos de la información se establecen los siguientes componentes a partir de la Norma Técnica Peruana en mención, los mismo que son:

- **Objetivo.** *Uso de La NTP ISO/IEC 27001:2014 En Las Entidaddes Integrantes Del Sistemas Nacional de Informática* (2015) menciona que el proyecto busca establecer los requisitos con la finalidad de mantener, implementar y mejorar el sistema de gestión de seguridad en las diversas organizaciones; de la misma manera se establece el tratamiento y gestión de riesgos de seguridad de la información, los

mismos que se buscan aplicar en los diversos niveles de gobiernos y organizaciones indistintamente al rubro de negocio o tamaño del mismo (p.4)

- **Referencias Normativas.** La NTP ISO/IEC27001 hace referencia a la norma ISO/IEC 27000 el mismo que establece normas y parámetros de seguridad de la información.
- **Términos y definiciones.** Como se menciona en el apartado anterior la NTP ISO/IEC 27001 hace referencia a los apartados ya proporcionados por el ISO/IEC 27000
- **Contexto de la organización.** Es el punto de partida para la implementación del SGSI “Sistema de Gestión de Seguridad de la Información”; en el mismo que se define el contexto interno y contexto externo, de la misma manera se debe comprender las necesidades y expectativas de las partes interesadas y finalmente se determina el alcance del sistema de gestión de seguridad de la información
- **Liderazgo.** El *Uso de La NTP ISO/IEC 27001:2014 En Las Entidaddes Integrantes Del Sistemas Nacional de Informática* (2015) menciona que la organización deberá demostrar compromiso y liderazgo relacionado al SGSI y deberá de establecer las políticas de seguridad e la información definidas, revisadas y aprobadas por la alta dirección y finalmente la alta dirección deberá de establecer roles, autoridad y responsabilidad del SGSI dentro de la organización.
- **Planificación.** El *Uso de La NTP ISO/IEC 27001:2014 En Las Entidaddes Integrantes Del Sistemas Nacional de Informática* (2015) menciona se establecen las acciones para tratar los riesgos y las

oportunidades, valorando el riesgos de seguridad de la información, tratando el riesgo de seguridad de la información; posteriormente se plantean los objetivos de seguridad de la información y planificación relacionados al Sistema de Gestión de Seguridad de la Información.

- **Soporte.** El *Uso de La NTP ISO/IEC 27001:2014 En Las Entidaddes Integrantes Del Sistemas Nacional de Informática* (2015) menciona que en el presente apartado se refiere a los recursos y el compromiso por parte de la organización, competencia, la concientización a los colaboradores de la organización, de la misma manera uno de los puntos primordiales es la comunicación y por ultimo se establece la información a documentar.
- **Operación.** El *Uso de La NTP ISO/IEC 27001:2014 En Las Entidaddes Integrantes Del Sistemas Nacional de Informática* (2015) menciona que en el siguiente apartado se debe planifircar, implementar y controlar los procesos necesarios con la finalidad de cumplir con los requisitos de seguridad de la información de la misma manera en este apartado se implementan las acciones como parte de la subsanación de brechas de seguridad, posteriormente se realiza nuevamente una evaluación de riesgos y finalmente el tratamiento de riesgos.
- **Evaluación del desempeño.** El *Uso de La NTP ISO/IEC 27001:2014 En Las Entidaddes Integrantes Del Sistemas Nacional de Informática* (2015) menciona que en el presente apartado se toma en cuenta el monitoreo, medición, análisis y evaluación del SGSI, se realiza una auditoria interna con la finalidad de buscar la mejora en SGSI y finalmente todo la documentación y procesos relacionados al SGSI deben ser revisados por la alta dirección.

- **Mejora continua.** El *Uso de La NTP ISO/IEC 27001:2014 En Las Entidaddes Integrantes Del Sistemas Nacional de Informática* (2015) menciona que la organización debe buscar la mejor continua con respecto a la adecuación y efectividad surgida a partir de nuevos requerimientos o la absolución de problemáticas detectadas correspondientes al Sistema de Gestión de Seguridad de la Información.

2.3. Definición de términos básicos

- **Activo informático.** Los activos informáticos son los equipos informáticos contando tanto a hardware y software dentro de una organización.
- **Amenaza informática.** Una amenaza informática es una eventual o posible actividad maliciosa que pueda afectar a una organización.
- **Ataque informático.** Es una actividad maliciosa con la finalidad de vulnerar la confidencialidad, integridad o disponibilidad de una organización.
- **Confidencialidad.** Es uno de los pilares de la seguridad de la información, está es la característica de que la información no sea divulgada sin mantener el consentimiento de una persona u organización.
- **Contingencia.** Es la actividad relacionada a tener una posibilidad de que un incidente pueda suceder o no en el transcurso del tiempo.
- **Disponibilidad.** Es uno de los pilares de la seguridad informática, la misma que se relaciona con que los servicios informáticos sean accesibles en todo momento que el usuario necesite de ellos.
- **Integridad.** Es uno de los pilares de la seguridad informática, la misma que se relaciona con que la información debe llegar a destino sin sufrir ninguna alteración por parte de personas malintencionadas.
- **Impacto.** Son los daños ocasionados a partir de un suceso o ataque informático.

- **ISO 27001.** Es un estándar enfocado a la seguridad de la información con la finalidad de asegurar los pilares de la seguridad de la información.
- **NTP ISO/IEC 27001:2014.** Es una norma técnica peruana la misma que adapta el ISO 27001 a la realidad y problemática peruana.
- **Riesgo.** Es la posibilidad de que un evento o incidente informático suceda.
- **Política de seguridad.** IBM (2021) menciona que "la política de seguridad define qué es lo que desea proteger, y los objetivos de seguridad expresan lo que espera de los usuarios del sistema".

2.4. Formulación de hipótesis

2.4.1. Hipótesis general

El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.

2.4.2. Hipótesis específicas

- El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la confidencialidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.
- El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la integridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.
- El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la

disponibilidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.

2.5. Identificación de variables.

2.5.1. Variable independiente.

NTP ISO/IEC 27001:2014.

2.5.2. Variable dependiente.

Sistema de gestión de seguridad de la información

2.6. Definición operacional de variables e indicadores.

Tabla 1. *Operacionalización de variables.*

Variables	Dimensiones	Indicadores
VI: NTP ISO/IEC 27001:2014	Dominios	• Número de dominios seleccionados. • Porcentaje de cumplimiento de los dominios.
	Controles	• Número de controles seleccionados. • Porcentaje de cumplimiento de los controles
VD: Sistema de gestión de seguridad de la información.	Confidencialidad	• Porcentaje de cumplimiento de la confidencialidad.
	Disponibilidad	• Tiempo promedio de incidentes de disponibilidad.
	Integridad.	• Porcentaje de cumplimiento de la integridad de la información.

Fuente: Elaboración Propia.

CAPÍTULO III

METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN

3.1. Tipo de investigación

La presente investigación es considerada del tipo aplicada debido a que el sistema de gestión de seguridad de la información implica la aplicación de normas y anexos recomendados por la NTP ISO/IEC 27001:2014; los mismos que se aplicaran en la confidencialidad, integridad y disponibilidad en los activos informáticos del Gobierno Regional Pasco; es por ello que referenciamos a Carrasco (2005) quien menciona que “está investigación se distingue por tener propósitos prácticos inmediatos bien definidos, es decir, se investiga para actuar, transformar, modificar o producir cambios en un determina sector de la realidad” (p.43). Es por ello que se consideró a la presente como investigación aplicada.

3.2. Nivel de investigación

La investigación en curso optó por hacer uso del nivel de investigación descriptivo debido al contenido y el objetivo de la presente; es por ello que para validar la decisión se optó por realizar la revisión literaria, es por ello que citamos a Carrasco (2005) quien menciona que “nos dice y refiere sobre las características, cualidad internas y externas, propiedades y rasgos esenciales

de los hechos y fenómenos de la realidad, en un momentos y tiempo histórico concreto y determinado" (p.42).

3.3. Métodos de investigación

Para la presente investigación se hizo uso del método inductivo – deductivo que mediante la revisión literaria se coincide con la razón de ser de la presente investigación es por ello que se cita a Bernal (2010) quien menciona que "este método de inferencia se basa en la lógica y estudia hechos particulares, aunque es deductivo en un sentido (parte de lo general a lo particular) e inductivo en sentido contrario (va de lo particular a lo general)" (p.60).

3.4. Diseño de investigación

La presente investigación debido a la estructura, razón de ser y el tipo de investigación optó por hacer uso del diseño de investigación cuasi experimental; es por ello que referenciamos a Hernández et al. (2013) quienes infieren que "manipulan deliberadamente, al menos, una variable independiente para observar su efecto sobre una o más variables dependientes, sólo que difieren de los experimentos puros en el grado de seguridad que pueda tenerse sobre la equivalencia inicial de los grupos" (p.151) de la misma manera mencionan que "los sujetos no se asignan al azar a los grupos ni se emparejan, sino que dichos grupos ya están conformados antes del experimento" (p.151).

3.5. Población y muestra

3.5.1. Población

Para la presente investigación se adopta como población a los trabajadores de la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco, los mismos que están conformados por un total de 12 colaboradores.

3.5.2. Muestra.

La presente investigación adoptó como muestreo no probabilístico del tipo muestreo intencional, debido a que como Carrasco (2005) menciona que “es aquella que el investigador selecciona según su propio criterio, sin ninguna regla matemática o estadística” (p.243), es por ello que para la muestra está conformada por la totalidad de los colaboradores de la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco los cuales son 12 colaboradores.

3.6. Técnicas e instrumentos de recolección de datos

La presente investigación, aplicó los siguientes instrumentos para la recolección de datos. Cabe recalcar que los instrumentos son validados previa a la realización de la investigación.

- Cuestionario.

3.7. Selección, validación y confiabilidad de los instrumentos de investigación

Para la validación de los instrumentos de recolección de datos se hizo uso de la validación mediante juicio de expertos los mismos que serán presentados en los anexos del presente documentos. De la misma manera para determinar la confiabilidad del instrumento de investigación se hizo uso de la estadística de confiabilidad de Cronbach la misma que se presenta en el siguiente capítulo del presente documento.

3.8. Técnicas de procesamiento y análisis de datos

Para el procesamiento y análisis de los datos se hizo uso del software estadístico paquete SPSS, porque permite realizar diversas actividades en relación a las variables en estudio (Estadística descriptiva e Inferencial), los mismos que son presentados mediante:

- En cuadros con frecuencias y porcentajes.
- Digitalización de datos.
- En gráfico circular.

- Elaboración del reporte final de la investigación.
- Presentación del reporte final de la investigación.

3.9. Tratamiento estadístico

Para el presente apartado se hizo uso de la estadística descriptiva con la finalidad de tabular y conocer mejor la información recolectada mediante las técnicas y análisis de datos; de la misma manera se hizo uso de la estadística inferencial para conocer y dar validación a la prueba de hipótesis.

3.10. Orientación ética, filosófica y epistémica

La presente tiene como orientación a la responsabilidad, rigor y veracidad como menciona Lopez (2018) quien menciona en la guía de investigación, código de ética para la investigación, en el artículo III, punto d) donde mencionan que “Los investigadores, estudiantes, autoridades y personal administrativo de la UNDAC deberán actuar con responsabilidad en relación con la pertinencia, los alcances y las repercusiones de la investigación, tanto a nivel individual e institucional como social” (p.27). de la misma manera menciona que “Deberán proceder con rigor científico asegurando la validez, la fiabilidad y credibilidad de sus métodos, fuentes y datos” (p.27).

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. Descripción del trabajo de campo

4.1.1. Descripción general de la institución.

El Gobierno Regional Pasco es el ente máximo en aspecto administrativo en el departamento Pasco, el mismo que se encarga de buscar el desarrollo económico, social y cultural de la región; el mismo que tiene como máximo representante al gobernador regional y consejo regional. Dentro de sus principales gerencias podemos encontrar a la Gerencia regional de planeamiento, presupuesto y acondicionamiento territorial, Gerencia regional de infraestructura, Gerencia región al d desarrollo social, Gerencia regional de desarrollo económico, Gerencia regional de recursos naturales y gestión del medio ambiente, entre otras. La misma que cuenta con la siguiente organización:

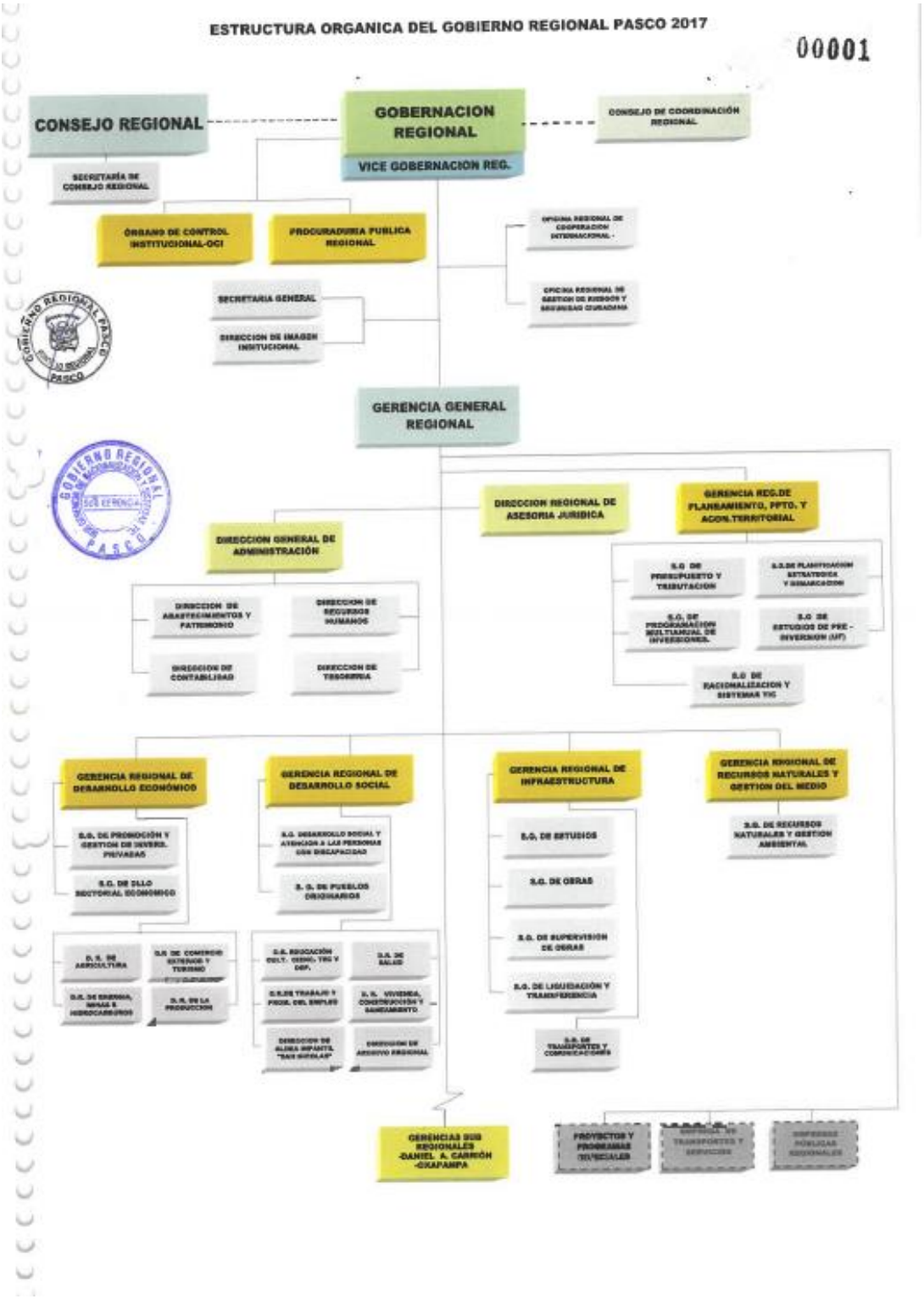


Figura 3. *Organigrama del Gobierno Regional Pasco.* ***Fuente:*** *Gobierno Regional Pasco (2017)*

De la misma manera podemos mencionar que el Gobierno Regional Pasco cuenta con una sede central la cual está ubicada en el: Edificio Estatal Nº

01 San Juan Pampa – Pasco, tal y como se puede observar en la siguiente figura:

Figura 4. *Ubicación geográfica Gobierno Regional Pasco.* ***Fuente:*** *Elaboración Propia.*

4.1.2. Desarrollo del proyecto.

El día 13 de setiembre se da inicio al diseño del sistema de gestión de seguridad digital en la Sub Gerencia de Racionalización y Sistemas TIC con la finalidad de tener a un buen resguardo los pilares de la seguridad de información los cuales son: disponibilidad, confidencialidad e integridad. Es por ello que se presenta la siguiente tabla en la cual se presenta la conformación del proyecto de diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2004.

Tabla 2. *Conformación del proyecto.*

NOMBRE DEL PROYECTO
Implementación de un sistema de gestión de seguridad de la información basada en la NTP ISO/IEC 27001:2014
DESCRIPCIÓN DEL PROYECTO
Implementación de un sistema de gestión de seguridad de la información basada en la NTP ISO/IEC el mismo que consiste en aplicar los anexos de la norma técnica. Los mismos que consistirán en las siguientes etapas de implementación: 27001:2014. **Etapas:** • Planificación del SGSI. • Implementación del SGSI. • Verificación del SGSI. • Mejora del SGSI. El proyecto se realizó desde el 13 de setiembre del 2021 hasta el 5 de abril del 2022.
PRODUCTO DEL PROYECTO
Se realizará la implementación del sistema de gestión de seguridad de la información basada en la NTP ISO/IEC 27001:2014 los mismo que se basarán en los procesos internos de la Sub Gerencia de Racionalización y Sistemas TIC.
ENTREGABLES DEL PROYECTO
• Se hará entrega de informes por cada etapa del desarrollo del proyecto. • Se hará entrega de un documento final.

Fuente: Elaboración Propia.

Tabla 3. *Objetivo del proyecto.*

Objetivos del Proyecto		
Concepto.	**Objetivos.**	**Criterios de éxito.**
Alcance	El proyecto en curso deberá de presentar los siguientes entregables: Alcance del SGSI, Políticas de seguridad informática, y demás.	• La entidad deberá recepciona y aprobar la documentación presentada.
Tiempo	El proyecto deberá de cumplir con los plazos determinados.	• Se realizará el seguimiento constante del cronograma propuesto.
Costo	Se deberá de cumplir con los presupuestos asignados.	• Se deberá de cumplir con el presupuesto sin excesos.

Fuente: Elaboración Propia.

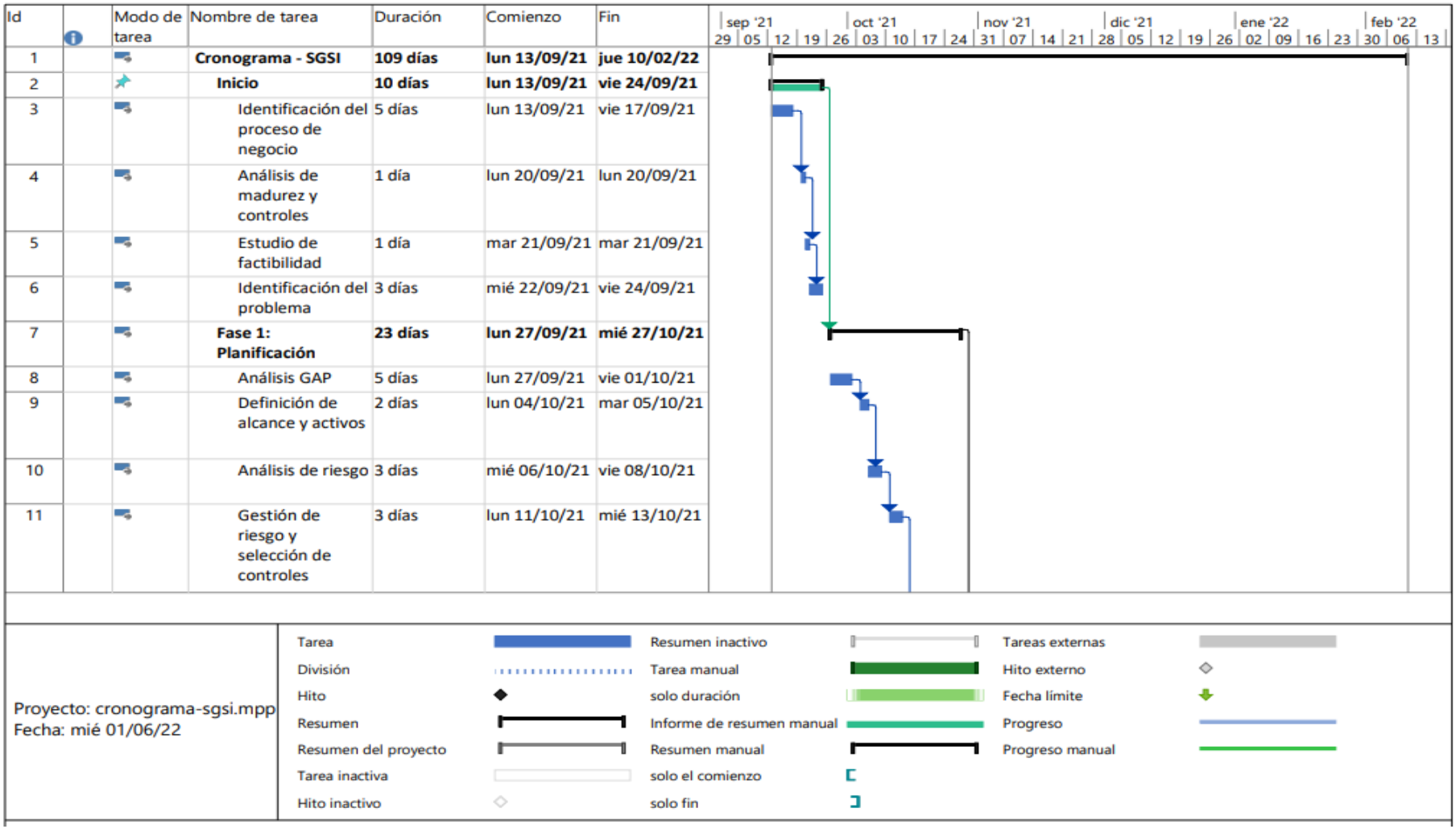
Tabla 4. *Finalidad del proyecto.*

FINALIDAD DEL PROYECTO		
Proteger la información generada por parte de la entidad con la finalidad de dar cumplimiento a la confidencialidad, disponibilidad e integridad.		
JUSTIFICACIÓN DEL PROYECTO		
Tener controles basados en buenas practicas recomendadas por la NTP ISO/IEC 27001 con respecto a la seguridad de la información.		
DESIGNACIÓN DEL PROJECT MANAGER DEL PROYECTO		
Encargado:	Oficial de seguridad	**Niveles de Autoridad**
Reporta a:	Gerente general.	Realizar seguimiento y exigir el cumplimiento del proyecto
Supervisa a:	Sub Gerente de Racionalización y Sistemas TIC	
CRONOGRAMA DE HITOS DEL PROYECTO:		
HITO O EVENTO		**PROGRAMACIÓN**
Diagnostico		13/09/21 al 24/09/21
Planificación		27/09/21 al 27/10/21
Implementación		28/10/21 al 09/12/21
Verificación		10/12/21 al 13/01/22
Mejora		14/01/22 al 10/02/22
Fin del proyecto		
PRINCIPALES AMENAZAS DEL PROYECTO		
• Limites de tiempo puede representar una amenaza para el proyecto debido a que puede ser un limitante al éxito del cumplimiento de todos los anexos que se referencia por el SGSI. • Versiones actualizadas de las normas. • Observaciones e incumplimientos de los entregables.		
PRINCIPALES OPORTUNIDADES DEL PROYECTO		
La implementación del SGSI permite la identificación del cumplimiento y medir la eficacia y eficiencia con respecto a los controles tecnológicos y físicos considerados en el presente proyecto.		

Fuente: Elaboración Propia.

4.1.3. Cronograma de trabajo.

En el presente apartado se presenta el cronograma tentativo presentado para el diseño e implementación del sistema de gestión de seguridad de la información, el mismo que muestra las fechas según cada una de las etapas consideradas en el presente proyecto, los cuales son etapa inicial, planificación, implementación, verificación y mejora del SGSI.



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Cronograma - SGSI**	**109 días**	**lun 13/09/21**	**jue 10/02/22**
2		**Inicio**	**10 días**	**lun 13/09/21**	**vie 24/09/21**
3		Identificación del proceso de negocio	5 días	lun 13/09/21	vie 17/09/21
4		Análisis de madurez y controles	1 día	lun 20/09/21	lun 20/09/21
5		Estudio de factibilidad	1 día	mar 21/09/21	mar 21/09/21
6		Identificación del problema	3 días	mié 22/09/21	vie 24/09/21
7		**Fase 1: Planificación**	**23 días**	**lun 27/09/21**	**mié 27/10/21**
8		Análisis GAP	5 días	lun 27/09/21	vie 01/10/21
9		Definición de alcance y activos	2 días	lun 04/10/21	mar 05/10/21
10		Análisis de riesgo	3 días	mié 06/10/21	vie 08/10/21
11		Gestión de riesgo y selección de controles	3 días	lun 11/10/21	mié 13/10/21

Figura 5. *Cronograma del SGSI – Parte 1.* ***Fuente:*** *Elaboración Propia.*

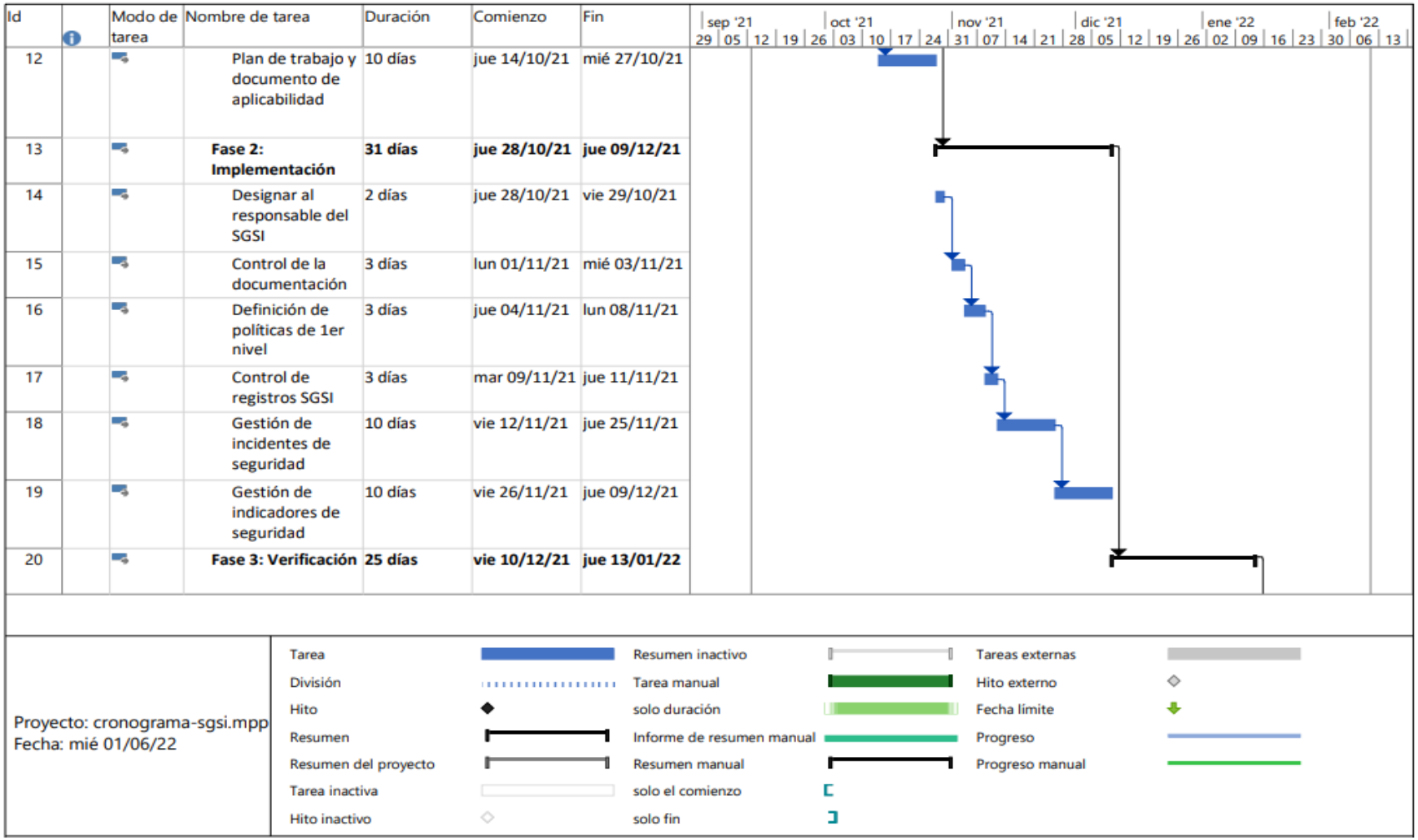


Figura 6. *Cronograma del SGSI – Parte 2.* ***Fuente:*** *Elaboración Propia.*

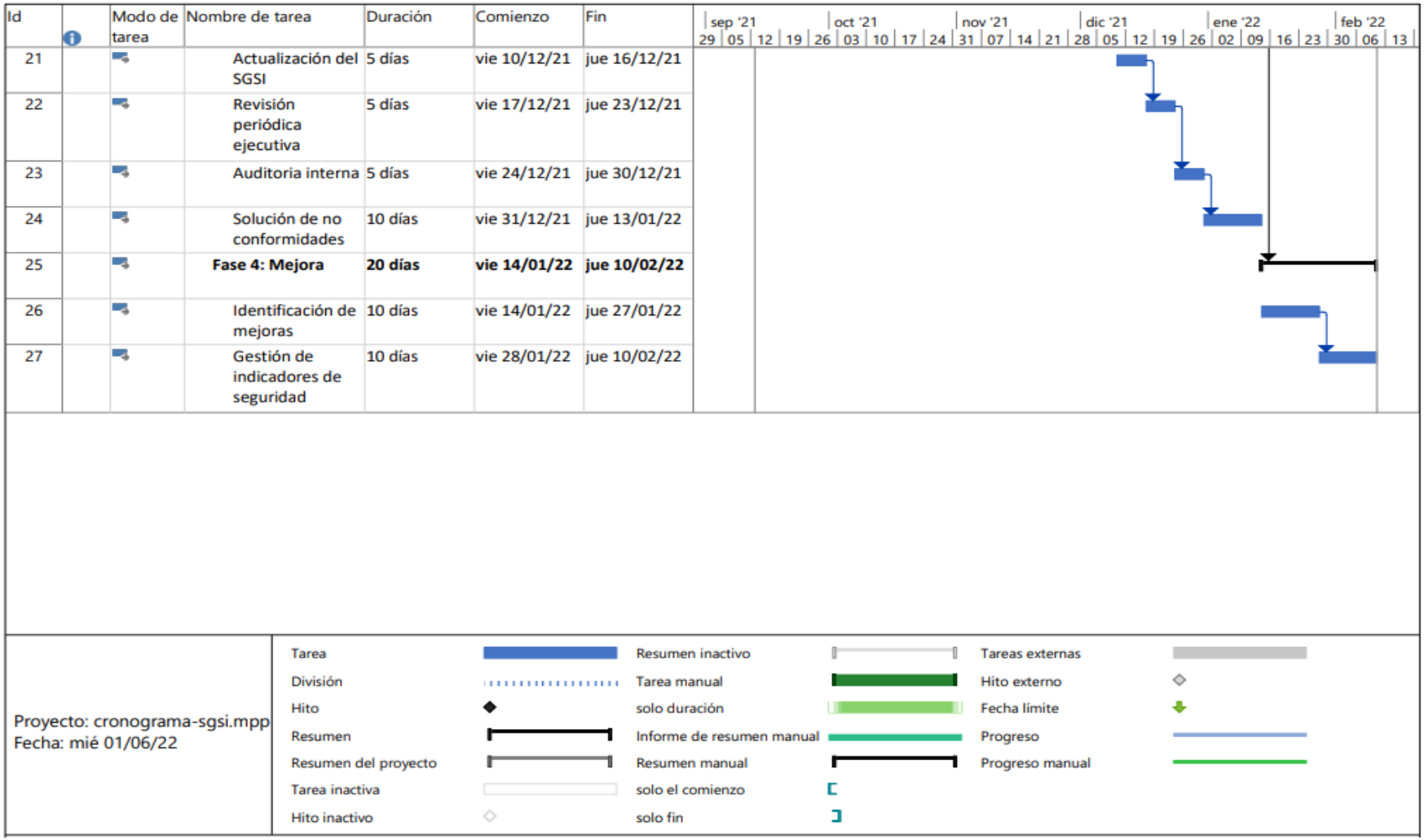


Figura 7. *Cronograma del SGSI – Parte 3.* ***Fuente:*** *Elaboración Propia.*

4.1.4. Recursos del proyecto.

En el siguiente apartado del proyecto se presentan los recursos utilizados para el desarrollo del diseño del sistema de gestión de seguridad de la información, los mismo que se presentan en la siguiente tabla.

Tabla 5. *Recursos del proyecto.*

ITEM		TOTAL
BIENES	✓ Material de escritorio. ✓ Laptop ✓ Dispositivo de almacenamiento externo	S/.550 S/. 4500 S/. 550
SERVICIOS	✓ Internet ✓ Fotocopias ✓ Impresión ✓ Asesoramiento ✓ Movilidad ✓ Encuadernación ✓ Alimentos	S/. 1200 S/. 500 S/. 1000 S/. 2500 S/. 500 S/. 150 S/. 2500
TOTAL		S/. 13950
FINANCIAMIENTO	El financiamiento del trabajo de investigación será autofinanciado por el tesista.	

Fuente: Elaboración Propia.

4.1.5. Diagnostico.

La razón de ser del presente proceso es la medición del cumplimiento institucional de la NTP ISO/IEC 27001:2014 en los procesos tecnológicos de la Sub Gerencia de Racionalización y Sistemas TIC. Por ello como parte de la medición y tener una clara visión de cumplimiento inicial se hace uso del estudio o análisis de brechas la misma que también es conocida como análisis GAP, a continuación, se muestran los resultados obtenidos a partir del análisis de brechas.

Tabla 6. *Diagnóstico inicial de los dominios basados en la NTP ISO/IEC 27001:2014.*

DOMINIOS NTP ISO/IEC 27001:2014	Nivel Actual	Nivel Deseado
A.05 Política de Seguridad de la Información.	1	4
A.06 Organización de la Seguridad de la Información.	0	3
A.07 Seguridad de los Recursos Humanos.	1	3
A.08 Gestión de Activos.	1	3
A.09 Control de Acceso.	1	3
A.10 Criptografía.	1	3
A.11 Seguridad Física y Ambiental.	1	3
A.12 Seguridad de las Operaciones.	0	3
A.13 Seguridad de las Comunicaciones.	1	1
A.14 Adquisición, desarrollo y mantenimiento de sistemas.	0	3
A.15 Relaciones con los proveedores.	0	3
A.16 Gestión de incidentes de seguridad de la información.	1	3
A.17 Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio	1	3
A.18 Cumplimiento.	1	3

Fuente: Elaboración Propia.

Tabla 7. *Diagnóstico inicial de los controles basados en la NTP ISO/IEC 27001:2014.*

	Nivel Actual	Nivel Deseado	Observaciones
A.05 Política de Seguridad de la Información.			
5.1. Directrices de la Dirección en seguridad de la información.			
5.1.1 Conjunto de políticas para la seguridad de la información.	**1**	**4**	
5.1.2 Revisión de las políticas para la seguridad de la información	**1**	**4**	
A.06 Organización de la Seguridad de la Información.			
6.1 Organización interna.			
6.1.1 Asignación de responsabilidades para la seguridad de la información.	**1**	**4**	
6.1.2 Segregación de tareas.	**0**	**4**	
6.1.3 Contacto con las autoridades.	**1**	**3**	
6.1.4 Contacto con grupos de interés especial.	**1**	**3**	
6.1.5 Seguridad de la información en la gestión de proyectos.	**0**	**3**	
6.2 Dispositivos para movilidad y teletrabajo.			
6.2.1 Política de uso de dispositivos para movilidad.	**0**	**3**	
6.2.2 Teletrabajo.	**0**	**3**	
A.07 Seguridad de los Recursos Humanos.			
7.1 Antes de la contratación.			
7.1.1 Investigación de antecedentes.	**1**	**3**	
7.1.2 Términos y condiciones de contratación.	**1**	**4**	
7.2 Durante la contratación.			
7.2.1 Responsabilidades de gestión.	**0**	**3**	
7.2.2 Concienciación, educación y capacitación en seguridad de la información	**0**	**4**	
7.2.3 Proceso disciplinario.			
7.3 Cese o cambio de puesto de trabajo.	**1**	**3**	
7.3.1 Cese o cambio de puesto de trabajo.	**1**	**3**	
A.08 Gestión de Activos.			
8.1 Responsabilidad sobre los activos.			
8.1.1 Inventario de activos.	**0**	**4**	

	8.1.2 Propiedad de los activos.	0	2	
	8.1.3 Uso aceptable de los activos.	1	3	
	8.1.4 Devolución de activos.	3	4	
	8.2 Clasificación de la información.			
	8.2.1 Directrices de clasificación.	2	3	
	8.2.2 Etiquetado y manipulado de la información.	1	3	
	8.2.3 Manipulación de activos.	1	3	
	8.3 Manejo de los soportes de almacenamiento.			
	8.3.1 Gestión de soportes extraíbles.	0	3	
	8.3.2 Eliminación de soportes.	0	3	
	8.3.3 Soportes físicos en tránsito.	0	3	
A.09 Control de Acceso.				
	9.1 Requisitos de negocio para el control de accesos.			
	9.1.1 Política de control de accesos.	2	3	
	9.1.2 Control de acceso a las redes y servicios asociados.	1	2	
	9.2 Gestión de acceso de usuario.			
	9.2.1 Gestión de altas/bajas en el registro de usuarios.	0	3	
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	1	3	
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	0	3	
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	1	3	
	9.2.5 Revisión de los derechos de acceso de los usuarios.	1	3	
	9.2.6 Retirada o adaptación de los derechos de acceso	1	3	
	9.3 Responsabilidades del usuario.			
	9.3.1 Uso de información confidencial para la autenticación.	1	3	
	9.4 Control de acceso a sistemas y aplicaciones.			
	9.4.1 Restricción del acceso a la información.	1	3	
	9.4.2 Procedimientos seguros de inicio de sesión.	1	3	
	9.4.3 Gestión de contraseñas de usuario.	1	3	
	9.4.4 Uso de herramientas de administración de sistemas.	1	3	
	9.4.5 Control de acceso al código fuente de los programas.	1	3	

A.10 Criptografía.				
	10.1 Controles criptográficos.			
	10.1.1 Política de uso de los controles criptográficos.	**1**	**3**	
	10.1.2 Gestión de claves	**1**	**3**	
A.11 Seguridad Física y Ambiental.				
	11.1 Áreas seguras.			
	11.1.1 Perímetro de seguridad física.	**1**	**3**	
	11.1.2 Controles físicos de entrada.	**1**	**3**	
	11.1.3 Seguridad de oficinas, despachos y recursos.	**1**	**3**	
	11.1.4 Protección contra las amenazas externas y ambientales.	**1**	**3**	
	11.1.5 El trabajo en áreas seguras.	**1**	**3**	
	11.1.6 Áreas de acceso público, carga y descarga.	**0**	**3**	
	11.2 Seguridad de los equipos.			
	11.2.1 Emplazamiento y protección de equipos.	**1**	**3**	
	11.2.2 Instalaciones de suministro.	**1**	**3**	
	11.2.3 Seguridad del cableado.	**0**	**3**	
	11.2.4 Mantenimiento de los equipos.	**1**	**3**	
	11.2.5 Salida de activos fuera de las dependencias de la empresa.	**1**	**3**	
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	**0**	**3**	
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	**1**	**3**	
	11.2.8 Equipo informático de usuario desatendido.	**1**	**3**	
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	**1**	**3**	
A.12 Seguridad de las Operaciones.				
	12.1 Responsabilidades y procedimientos de operación.			
	12.1.1 Documentación de procedimientos de operación.	**0**	**3**	
	12.1.2 Gestión de cambios.	**0**	**2**	
	12.1.3 Gestión de capacidades.	**0**	**2**	
	12.1.4 Separación de entornos de desarrollo, prueba y producción.	**0**	**2**	
	12.2 Protección contra código malicioso.			
	12.2.1 Controles contra el código malicioso.	**0**	**3**	

	12.3 Copias de seguridad.			
	12.3.1 Copias de seguridad de la información.	**2**	**3**	
	12.4 Registro de actividad y supervisión.			
	12.4.1 Registro y gestión de eventos de actividad.	**0**	**3**	
	12.4.2 Protección de los registros de información.	**1**	**3**	
	12.4.3 Registros de actividad del administrador y operador del sistema.	**1**	**3**	
	12.4.4 Sincronización de relojes.	**0**	**3**	
	12.5 Control del software en explotación.			
	12.5.1 Instalación del software en sistemas en producción.	**0**	**4**	
	12.6 Gestión de la vulnerabilidad técnica.			
	12.6.1 Gestión de las vulnerabilidades técnicas.	**0**	**4**	
	12.6.2 Restricciones en la instalación de software.	**0**	**4**	
	12.7 Consideraciones de las auditorías de los sistemas de información.			
	12.7.1 Controles de auditoría de los sistemas de información.	**1**	**3**	
A.13 Seguridad de las Comunicaciones.				
	13.1 Gestión de la seguridad en las redes.			
	13.1.1 Controles de red.	**1**	**3**	
	13.1.2 Mecanismos de seguridad asociados a servicios en red.	**1**	**3**	
	13.1.3 Segregación de redes.	**2**	**3**	
	13.2 Intercambio de información con partes externas.			
	13.2.1 Políticas y procedimientos de intercambio de información.			**No aplica**
	13.2.2 Acuerdos de intercambio.			**No aplica**
	13.2.3 Mensajería electrónica.			**No aplica**
	13.2.4 Acuerdos de confidencialidad y secreto.			**No aplica**
A.14 Adquisición, desarrollo y mantenimiento de sistemas.				
	14.1 Requisitos de seguridad de los sistemas de información.			
	14.1.1 Análisis y especificación de los requisitos de seguridad.	**1**	**2**	
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	**1**	**2**	
	14.1.3 Protección de las transacciones por redes telemáticas.	**0**	**2**	
	14.2 Seguridad en los procesos de desarrollo y soporte.			

	14.2.1 Política de desarrollo seguro de software.	0	3	
	14.2.2 Procedimientos de control de cambios en los sistemas.	0	3	
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	0	3	
	14.2.4 Restricciones a los cambios en los paquetes de software.	0	2	
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	0	2	
	14.2.6 Seguridad en entornos de desarrollo.	0	3	
	14.2.7 Externalización del desarrollo de software.	0	3	
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	1	3	
	14.2.9 Pruebas de aceptación.	0	3	
	14.3 Datos de prueba.			
	14.3.1 Protección de los datos utilizados en pruebas.	0	3	
A.15 Relaciones con los proveedores.				
	15.1 Seguridad de la información en las relaciones con suministradores.			
	15.1.1 Política de seguridad de la información para suministradores.	0	3	
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	0	3	
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	0	3	
	15.2 Gestión de la prestación del servicio por suministradores.			
	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	0	3	
	15.2.2 Gestión de cambios en los servicios prestados por terceros.	1	3	
A.16 Gestión de incidentes de seguridad de la información.				
	16.1 Gestión de incidentes de seguridad de la información y mejoras.			
	16.1.1 Responsabilidades y procedimientos.	1	3	
	16.1.2 Notificación de los eventos de seguridad de la información.	1	3	
	16.1.3 Notificación de puntos débiles de la seguridad.	1	3	
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	1	3	
	16.1.5 Respuesta a los incidentes de seguridad.	1	3	
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	1	3	
	16.1.7 Recopilación de evidencias.	1	3	

A.17 Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio				
	17.1 Continuidad de la seguridad de la información.			
	17.1.1 Planificación de la continuidad de la seguridad de la información.	**1**	**3**	
	17.1.2 Implantación de la continuidad de la seguridad de la información.	**1**	**3**	
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	**1**	**3**	
	17.2 Redundancias.			
	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	**0**	**3**	
A.18 Cumplimiento.				
	18.1 Cumplimiento de los requisitos legales y contractuales.			
	18.1.1 Identificación de la legislación aplicable.	**2**	**3**	
	18.1.2 Derechos de propiedad intelectual (DPI).	**1**	**3**	
	18.1.3 Protección de los registros de la organización.	**1**	**3**	
	18.1.4 Protección de datos y privacidad de la información personal.	**2**	**3**	
	18.1.5 Regulación de los controles criptográficos.	**1**	**3**	
	18.2 Revisiones de la seguridad de la información.			
	18.2.1 Revisión independiente de la seguridad de la información.	**1**	**3**	
	18.2.2 Cumplimiento de las políticas y normas de seguridad.	**1**	**3**	
	18.2.3 Comprobación del cumplimiento.	**1**	**3**	

Fuente: Elaboración Propia

En la tabla presenta anteriormente tabla 6 y tabla 7 se presentan los resultados del diagnóstico inicial de los controles y dominios del SGSI los mismos que se valoran de la siguiente manera:

- 0 = Controles inexistentes
- 1 = Controles Ad-hoc y Desorganizados

- 2 = Controles siguen un patrón regular
- 3 = Controles documentadas, asignadas y comunicadas
- 4 = Controles monitoreadas y medidas
- 5 = Buenas prácticas implementadas y automatizadas

4.1.6. Planificación.

4.1.6.1. Procesos involucrados en el proyecto.

En el presente apartado se muestran los procesos que están involucrados en el sistema de gestión de seguridad de la información, los cuales están divididos en procesos operativos y procesos de soporte los cuales son presentados a continuación:

- **Procesos operativos.** Los procesos operativos son: el proceso de gestión administrativa, proceso de gestión financiera, proceso de gestión documental. Los mencionados soportes tienen el alcance en:
  - **Mesa de servicios.**
    - Gestionar el parqueo informático del Gobierno Regional Pasco, de la misma manera se encargarán las actividades de mantenimiento preventivo y correctivo de los mismos.
    - Gestión de solicitudes de atención a incidentes de soporte técnico e informáticos a las diferentes unidades de la entidad.
    - Gestión de atenciones de soporte técnico e informático cotidiano (instalación y configuración de impresoras, instalación de configuración de software, reparaciones, entre otras).
  - **Administración de TI.**
    - **Base de datos.** La presente está compuesta por las actividades de gestión las mismas que se componen por (administrar, monitorear, configurar y gestionar los accesos a la misma). De la misma manera son considerados los mantenimientos de los datos y las auditorias de datos.

- **Servidores.** Está compuesto por actividades de mantenimiento preventivo y correctivo, monitoreos constantes y el control de acceso a las mismas.
- **Aplicaciones.** La gestión de aplicaciones implica el mantenimiento predictivo y correctivo del servidor de aplicaciones; monitoreo de las aplicaciones, modificaciones de seguridad en las aplicaciones; creación, modificaciones y eliminación de aplicaciones.
- **Redes y comunicaciones.** La gestión de las redes y comunicaciones incluye las actividades de monitoreo de los servidores físicos y virtuales; centralizar la documentación generada por parte de la organización mediante un servidor de archivos; actualización de seguridad tanto en bios y firmware, parches de seguridad y otros; inspeccionar los diversos recursos informáticos a su cargo tanto hardware como software y mantener actualizado el parqueo informático e inventario de IP´s.
- **Seguridad perimetral.** El siguiente proceso se refiere a los mecanismos y servicios implementados con la finalidad de mantener la seguridad informática de la organización. Dentro de los cuales podemos mencionar a:
  - Gestión de accesos.
  - Gestión de repuesta a incidentes de seguridad de la información.
  - Gestión de mantenimiento a los activos informáticos relacionados con seguridad perimetral, acceso a internet, accesos remotos, entre otros.
  - Gestión de actualizaciones de seguridad.

        - Gestión de protección de puestos de trabajo.
    - **Otros.** Entre las diversas gestiones de operaciones podemos encontrar también a los siguientes procesos:
        - Gestión de accesos físicos al centro de datos.
        - Gestión de calidad software y pase a producción.
        - Diseño e implementación de scripts.
        - Gestión de copias de seguridad.
        - Gestión de respuesta de incidentes.
        - Medios y dispositivos externos de almacenamiento.
        - Gestión de soporte preventivo y correctivo del centro de datos.
        - Gestión de monitoreo de los servicios informáticos.

- **Procesos de soporte.**

el siguiente apartado presente a los procesos los cuales dan soporte a las actividades operativas de la organización las mismas que son cumplidas por los servidores públicos del Gobierno Regional Pasco.

- **Gestión de financiera.** Gestionar las actividades relacionadas a la ejecución presupuestal, de la misma manera se deberá ofrecer un servicio de calidad con respecto al sistema de administración financiera a todos los usuarios que requieran soporte técnico e informático. De la misma manera la organización deberá estar comprometida con los recursos económicos para ofrecer los servicios de calidad en favor de la población.
- **Gestión administrativa.** Gestionar la información relacionada con la gestión administrativa la misma que se hace uso

mediante un sistema de gestión administrativa; de la misma manera la organización deberá de colaborar en cada uno de los requerimientos técnicos y de información que requiera el proyecto.

- **Gestión documental.** La organización deberá de gestionar adecuadamente la documentación generada por parte del proyecto las mismas que son de vital importancia para el cumplimiento y auditoria del SGSI.

4.1.6.2. Alcance del SGSI.

Se define el alcance del sistema de gestión de la seguridad de la información con la finalidad de tener un panorama más claro acerca del proyecto.

Es por ello que el sistema de gestión de seguridad de la información plantea como objetivo involucrar los procesos y los riesgos asociados con los datos generados por parte de las actividades relacionadas a ellas, es por ello que se observa en la siguiente tabla el alcance del SGSI.

Tabla 8. *Alcance del SGSI.*

Código	Procesos involucrados en el SGSI	Áreas involucradas directamente
PE1	Gestión financiera, gestión administrativa y gestión documental.	Sub gerencia de racionalización y sistemas TIC, secretaria general, Dirección General de administración, Dirección de abastecimientos.

Fuente: Elaboración Propia.

4.1.6.3. Liderazgo y compromiso.

El siguiente está basada en el compromiso de la institución al realizar la definición de los roles y responsabilidades, los recursos, la

política de seguridad de la información y los objetivos de seguridad de la información.

4.1.6.4. Política de seguridad de la información.

La Sub Gerencia de Racionalización y Sistemas TIC como parte de la gestión tecnológica de la gestión financiera, administrativa y documental, siendo conscientes de la importancia de la protección de la información generada por los procesos en cuestión se debe de implementar el sistema de gestión de seguridad de la información SGSI, es por lo expresado que se determina como política:

La institución ha determinado como política de seguridad de la información, con la finalidad de poner en buen recaudo la información generada a partir de la gestión financiera, administrativa y documental, se compromete a:

- El cumplimiento de las normas propuestas por el Gobierno Central con respecto a seguridad de la información.
- Gestionar la mejora continua del SGSI.
- Orientar y gestionar la cultura de seguridad de la información para con todos los colaboradores del Gobierno Regional Pasco.
- Respaldar la información de los procesos en cuestión con la finalidad de asegurar la información basados en la confidencialidad, integridad y disponibilidad.
- Gestionar los incidentes de seguridad informática.

4.1.6.5. Definición de roles y actividades del SGSI.

- **Comité de transformación digital.**

  El comité de transformación digital está conformado por el titular del pliego, el responsable de la información el cual es el

Secretario General, el Director de Recursos Humanos, el responsable de TI y el oficial de seguridad digital. Los mismo que deberán cumplir con las siguientes responsabilidades:

- Gestionar las políticas y objetivos de la seguridad de la información.
- Revisar el cumplimiento de requisitos del SGSI. Los mismo que deberán de integrarse a uno o varios procesos determinados al inicio de cada proyecto.
- Definir y gestionar los recursos necesarios para el alcance del SGSI.
- Gestionar la mejora continua.
- Asignar roles y responsabilidades en temas de seguridad de la información.
- Gestionar y evaluar el cumplimiento y los resultados de la gestión de riesgos de la información.
- Gestionar las mejoras propuestas a partir de las auditorias.

- **Oficial de seguridad digital.** El oficial de seguridad digital será el encargado de realizar la gestión del sistema de gestión de seguridad de la información las mismas que estarán basadas en el análisis de los resultados; gestionar las auditorias del SGSI; ser participe y organizador de la concientización en gestión de seguridad de la información; de la misma manera es el encargado de conducir y proponer mejorar en el SGSI.
- **Propietario del activo de información.** Es el colaborador o funcionario público de la institución el mismo que deberá de controlar y asegurar los activos informáticos proporcionados por parte de la institución; también el funcionario público deberá ser consciente y deberá de preservar la información proporcionada; de

la misma manera el propietario de la información deberá de hacer uso de los activos a su cargo solamente con fines y propósitos de la organización.

- **Custodio del activo de información.** El custodio tendrá como principales responsabilidades cumplir con los controles, dominio del SGSI de la misma manera con las políticas de seguridad de la información; deberá de hacer un uso correcto sobre los activos proporcionados por la institución; deberá de tener una comunicación constante con los propietarios de la información comunicando las vulnerabilidades identificadas.
- **Propietario del riesgo.** El propietario del riesgo será la persona encargada en verificar el cumplimiento de los controles de seguridad definidos con la finalidad de reducir el impacto del riesgo.

4.1.6.6. Declaración de aplicabilidad.

En el presente apartado se presentan los controles y los dominios con la finalidad de realizar la definición de los controles basados en anexo A del ISO 27001:2013; para el presente proyecto se aplicaron los siguientes controles:

Tabla 9. *Diagnóstico inicial de los controles basados en la NTP ISO/IEC 27001:2014.*

Controles	¿Aplica?	Evidencia / Propuesta
A.05 Política de Seguridad de la Información.		
5.1. Directrices de la Dirección en seguridad de la información.		
5.1.1 Conjunto de políticas para la seguridad de la información.	Si	Política de seguridad de la información
5.1.2 Revisión de las políticas para la seguridad de la información	Si	Política de seguridad de la información
A.06 Organización de la Seguridad de la Información.		
6.1 Organización interna.		
6.1.1 Asignación de responsabilidades para la seguridad de la información.	Si	Manual de organizaciones y funciones (MOF)
6.1.2 Segregación de tareas.	Si	Manual de organizaciones y funciones (MOF)
6.1.3 Contacto con las autoridades.	Si	Directorio de contactos.
6.1.4 Contacto con grupos de interés especial.	Si	Directorio de contactos.
6.1.5 Seguridad de la información en la gestión de proyectos.	Si	Manual de gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.		
6.2.1 Política de uso de dispositivos para movilidad.	Si	Directiva de TI y seguridad de la información.
6.2.2 Teletrabajo.	Si	Directiva de teletrabajo.
A.07 Seguridad de los Recursos Humanos.		
7.1 Antes de la contratación.		
7.1.1 Investigación de antecedentes.	Si	Términos de referencia de contrataciones.
7.1.2 Términos y condiciones de contratación.	Si	Terminas de referencia de contrataciones / Contratos
7.2 Durante la contratación.		
7.2.1 Responsabilidades de gestión.	Si	Manual de organizaciones y funciones (MOF)
7.2.2 Concienciación, educación y capacitación en seguridad de la información	Si	Plan de capacitaciones en seguridad de la información.

	7.2.3 Proceso disciplinario.		
	7.3 Cese o cambio de puesto de trabajo.	Si	Carta de agradecimiento.
	7.3.1 Cese o cambio de puesto de trabajo.	Si	Carta de agradecimiento.
A.08 Gestión de Activos.			
	8.1 Responsabilidad sobre los activos.		
	8.1.1 Inventario de activos.	Si	Inventario de activos de la información.
	8.1.2 Propiedad de los activos.	Si	Inventario de activos de la información.
	8.1.3 Uso aceptable de los activos.	Si	Directiva de TI y seguridad de la información.
	8.1.4 Devolución de activos.	Si	Directiva de TI y seguridad de la información.
	8.2 Clasificación de la información.		
	8.2.1 Directrices de clasificación.	Si	Directiva de TI y seguridad de la información.
	8.2.2 Etiquetado y manipulado de la información.	Si	Directiva de TI y seguridad de la información.
	8.2.3 Manipulación de activos.	Si	Directiva de TI y seguridad de la información.
	8.3 Manejo de los soportes de almacenamiento.		
	8.3.1 Gestión de soportes extraíbles.	Si	Directiva de TI y seguridad de la información.
	8.3.2 Eliminación de soportes.	Si	Directiva de TI y seguridad de la información.
	8.3.3 Soportes físicos en tránsito.	Si	Directiva de TI y seguridad de la información.
A.09 Control de Acceso.			
	9.1 Requisitos de negocio para el control de accesos.		
	9.1.1 Política de control de accesos.	Si	Documento de gestión de accesos.
	9.1.2 Control de acceso a las redes y servicios asociados.	Si	Documento de gestión de accesos.
	9.2 Gestión de acceso de usuario.		
	9.2.1 Gestión de altas/bajas en el registro de usuarios.	Si	Documento de gestión de accesos.
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Si	Documento de gestión de accesos.
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Si	Documento de gestión de accesos.
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Si	Documento de gestión de accesos.
	9.2.5 Revisión de los derechos de acceso de los usuarios.	Si	Documento de gestión de accesos.

	9.2.6 Retirada o adaptación de los derechos de acceso	Si	Documento de gestión de accesos.
	9.3 Responsabilidades del usuario.		
	9.3.1 Uso de información confidencial para la autenticación.	Si	Acuerdo de confidencialidad.
	9.4 Control de acceso a sistemas y aplicaciones.		
	9.4.1 Restricción del acceso a la información.	Si	Documento de gestión de accesos.
	9.4.2 Procedimientos seguros de inicio de sesión.	Si	Documento de gestión de accesos.
	9.4.3 Gestión de contraseñas de usuario.	Si	Documento de gestión de accesos.
	9.4.4 Uso de herramientas de administración de sistemas.	Si	Directiva de TI y seguridad de la información.
	9.4.5 Control de acceso al código fuente de los programas.	Si	Documento de gestión de accesos.
A.10 Criptografía.			
	10.1 Controles criptográficos.		
	10.1.1 Política de uso de los controles criptográficos.	Si	Política de seguridad de la información
	10.1.2 Gestión de claves	Si	Política de seguridad de la información
A.11 Seguridad Física y Ambiental.			
	11.1 Áreas seguras.		
	11.1.1 Perímetro de seguridad física.	Si	Data center, instalaciones y perímetros de seguridad física.
	11.1.2 Controles físicos de entrada.	Si	Personal de vigilancia.
	11.1.3 Seguridad de oficinas, despachos y recursos.	Si	Gestión de accesos físicos.
	11.1.4 Protección contra las amenazas externas y ambientales.	Si	Data center, instalaciones y perímetros de seguridad física
	11.1.5 El trabajo en áreas seguras.	Si	Data center, instalaciones y perímetros de seguridad física
	11.1.6 Áreas de acceso público, carga y descarga.	Si	Data center, instalaciones y perímetros de seguridad física
	11.2 Seguridad de los equipos.		
	11.2.1 Emplazamiento y protección de equipos.	Si	Directiva de TI y seguridad de la información.
	11.2.2 Instalaciones de suministro.	Si	Herramientas de soporte.
	11.2.3 Seguridad del cableado.	Si	Cableado estructurado y equipos de redes y comunicaciones
	11.2.4 Mantenimiento de los equipos.	Si	Directiva de TI y seguridad de la información.
	11.2.5 Salida de activos fuera de las dependencias de la empresa.	Si	Directiva de TI y seguridad de la información.

	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Si	Directiva de TI y seguridad de la información.
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Si	Directiva de TI y seguridad de la información.
	11.2.8 Equipo informático de usuario desatendido.	Si	Directiva de TI y seguridad de la información.
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Si	Política de seguridad de la información.
A.12 Seguridad de las Operaciones.			
	12.1 Responsabilidades y procedimientos de operación.		
	12.1.1 Documentación de procedimientos de operación.	Si	Equipos ubicados bajo instalaciones protegidas.
	12.1.2 Gestión de cambios.	Si	Directiva de TI y seguridad de la información.
	12.1.3 Gestión de capacidades.	Si	Directiva de TI y seguridad de la información.
	12.1.4 Separación de entornos de desarrollo, prueba y producción.	Si	Directiva de TI y seguridad de la información.
	12.2 Protección contra código malicioso.		
	12.2.1 Controles contra el código malicioso.	Si	Directiva de TI y seguridad de la información.
	12.3 Copias de seguridad.		
	12.3.1 Copias de seguridad de la información.	Si	Política de seguridad de la información.
	12.4 Registro de actividad y supervisión.		
	12.4.1 Registro y gestión de eventos de actividad.	Si	Auditoria de eventos.
	12.4.2 Protección de los registros de información.	Si	Ejecución de copias de seguridad.
	12.4.3 Registros de actividad del administrador y operador del sistema.	Si	Auditoria de eventos.
	12.4.4 Sincronización de relojes.	Si	Sincronización de relojes de los activos de información.
	12.5 Control del software en explotación.		
	12.5.1 Instalación del software en sistemas en producción.	Si	Directiva de TI y seguridad de la información.
	12.6 Gestión de la vulnerabilidad técnica.		
	12.6.1 Gestión de las vulnerabilidades técnicas.	Si	Actualización de software y gestión de riesgos.
	12.6.2 Restricciones en la instalación de software.	Si	Directiva de TI y seguridad de la información.

	12.7 Consideraciones de las auditorías de los sistemas de información.		
	12.7.1 Controles de auditoría de los sistemas de información.	Si	Auditoria de eventos.
A.13 Seguridad de las Comunicaciones.			
	13.1 Gestión de la seguridad en las redes.		
	13.1.1 Controles de red.	Si	Seguridad tecnológica perimetral.
	13.1.2 Mecanismos de seguridad asociados a servicios en red.	Si	Gestión de control de accesos.
	13.1.3 Segregación de redes.	Si	Segmentación de redes VLAN
	13.2 Intercambio de información con partes externas.		
	13.2.1 Políticas y procedimientos de intercambio de información.	No	
	13.2.2 Acuerdos de intercambio.	No	
	13.2.3 Mensajería electrónica.	No	
	13.2.4 Acuerdos de confidencialidad y secreto.	No	
A.14 Adquisición, desarrollo y mantenimiento de sistemas.			
	14.1 Requisitos de seguridad de los sistemas de información.		
	14.1.1 Análisis y especificación de los requisitos de seguridad.	Si	Seguridad perimetral.
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	Si	Seguridad perimetral.
	14.1.3 Protección de las transacciones por redes telemáticas.	Si	Seguridad perimetral.
	14.2 Seguridad en los procesos de desarrollo y soporte.		
	14.2.1 Política de desarrollo seguro de software.	Si	Política de seguridad de la información.

	14.2.2 Procedimientos de control de cambios en los sistemas.	Si	Política de seguridad de la información.
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Si	Política de seguridad de la información.
	14.2.4 Restricciones a los cambios en los paquetes de software.	Si	Política de seguridad de la información.
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	Si	Política de seguridad de la información.
	14.2.6 Seguridad en entornos de desarrollo.	Si	Política de seguridad de la información.
	14.2.7 Externalización del desarrollo de software.	Si	Política de seguridad de la información.
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	Si	Política de seguridad de la información.
	14.2.9 Pruebas de aceptación.	Si	Política de seguridad de la información.
	14.3 Datos de prueba.		
	14.3.1 Protección de los datos utilizados en pruebas.	Si	Política de seguridad de la información.
A.15 Relaciones con los proveedores.			
	15.1 Seguridad de la información en las relaciones con suministradores.		
	15.1.1 Política de seguridad de la información para suministradores.	Si	Política de seguridad de la información.
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	Si	Contrato de servicios.
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	Si	Contrato de servicios
	15.2 Gestión de la prestación del servicio por suministradores.		
	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Si	Informe mensual de servicio.
	15.2.2 Gestión de cambios en los servicios prestados por terceros.	Si	Gestión de cambios.

A.16 Gestión de incidentes de seguridad de la información.		
16.1 Gestión de incidentes de seguridad de la información y mejoras.		
16.1.1 Responsabilidades y procedimientos.	Si	Gestión de incidentes de seguridad de la información
16.1.2 Notificación de los eventos de seguridad de la información.	Si	Gestión de incidentes de seguridad de la información
16.1.3 Notificación de puntos débiles de la seguridad.	Si	Gestión de incidentes de seguridad de la información
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	Si	Gestión de incidentes de seguridad de la información
16.1.5 Respuesta a los incidentes de seguridad.	Si	Gestión de incidentes de seguridad de la información
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	Si	Gestión de incidentes de seguridad de la información
16.1.7 Recopilación de evidencias.	Si	Gestión de incidentes de seguridad de la información
A.17 Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio		
17.1 Continuidad de la seguridad de la información.		
17.1.1 Planificación de la continuidad de la seguridad de la información.	Si	Plan de contingencia.
17.1.2 Implantación de la continuidad de la seguridad de la información.	Si	Plan de contingencia.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Si	Informe de pruebas de contingencia.
17.2 Redundancias.		
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	Si	Centro de datos.
A.18 Cumplimiento.		
18.1 Cumplimiento de los requisitos legales y contractuales.		
18.1.1 Identificación de la legislación aplicable.	Si	Leyes peruanas.

	18.1.2 Derechos de propiedad intelectual (DPI).	Si	Directiva de TI y seguridad de la información.
	18.1.3 Protección de los registros de la organización.	Si	Control de documentos.
	18.1.4 Protección de datos y privacidad de la información personal.	Si	
	18.1.5 Regulación de los controles criptográficos.	Si	Directiva de TI y seguridad de la información.
	18.2 Revisiones de la seguridad de la información.		
	18.2.1 Revisión independiente de la seguridad de la información.	Si	Auditoría interna.
	18.2.2 Cumplimiento de las políticas y normas de seguridad.	Si	Medición del SGSI
	18.2.3 Comprobación del cumplimiento.	Si	Informes

Fuente: Elaboración Propia

En la tabla 7 se realizaron la selección de controles y la declaración de aplicabilidad de la misma manera se describen los controles que se llevaran a cabo los mismos que pueden estar basados en documentos o controles físicos o virtuales.

4.1.6.7. Gestión de continuidad de negocio.

- **Planificación de continuidad de negocio.** La continuidad de la seguridad de la información tiene como objetivo asegurar la disponibilidad y continuidad de los procesos institucionales, los mismos que estarán establecidos mediante planes que incluirán los procesos mencionados con la finalidad de mantener la seguridad de la información.
- **Implementación de continuidad de negocio.** En el siguiente proceso la institución deberá de establecer y realizar el cumplimiento de los planes de continuidad de negocio, los mismo que se activaran en el proceso de incidentes de disponibilidad relacionados a la continuidad del negocio.
- **Verificación, revisión y evaluación de la continuidad de negocio.** Los planes de continuidad del negocio se deberán de verificar, revisar y evaluar con la finalidad de tener plan robusto el mismo que será encargado como actividad y responsabilidad del comité de gobierno digital; posterior a ello el área usuaria deberá de realizar las pruebas de continuidad de negocio con la finalidad de evaluar los resultados.
- **Disponibilidad de las instalaciones de procesamiento de la información.** Las instalaciones del centro de datos del Gobierno Regional Pasco, cuentan con redundancia eléctrica y tecnológica con la finalidad de tener disponibilidad ante casos de emergencia.

4.1.6.8. Gestión de cambios.

Los cambios realizados en la organización se deberán de administrar debidamente con la finalidad de garantizar que el sistema de

gestión de seguridad de la información mantenga su validez respecto a los pilares de la seguridad de la información.

De la misma manera se pueden identificar a los cambios que pueden representar la afectación en le sistema de gestión de seguridad de la información a:

- Revisión por parte de las gerencias.
- Auditoría interna.
- Mediciones de indicadores de éxito.
- Documentación.

La gestión de cambios contara con los siguientes procesos:

- **Evaluación de cambio.** El comité de transformación digital recepciona la solicitud de cambio para posteriormente evaluar la factibilidad del cambio. La misma que deberá contar con la siguiente estructura:
  - Finalidad del cambio.
  - Consecuencias positivas y negativas correspondientes al cambio.
  - Control del cambio.
  - Recursos requeridos para el cambio.
  - Definición de responsabilidades y autoridades.
- **Implementación de cambio.** Posterior a la aceptación del cambio por parte del comité de transformación digital se deberá de implementar sin afectar el transcurso del sistema de gestión de seguridad de la información.
- **Seguimiento del cambio.** El líder de implementación encargado del sistema de gestión de seguridad de la información deberá hacer el

seguimiento del cambio, de la misma manera se deberá de informar el estado de implementación al comité de transformación digital.

4.1.6.9. Gestión de incidentes de seguridad de la información.

La presente gestión tendrá como objetivo brindar una respuesta rápida ante posibles incidentes de seguridad de la información. Es por ello que el comité de transformación digital realiza el seguimiento y control; de la misma manera realiza la toma de decisiones respecto a los incidentes.

- **Responsabilidades.**

  Las responsabilidades con respecto a la gestión de incidentes estarán lideradas por el responsable del SGSI, se deberá de asegurar la respuesta rápida de los eventos; deberán de tener contemplar acciones disciplinarias si los el caso lo requiera. Se deberán de gestionar adecuadamente la información recopilada a partir del suceso de un incidente.

  De la misma manera el oficial de seguridad digital es el responsable del análisis de alcance de los incidentes de seguridad de la información, en coordinación con las áreas interesadas. De la misma manera es la persona quien informará acerca de los incidentes al comité de transformación digital.

- **Eventos de seguridad de la información.** Los eventos de seguridad de la información pueden ser, pero no se limitan a los siguientes puntos.
  - Detección de un error en la aplicación.
  - Conexión fallida de un usuario.
  - Conexiones al sistema de seguridad perimetral.

- Notificación de cambio de contraseña de usuarios con privilegios.
- Accesos físicos abiertos.
- Publicación de información sensible.
- Entre otros.

- **Incidentes de seguridad de la información.** El presente apartado presenta los incidentes de seguridad de la información, los mismos que pueden ser:
  - Acceso no autorizado a activos de seguridad de la información.
  - Alteración de los activos de seguridad de la información.
  - Divulgación de información sensible o no autorizada.
  - Interrupciones de disponibilidad de la información.
  - Perdida de los activos de seguridad de la información.
  - Ataque físico e informático.
  - Entre otras.
- **Informe de eventos de seguridad de la información.**

  Los eventos de seguridad de la información suscitados en la institución deberán de ser comunicados lo más pronto posible a los encargados para el tratamiento del incidente indistintamente de la procedencia o canal afectado.

- **Aprendizaje de los incidentes de seguridad de la información.**

Las aplicaciones de solución a incidentes deberán de ser de documentadas mediante buenas prácticas, las mismas que se comunicarán a todo el personal de involucrado con la finalidad de tener antecedentes en futuros incidentes de seguridad de la información.

4.1.6.10. Gestión de competencias y conocimientos.

El personal participante del proyecto de implementación del sistema de gestión de seguridad de la información deberá de ser multidisciplinario y de la misma manera tener conocimientos en la norma ISO 27001, COBIT 5, NIST, ISO 31000, entre otras buenas prácticas o normas para la gestión de seguridad de la información.

4.1.7. Implementación.

4.1.7.1. Inventario de activos.

En el presente proceso se identifican los activos de información; detallándolos con la finalidad de conocer toda la información relevante para el proyecto. Los mismos que se dividen en ítem, nombre del activo, descripción del activo, tipo del activo, categoría del activo, propietario del activo, clasificación de la información, ubicación del activo y la valoración del activo. Todo lo descrito se presenta en la siguiente tabla.

Tabla 10. *Inventario de activos.*

ITEM	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO	CATEGORÍA DE ACTIVO	PROPIETARIO DEL ACTIVO	CLASIFICACIÓN DE INFORMACIÓN	UBICACIÓN ESPECÏFICA	VALORACIÓN DEL ACTIVO
1	SRV-SIAF	SO. Windows Server 2008 Marca: HPE Proliant Modelo: DL380 G7	HARDWARE	SERVIDOR	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
2	SRV-SIGA	SO. Windows Server 2008 Marca: HPE Proliant Modelo: DL380 G7	HARDWARE	SERVIDOR	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
3	SRV-SIGAWEB	SO. Windows Server 2012 Marca: HPE Proliant Modelo: DL380 G7	HARDWARE	SERVIDOR	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
4	SRV-WEB	SO. Windows Server 2012 Marca: HPE Proliant Modelo: DL380 G7	HARDWARE	SERVIDOR	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
5	SRV-SISGEDO	SO. Windows Server 2012 Marca: HPE Proliant Modelo: DL380 G7	HARDWARE	SERVIDOR	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
6	SRV-DOMINIO	SO. Windows Server 2012 Marca: HPE Proliant Modelo: DL380 G7	HARDWARE	SERVIDOR	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5

7	SRV-VM	SO. Windows Server 2012 Marca: HPE Proliant Modelo: DL380 G7	HARDWARE	SERVIDOR	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	4
8	APLICACIONES PRINCIPALES DEL GOBIERNO REGIONAL PASCO	Servicios principales almacenados en el centro de datos del Gobierno Regional Pasco.	SOFTWARE	SERVICIOS INFORMÁTICOS	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
9	APLICACIONES DEL GOBIERNO REGIONAL PASCO	Servicios que no son principales, almacenados en el centro de datos del Gobierno Regional Pasco.	SOFTWARE	SERVICIOS INFORMÁTICOS	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	4
10	SISTEMAS OPERATIVOS MICRSOFOT	Sistemas operativos que soportan los servicios de los servidores institucionales.	SOFTWARE	SERVICIOS INFORMÁTICOS	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
11	SISTEMAS OPERATIVOS LINUX	Sistemas operativos que soportan los servicios de los servidores institucionales.	SOFTWARE	SERVICIOS INFORMÁTICOS	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
12	STORAGE BOX	Administrador SAN de almacenamiento	HARDWARE	SERVIDOR	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5

13	DB_SIAF	Base de datos administrador por la aplicación SIAF	DATOS E INFORMACIÓN	BASE DE DATOS	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
14	DB_SIGA	Base de datos administrador por la aplicación SIGA	DATOS E INFORMACIÓN	BASE DE DATOS	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
15	DB_SISGEDO	Base de datos administrador por la aplicación SISGEDO	DATOS E INFORMACIÓN	BASE DE DATOS	SGRSTIC / Ingeniero de Seguridad informática	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
16	DB_WEB	Base de datos administrador por la página web	DATOS E INFORMACIÓN	BASE DE DATOS	SGRSTIC / Administrador web	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
17	SWITCH DE RED	equipos de red que distribuyen la conectividad mediante un cableado estructurado	REDES Y COMUNICACIONES	REDES Y COMUNICACIONES	SGRSTIC / Jefe de Redes y Comunicaciones	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
18	FIREWALL	Equipo de seguridad perimetral que ayuda a la seguridad informática.	REDES Y COMUNICACIONES	REDES Y COMUNICACIONES	SGRSTIC / Jefe de Redes y Comunicaciones	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5

19	SWITCH CORE	Equipo de red principal que tiene como objetivo una mejor administración de red.	REDES Y COMUNICACIONES	REDES Y COMUNICACIONES	SGRSTIC / Jefe de Redes y Comunicaciones	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
20	ACCESS POINT	Equipo de red que brinda conectividad inalámbrica.	REDES Y COMUNICACIONES	REDES Y COMUNICACIONES	SGRSTIC / Jefe de Redes y Comunicaciones	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
21	TELEFONIA IP	Equipos de intercomunicaciones.	REDES Y COMUNICACIONES	REDES Y COMUNICACIONES	SGRSTIC / Jefe de Redes y Comunicaciones	RESTRINGIDO	Centro de datos / Sede Antigua del GRP	5
21	JEFE DE SOPORTE TECNICO	Responsable del área de soporte técnico e informático	PERSONAL	PERSONAL	SGRSTIC	RESTRINGIDO	SGRSTIC	4
21	JEFE DE REDES Y COMUNICACIONES	Responsable del área de redes y comunicaciones	PERSONAL	PERSONAL	SGRSTIC	RESTRINGIDO	SGRSTIC	4
21	WEB MASTER	Responsable de la administración del portal institucional.	PERSONAL	PERSONAL	SGRSTIC	RESTRINGIDO	SGRSTIC	4
21	INGENIERO DE SEGURIDAD INFORMATICA	Responsable de la seguridad informática de la institución.	PERSONAL	PERSONAL	SGRSTIC	RESTRINGIDO	SGRSTIC	4
21	INGENIERO I	Jefe directo de la unidad de TIC	PERSONAL	PERSONAL	SGRSTIC	RESTRINGIDO	SGRSTIC	4

Fuente: Elaboración Propia.

4.1.7.2. Evaluación de riesgos.

Para la evaluación de los riesgos se tomaron en cuenta los aspectos de datos e información, sistemas e infraestructura y personas los mismas que se interrelacionan con los Actos originados por la criminalidad común y motivación política, Sucesos de origen físico, Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales los mismos que se presentan en las siguientes tablas:

- **Datos e información - Actos originados por la criminalidad común y motivación política.**

Tabla 11. *Evaluación de riesgos de Datos e información - Actos originados por la criminalidad común y motivación política.*

Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política												
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo (físico)	Robo de información electrónica	Intrusión a Red interna	Infiltración	Malware / Ejecución no autorizado de programas	Violación a derechos de autor
					2	2	1	4	2	2	2	2	4	4	4	3	4
PLAN ESTRATEGICO INSTITUCIONAL		x		2	4	4	2	8	4	4	4	4	8	8	8	6	8
PROGRAMACIÓN ECONÓMICA		x		2	4	4	2	8	4	4	4	4	8	8	8	6	8
PLAN OPERATIVO INSTITUCIONAL		x		2	4	4	2	8	4	4	4	4	8	8	8	6	8

ORDEN DE SERVICIO		x		**2**	4	4	2	8	4	4	4	4	8	8	8	6	8
DOCUMENTOS DE GESTIÓN INSTITUCIONAL		x		**2**	4	4	2	8	4	4	4	4	8	8	8	6	8
INFORMACIÓN CONTABLE Y PLANILLAS	x			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16
BOLETAS DE DEVENGADO	x			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16
INFORMACIÓN DE PERSONAL	x			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16
DIRECTORIO DE CONTACTOS	x			**3**	6	6	3	12	6	6	6	6	12	12	12	9	12
MOF Y ROF		x		**2**	4	4	2	8	4	4	4	4	8	8	8	6	8
TUPA		x		**2**	4	4	2	8	4	4	4	4	8	8	8	6	8
BASE DE DATOS INTERNAS	x			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16
BASE DE DATOS COLABORATIVAS	x			**3**	6	6	3	12	6	6	6	6	12	12	12	9	12
PORTAL WEB		X		**3**	6	6	3	12	6	6	6	6	12	12	12	9	12

COPIAS DE SEGURIDAD	**x**			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16
INFRAESTRUCTURA TECNOLOGICA (PLANES, DOCUMNETACIÓN DOCUMENTOS CONFIDENCIALES, ETC)	**x**			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16
INFORMATICA (PLANES, DOCUMNETACIÓN DOCUMENTOS CONFIDENCIALES, ETC)	**x**			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16
BASE DE DATOS DE CONTRASEÑAS	**x**			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16
MENSAJERIA INTERNA	**x**			**3**	6	6	3	12	6	6	6	6	12	12	12	9	12
MENSAJERIA EXTERNA	**x**			**3**	6	6	3	12	6	6	6	6	12	12	12	9	12
COMUNICACIÓN POR VOZ INTERNA	**x**			**2**	4	4	2	8	4	4	4	4	8	8	8	6	8
COMUNICACIÓN POR VOZ EXTERNA	**x**			**4**	8	8	4	16	8	8	8	8	16	16	16	12	16

Fuente: Elaboración Propia.

- **Datos e información - Sucesos de origen físico.**

Tabla 12. *Evaluación de riesgos de Datos e información - Sucesos de origen físico.*

Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos de origen físico								
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	1	2	4	3	3	4	4	4
PLAN ESTRATEGICO INSTITUCIONAL		x		2	4	2	4	8	6	6	8	8	8
PROGRAMACIÓN ECONÓMICA		x		2	4	2	4	8	6	6	8	8	8
PLAN OPERATIVO INSTITUCIONAL		x		2	4	2	4	8	6	6	8	8	8

ORDEN DE SERVICIO		x		2	4	2	4	8	6	6	8	8	8
DOCUMENTOS DE GESTIÓN INSTITUCIONAL		x		2	4	2	4	8	6	6	8	8	8
INFORMACIÓN CONTABLE Y PLANILLAS	X			4	8	4	8	16	12	12	16	16	16
BOLETAS DE DEVENGADO	X			4	8	4	8	16	12	12	16	16	16
INFORMACIÓN DE PERSONAL	X			4	8	4	8	16	12	12	16	16	16
DIRECTORIO DE CONTACTOS	X			3	6	3	6	12	9	9	12	12	12
MOF Y ROF		x		2	4	2	4	8	6	6	8	8	8
TUPA		x		2	4	2	4	8	6	6	8	8	8
BASE DE DATOS INTERNAS	X			4	8	4	8	16	12	12	16	16	16
BASE DE DATOS COLABORATIVAS	X			3	6	3	6	12	9	9	12	12	12
PORTAL WEB		x		3	6	3	6	12	9	9	12	12	12

COPIAS DE SEGURIDAD	**X**			**4**	8	4	8	16	12	12	16	16	16
INFRAESTRUCTURA TECNOLOGICA (PLANES, DOCUMNETACIÓN DOCUMENTOS CONFIDENCIALES, ETC)	**X**			**4**	8	4	8	16	12	12	16	16	16
INFORMATICA (PLANES, DOCUMNETACIÓN DOCUMENTOS CONFIDENCIALES, ETC)	**X**			**4**	8	4	8	16	12	12	16	16	16
BASE DE DATOS DE CONTRASEÑAS	**X**			**4**	8	4	8	16	12	12	16	16	16
MENSAJERIA INTERNA	**X**			**3**	6	3	6	12	9	9	12	12	12
MENSAJERIA EXTERNA	**X**			**3**	6	3	6	12	9	9	12	12	12
COMUNICACIÓN POR VOZ INTERNA	**X**			**2**	4	2	4	8	6	6	8	8	8
COMUNICACIÓN POR VOZ EXTERNA	**X**			**4**	8	4	8	16	12	12	16	16	16

Fuente: Elaboración Propia.

- **Datos e información - Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales**.

Tabla 13. *Evaluación de riesgos de Datos e información - Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.*

Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																								
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Falta de inducción, capacitación y	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados /	Falta de pruebas de software nuevo con datos	Perdida de datos	Infección de sistemas a través de unidades	Manejo inadecuado de datos críticos (codificar,	Unidades portables con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (inseguras,	Compartir contraseñas o permisos a terceros	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades de	Sobrepasar autoridades	Falta de definición de perfil, privilegios y	Falta de mantenimiento físico (proceso,	Falta de actualización de software (proceso y	Fallas en permisos de usuarios (acceso a	Acceso electrónico no autorizado a sistemas	Acceso electrónico no autorizado a sistemas	Red cableada expuesta para el acceso no	Red inalámbrica expuesta al acceso no	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no	Falta de mecanismos de verificación de normas	Ausencia de documentación
					4	4	4	4	3	3	4	4	3	4	4	4	2	2	4	4	4	4	3	3	3	4	1	4	4	4
PLAN ESTRATEGICO INSTITUCIONAL		x		2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
PROGRAMACIÓN ECONÓMICA		x		2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8

PLAN OPERATIVO INSTITUCIONAL		x		2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
ORDEN DE SERVICIO		x		2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
DOCUMENTOS DE GESTIÓN INSTITUCIONAL		x		2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
INFORMACIÓN CONTABLE Y PLANILLAS	X			4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
BOLETAS DE DEVENGADO	X			4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
INFORMACIÓN DE PERSONAL	X			4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
DIRECTORIO DE CONTACTOS	X			3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
MOF Y ROF		x		2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
TUPA		x		2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
BASE DE DATOS INTERNAS	X			4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
BASE DE DATOS COLABORATIVAS	X			3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12

PORTAL WEB		x		**3**	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
COPIAS DE SEGURIDAD	X			**4**	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
INFRAESTRUCTURA TECNOLOGICA (PLANES, DOCUMNETACIÓN DOCUMENTOS CONFIDENCIALES, ETC)	x			**4**	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
INFORMATICA (PLANES, DOCUMNETACIÓN DOCUMENTOS CONFIDENCIALES, ETC)	X			**4**	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
BASE DE DATOS DE CONTRASEÑAS	X			**4**	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
MENSAJERIA INTERNA	X			**3**	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
MENSAJERIA EXTERNA	X			**3**	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
COMUNICACIÓN POR VOZ INTERNA	X			**2**	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
COMUNICACIÓN POR VOZ EXTERNA	X			**4**	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16

Fuente: Elaboración Propia.

- **Sistemas e infraestructura - Actos originados por la criminalidad común y motivación política.**

Tabla 14. *Evaluación de riesgos de Sistemas e infraestructura - Actos originados por la criminalidad común y motivación política.*

Sistemas e Infraestructura	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política												
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo (físico)	Robo de información electrónica	Intrusión a Red interna	Infiltración	Malware / Ejecución no autorizado de programas	Violación a derechos de autor
					2	2	1	4	2	2	2	2	4	4	4	3	4
Equipos de redes y telecomunicaciones cableadas (router, switch, etc.)	X			4	8	8	4	16	8	8	8	8	16	16	16	12	16
Equipos de la redes y telecomunicaciones inalámbrica (router, punto de acceso, etc.)	X			3	6	6	3	12	6	6	6	6	12	12	12	9	12

Infraestructura (Centro de datos.)		x		1	2	2	1	4	2	2	2	2	4	4	4	3	4
Servidores			x	4	8	8	4	16	8	8	8	8	16	16	16	12	16
Computadoras	X			3	6	6	3	12	6	6	6	6	12	12	12	9	12
Portátiles	X			2	4	4	2	8	4	4	4	4	8	8	8	6	8
Sistema de administración Financiera (SIAF)	X			4	8	8	4	16	8	8	8	8	16	16	16	12	16
Sistema de gestión administrativa (SIGA)		x		4	8	8	4	16	8	8	8	8	16	16	16	12	16
Sistema de gestión documental (SISGEDO)	X			4	8	8	4	16	8	8	8	8	16	16	16	12	16
Aplicaciones intitucionales (mesa de partes virtual, catalago de normas, etc.)				3	6	6	3	12	6	6	6	6	12	12	12	9	12
Servidor DNS				3	6	6	3	12	6	6	6	6	12	12	12	9	12
Dominio				3	6	6	3	12	6	6	6	6	12	12	12	9	12
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	X			3	6	6	3	12	6	6	6	6	12	12	12	9	12

Impresoras	X			2	4	4	2	8	4	4	4	4	8	8	8	6	8
Celulares	X			1	2	2	1	4	2	2	2	2	4	4	4	3	4
Telefonia IP	X			1	2	2	1	4	2	2	2	2	4	4	4	3	4

Fuente: Elaboración Propia.

- **Sistemas e infraestructura - Sucesos de origen físico.**

Tabla 15. *Evaluación de riesgos de Sistemas e infraestructura - Sucesos de origen físico.*

Sistemas e Infraestructura	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos de origen físico								
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	1	2	4	3	3	4	4	4
Equipos de redes y telecomunicaciones cableadas (router, switch, etc.)	x			4	8	4	8	16	12	12	16	16	16
Equipos de la redes y telecomunicaciones inalámbrica (router, punto de acceso, etc.)	x			3	6	3	6	12	9	9	12	12	12
Infraestructura (Centro de datos.)		x		1	2	1	2	4	3	3	4	4	4

Servidores			x	4	8	4	8	16	12	12	16	16	16
Computadoras	x			3	6	3	6	12	9	9	12	12	12
Portátiles	x			2	4	2	4	8	6	6	8	8	8
Sistema de administración Financiera (SIAF)	x			4	8	4	8	16	12	12	16	16	16
Sistema de gestión administrativa (SIGA)		x		4	8	4	8	16	12	12	16	16	16
Sistema de gestión documental (SISGEDO)	x			4	8	4	8	16	12	12	16	16	16
Aplicaciones intitucionales (mesa de partes virtual, catalago de normas, etc.)				3	6	3	6	12	9	9	12	12	12
Servidor DNS				3	6	3	6	12	9	9	12	12	12
Dominio				3	6	3	6	12	9	9	12	12	12
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	X			3	6	3	6	12	9	9	12	12	12
Impresoras	X			2	4	2	4	8	6	6	8	8	8

Celulares	X			1	2	1	2	4	3	3	4	4	4
Telefonia IP	X			1	2	1	2	4	3	3	4	4	4

Fuente: Elaboración Propia.

- **Sistemas e infraestructura - Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.**

Tabla 16. *Evaluación de riesgos de Sistemas e infraestructura - Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.*

Sistemas e Infraestructura	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																						
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Falta de inducción, capacitación y	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados /	Falta de pruebas de software nuevo con	Perdida de datos	Infección de sistemas a través de	Manejo inadecuado de datos críticos	Unidades portables con información sin	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas	Compartir contraseñas o permisos a	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades	Sobrepasar autoridades	Falta de definición de perfil, privilegios y	Falta de mantenimiento físico (proceso,	Falta de actualización de software	Fallas en permisos de usuarios (acceso a	Acceso electrónico no autorizado a	Acceso electrónico no autorizado a	Red cableada expuesta para el acceso no	Red inalámbrica expuesta al acceso no	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no	Falta de mecanismos de verificación de	Ausencia de documentación

					4	4	4	4	3	3	4	4	3	4	4	4	2	2	4	4	4	4	3	3	3	4	1	4	4	4
Equipos de redes y telecomunicaciones cableadas (router, switch, etc.)	x			4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
Equipos de la redes y telecomunicaciones inalámbrica (router, punto de acceso, etc.)	x			3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Infraestructura (Centro de datos.)		x		1	4	4	4	4	3	3	4	4	3	4	4	4	2	2	4	4	4	4	3	3	3	4	1	4	4	4
Servidores			x	4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
Computadoras	x			3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Portátiles	x			2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
Sistema de administración Financiera (SIAF)	x			4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
Sistema de gestión administrativa (SIGA)		x		4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
Sistema de gestión documental (SISGEDO)	x			4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16

Aplicaciones intitucionales (mesa de partes virtual, catalago de normas, etc.)				3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Servidor DNS				3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Dominio				3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x			3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Impresoras	x			2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
Celulares	x			1	4	4	4	4	3	3	4	4	3	4	4	4	2	2	4	4	4	4	3	3	3	4	1	4	4	4
Telefonia IP	x			1	4	4	4	4	3	3	4	4	3	4	4	4	2	2	4	4	4	4	3	3	3	4	1	4	4	4

Fuente: Elaboración Propia.

- **Personal - Actos originados por la criminalidad común y motivación política.**

Tabla 17. *Evaluación de riesgos de Personal - Actos originados por la criminalidad común y motivación política.*

Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política												
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo (físico)	Robo de información electrónica	Intrusión a Red interna	Infiltración	Malware / Ejecución no autorizado de programas	Violación a derechos de autor
					2	2	1	4	2	2	2	2	4	4	4	3	4
Consejo Regional	X			3	6	6	3	12	6	6	6	6	12	12	12	9	12
Gerencia General	X			3	6	6	3	12	6	6	6	6	12	12	12	9	12
Direcciones (Contabilidad, RRHH, Abasteciminetos, TIC, entre otros)	X			3	6	6	3	12	6	6	6	6	12	12	12	9	12

Funcionarios Públicos.		x		3	6	6	3	12	6	6	6	6	12	12	12	9	12
Mesa de Partes		x		2	4	4	2	8	4	4	4	4	8	8	8	6	8
SGRSTIC (Jefe de soporte técnico, Redes y Comuncaciones, web master, seguridad informatica)		X		4	8	8	4	16	8	8	8	8	16	16	16	12	16
Sub Gerentes, Directores, Gerentes		X		3	6	6	3	12	6	6	6	6	12	12	12	9	12
Servicio de limpieza		X		3	6	6	3	12	6	6	6	6	12	12	12	9	12

Fuente: Elaboración Propia.

- **Personal - Sucesos de origen físico.**

Tabla 18. *Evaluación de riesgos de Personal - Sucesos de origen físico.*

Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos de origen físico								
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	1	2	4	3	3	4	4	4
Consejo Regional	X			3	6	3	6	12	9	9	12	12	12
Gerencia General	X			3	6	3	6	12	9	9	12	12	12
Direcciones (Contabilidad, RRHH, Abasteciminetos, TIC, entre otros)	X			3	6	3	6	12	9	9	12	12	12

Funcionarios Públicos.		x		3	6	3	6	12	9	9	12	12	12
Mesa de Partes		x		2	4	2	4	8	6	6	8	8	8
SGRSTIC (Jefe de soporte técnico, Redes y Comuncaciones, web master, seguridad informatica)		x		4	8	4	8	16	12	12	16	16	16
Sub Gerentes, Directores, Gerentes		x		3	6	3	6	12	9	9	12	12	12
Servicio de limpieza		x		3	6	3	6	12	9	9	12	12	12

Fuente: Elaboración Propia.

- **Personal - Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.**

Tabla 19. *Evaluación de riesgos de Personal - Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales.*

Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																								
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Top Secret		Falta de inducción, capacitación y	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados /	Falta de pruebas de software nuevo con	Perdida de datos	Infección de sistemas a través de	Manejo inadecuado de datos críticos	Unidades portables con información sin	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas	Compartir contraseñas o permisos a	Transmisión de contraseñas por teléfono	Exposición o extravío de equipo, unidades	Sobrepasar autoridades	Falta de definición de perfil, privilegios y	Falta de mantenimiento físico (proceso,	Falta de actualización de software	Fallas en permisos de usuarios (acceso a	Acceso electrónico no autorizado a	Acceso electrónico no autorizado a	Red cableada expuesta para el acceso no	Red inalámbrica expuesta al acceso no	Dependencia a servicio técnico externo	Falta de normas y reglas claras (no	Falta de mecanismos de verificación de	Ausencia de documentación
					4	4	4	4	3	3	4	4	3	4	4	4	2	2	4	4	4	4	3	3	3	4	1	4	4	4
Consejo Regional	x			3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Gerencia General	x			3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Direcciones (Contabilidad, RRHH, Abasteciminet	x			3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12

os, TIC, entre otros)																																
Funcionarios Públicos.		x		3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Mesa de Partes		x		2	8	8	8	8	6	6	8	8	6	8	8	8	4	4	8	8	8	8	6	6	6	8	2	8	8	8
SGRSTIC (Jefe de soporte técnico, Redes y Comuncaciones, web master, seguridad informatica)		x		4	16	16	16	16	12	12	16	16	12	16	16	16	8	8	16	16	16	16	12	12	12	16	4	16	16	16
Sub Gerentes, Directores, Gerentes		x		3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12
Servicio de limpieza		x		3	12	12	12	12	9	9	12	12	9	12	12	12	6	6	12	12	12	12	9	9	9	12	3	12	12	12

Fuente: Elaboración Propia.

4.1.7.3. Análisis de riesgos.

Tabla 20. *Evaluación de riesgos de Personal*

Análisis de Riesgo promedio		Probabilidad de Amenaza		
		Criminalidad o Político	Sucesos de origen físico	Negligencia o Institucional
Magnitud de Daño	Datos e Información	8.4	9.1	10.7
	Sistemas e Infraestructura	6.6	7.1	8.3
	Personal	8.3	9.0	10.5

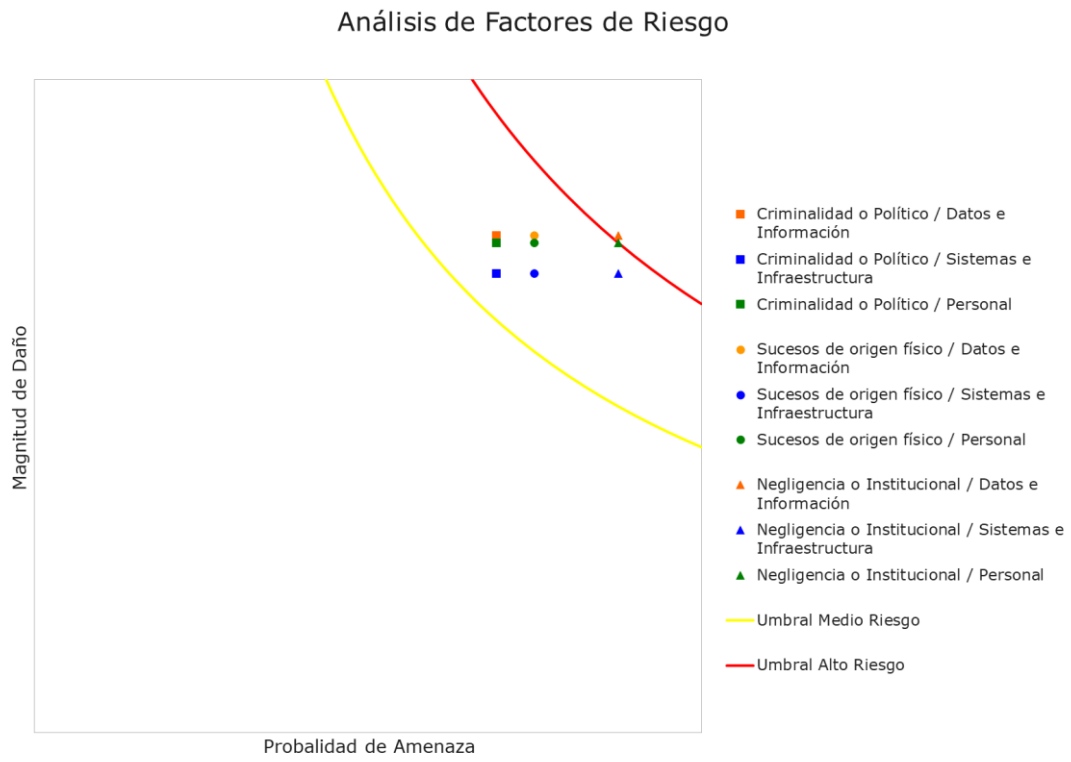
Fuente: Elaboración Propia.

Posterior a la realización de la evaluación de riesgos se obtuvieron los puntajes mostrados en la tabla 20, donde se pueden destacar los siguientes puntos:

- Con respecto al riesgo de datos e información los puntajes son elevados sobrepasando el umbral medio de riesgo en los puntos de criminalidad o político se obtiene un puntaje de 8.4 y para sucesos de origen físico 9.1; mientras que para negligencia o institucional supera el umbral de riesgo alto con un puntaje de 10.7.
- Para el criterio de sistemas e infraestructura las probabilidades de amenazas son menores que en el punto anterior obteniendo un umbral de riesgo bajo para la criminalidad o político; mientras que para sucesos de origen físico (7.1) y negligencia institucional (8.3) los mismos que se encuentran en el umbral medio de riesgo.
- Para el criterio de personal el umbral de riesgo obtenido es medio obteniendo para criminalidad o político una probabilidad de 8.3 para sucesos de origen físico 9.0 y para negligencia institucional 10.5 el mismo que se encuentra al borde del umbral de riesgo alto.

Los puntos explicados a continuación pueden observarse en mejor medida según clasificación de umbral de riesgo en la siguiente figura.

Figura 8. *Análisis de Factores.*



Fuente: Elaboración Propia

4.1.8. Verificación.

4.1.8.1. Medición del sistema de gestión de seguridad de la información.

En el siguiente apartado se presentan la medición del SGSI los mismos que son evaluados de acuerdo a los dominios y controles propuestos por el SoA o la declaración de aplicabilidad.

Tabla 21. *Diagnóstico inicial de los controles basados en la NTP ISO/IEC 27001:2014.*

Controles	Control	Método de medición	Indicador	Responsable de medición	Nivel alcanzado
A.05 Política de Seguridad de la Información.					
5.1. Directrices de la Dirección en seguridad de la información.					
5.1.1 Conjunto de políticas para la seguridad de la información.	Política de seguridad de la información	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	4
5.1.2 Revisión de las políticas para la seguridad de la información	Política de seguridad de la información	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	4
A.06 Organización de la Seguridad de la Información.					
6.1 Organización interna.					
6.1.1 Asignación de responsabilidades para la seguridad de la información.	Manual de organizaciones y funciones (MOF)	Verificación de cumplimiento del MOF	% de cumplimiento del MOF	Oficial de seguridad digital	4

	6.1.2 Segregación de tareas.	Manual de organizaciones y funciones (MOF)	Verificación de cumplimiento del MOF	% de cumplimiento del MOF	Oficial de seguridad digital	4
	6.1.3 Contacto con las autoridades.	Directorio de contactos.	Verificación de cumplimiento de seguridad en el directorio de contactos	N° de directorios de contactos	Oficial de seguridad digital	3
	6.1.4 Contacto con grupos de interés especial.	Directorio de contactos.	Verificación de cumplimiento de seguridad en el directorio de contactos	N° de directorios de contactos	Oficial de seguridad digital	3
	6.1.5 Seguridad de la información en la gestión de proyectos.	Manual de gestión de proyectos.	Verificación del cumplimiento del manual de gestión de proyectos.	N° de proyectos.	Oficial de seguridad digital.	3
	6.2 Dispositivos para movilidad y teletrabajo.					
	6.2.1 Política de uso de dispositivos para movilidad.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados al uso de dispositivos	Oficial de seguridad digital.	3
	6.2.2 Teletrabajo.	Directiva de teletrabajo.	Verificación de personal en teletrabajo	N° de funcionarios públicos en teletrabajo	Oficial de seguridad digital.	3
A.07 Seguridad de los Recursos Humanos.						
	7.1 Antes de la contratación.					
	7.1.1 Investigación de antecedentes.	Términos de referencia de contrataciones.	Verificación de TDR	N° de TDR verificados.	Oficial de seguridad digital	3
	7.1.2 Términos y condiciones de contratación.	Terminas de referencia de contrataciones / Contratos	Verificación de TDR	N° de TDR verificados.	Oficial de seguridad digital.	4
	7.2 Durante la contratación.					

	7.2.1 Responsabilidades de gestión.	Manual de organizaciones y funciones (MOF)	Verificación de cumplimiento del MOF	% de cumplimiento del MOF	Oficial de seguridad digital	3
	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Plan de capacitaciones en seguridad de la información.	Verificación del cumplimiento de capacitaciones en SGSI	N° de funcionarios capacitados	Oficial de seguridad digital.	4
	7.2.3 Proceso disciplinario.					
	7.3 Cese o cambio de puesto de trabajo.	Carta de agradecimiento.	Verificación de cambio de puesto de trabajo	N° de ceses o cambio de puesto de trabajo.	Oficial de seguridad digital	3
	7.3.1 Cese o cambio de puesto de trabajo.	Carta de agradecimiento.	Verificación de cese o cambio de puesto de trabajo	N° de cese o cambio de puesto de trabajo	Oficial de seguridad digital.	3
A.08 Gestión de Activos.						
	8.1 Responsabilidad sobre los activos.					
	8.1.1 Inventario de activos.	Inventario de activos de la información.	Verificación de inventario de activos	N° de activos de información	Oficial de seguridad digital	4
	8.1.2 Propiedad de los activos.	Inventario de activos de la información.	Verificación de inventario de activos	N° de activos de información	Oficial de seguridad digital.	2
	8.1.3 Uso aceptable de los activos.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados al uso de activos.	Oficial de seguridad digital.	3
	8.1.4 Devolución de activos.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la devolución de activos.	Oficial de seguridad digital.	4

	8.2 Clasificación de la información.					
	8.2.1 Directrices de clasificación.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a las directrices de clasificación.	Oficial de seguridad digital.	**3**
	8.2.2 Etiquetado y manipulado de la información.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados al manipulados de la información.	Oficial de seguridad digital.	**3**
	8.2.3 Manipulación de activos.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la manipulación de activos.	Oficial de seguridad digital.	**3**
	8.3 Manejo de los soportes de almacenamiento.					
	8.3.1 Gestión de soportes extraíbles.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados al soporte extraíble.	Oficial de seguridad digital.	**3**
	8.3.2 Eliminación de soportes.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la eliminación de soportes.	Oficial de seguridad digital.	**3**
	8.3.3 Soportes físicos en tránsito.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados al soporte físico.	Oficial de seguridad digital.	**3**
A.09 Control de Acceso.						
	9.1 Requisitos de negocio para el control de accesos.					
	9.1.1 Política de control de accesos.	Documento de gestión de accesos.	Verificación de políticas de control de accesos	N° de políticas de control de accesos.	Oficial de seguridad digital.	**3**

	9.1.2 Control de acceso a las redes y servicios asociados.	Documento de gestión de accesos.	Verificación de control de acceso a las redes y servicios asociados.	N° de controles de acceso a las redes.	Oficial de seguridad digital.	2
	9.2 Gestión de acceso de usuario.					
	9.2.1 Gestión de altas/bajas en el registro de usuarios.	Documento de gestión de accesos.	Verificación de cumplimiento de altas/bajas en el registro de usuarios.	N° de registro de usuarios.	Oficial de seguridad digital.	3
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Documento de gestión de accesos.	Verificación de los derechos de accesos asignados a usuarios.	N° de registro de usuarios.	Oficial de seguridad digital.	3
	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Documento de gestión de accesos.	Verificación de los derechos de accesos con privilegios.	N° de registro de usuarios.	Oficial de seguridad digital.	3
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Documento de gestión de accesos.	Verificación de información confidencial de autenticación de usuarios.	N° de registro de usuarios.	Oficial de seguridad digital.	3
	9.2.5 Revisión de los derechos de acceso de los usuarios.	Documento de gestión de accesos.	Verificación de información confidencial de autenticación de usuarios.	N° de registro de usuarios.	Oficial de seguridad digital.	3
	9.2.6 Retirada o adaptación de los derechos de acceso	Documento de gestión de accesos.	Verificación de información confidencial de autenticación de usuarios.	N° de registro de usuarios.	Oficial de seguridad digital.	3
	9.3 Responsabilidades del usuario.					
	9.3.1 Uso de información confidencial para la autenticación.	Acuerdo de confidencialidad.	Verificación de información confidencial para la autenticidad.	N° de activos de información confidencial.	Oficial de seguridad digital.	3

	9.4 Control de acceso a sistemas y aplicaciones.					
	9.4.1 Restricción del acceso a la información.	Documento de gestión de accesos.	Verificación de información confidencial de autenticación de usuarios.	N° de registro de usuarios.	Oficial de seguridad digital.	**3**
	9.4.2 Procedimientos seguros de inicio de sesión.	Documento de gestión de accesos.	Verificación de información confidencial de autenticación de usuarios.	N° de registro de usuarios.	Oficial de seguridad digital.	**3**
	9.4.3 Gestión de contraseñas de usuario.	Documento de gestión de accesos.	Verificación de información confidencial de autenticación de usuarios.	N° de registro de usuarios.	Oficial de seguridad digital.	**3**
	9.4.4 Uso de herramientas de administración de sistemas.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la herramienta de administración de sistemas.	Oficial de seguridad digital.	**3**
	9.4.5 Control de acceso al código fuente de los programas.	Documento de gestión de accesos.	Verificación de cumplimiento de directiva	N° de artículos orientados al control de accesos al código fuente de los programas.	Oficial de seguridad digital.	**3**
A.10 Criptografía.						
	10.1 Controles criptográficos.					
	10.1.1 Política de uso de los controles criptográficos.	Política de seguridad de la información	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	**3**
	10.1.2 Gestión de claves	Política de seguridad de la información	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	**3**
A.11 Seguridad Física y Ambiental.						
	11.1 Áreas seguras.					

	11.1.1 Perímetro de seguridad física.	Data center, instalaciones y perímetros de seguridad física.	Verificación de controles y manuales del centro de datos, instalaciones y perímetros de seguridad físicas.	N° de dispositivos de seguridad física.	Oficial de seguridad digital	3
	11.1.2 Controles físicos de entrada.	Personal de vigilancia.	Verificación de controles físicos de entradas.	N° de controles físicos de entrada.	Oficial de seguridad digital	3
	11.1.3 Seguridad de oficinas, despachos y recursos.	Gestión de accesos físicos.	Verificación de seguridad de oficinas, despachos y recursos.	N° de controles de acceso fisico	Oficial de seguridad digital	3
	11.1.4 Protección contra las amenazas externas y ambientales.	Data center, instalaciones y perímetros de seguridad física	Verificación de controles y manuales del centro de datos, instalaciones y perímetros de seguridad físicas.	N° de dispositivos contra amenazas externas y ambiental.	Oficial de seguridad digital	3
	11.1.5 El trabajo en áreas seguras.	Data center, instalaciones y perímetros de seguridad física	Verificación de controles y manuales del centro de datos, instalaciones y perímetros de seguridad físicas.	N° de dispositivos en el trabajo en áreas seguras.	Oficial de seguridad digital	3
	11.1.6 Áreas de acceso público, carga y descarga.	Data center, instalaciones y perímetros de seguridad física	Verificación de controles y manuales del centro de datos, instalaciones y perímetros de seguridad físicas.	N° de dispositivos de áreas de acceso público, carga y descarga.	Oficial de seguridad digital	3
	11.2 Seguridad de los equipos.					
	11.2.1 Emplazamiento y protección de equipos.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados al emplazamiento y protección de equipos.	Oficial de seguridad digital.	3
	11.2.2 Instalaciones de suministro.	Herramientas de soporte.	Verificación de instalaciones de suministro.	N° de herramientas de soporte.	Oficial de seguridad digital.	3

	11.2.3 Seguridad del cableado.	Cableado estructurado y equipos de redes y comunicaciones	Verificación de seguridad del cableado.	N° de cableado estructura y equipos de redes y comunicaciones.	Oficial de seguridad digital.	3
	11.2.4 Mantenimiento de los equipos.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados al mantenimiento de los equipos.	Oficial de seguridad digital.	3
	11.2.5 Salida de activos fuera de las dependencias de la empresa.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la salida de activos.	Oficial de seguridad digital.	3
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la seguridad de los equipos.	Oficial de seguridad digital.	3
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la reutilización o retirada segura de dispositivos.	Oficial de seguridad digital.	3
	11.2.8 Equipo informático de usuario desatendido.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados al equipo informático.	Oficial de seguridad digital.	3
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Política de seguridad de la información.	Verificación de políticas de seguridad de la información.	N° de políticas de seguridad de la información.	Oficial de seguridad digital.	3
A.12 Seguridad de las Operaciones.						
	12.1 Responsabilidades y procedimientos de operación.					

	12.1.1 Documentación de procedimientos de operación.	Equipos ubicados bajo instalaciones protegidas.	Verificación de documentación de procedimientos de operación.	N° de equipos ubicados bajo instalaciones protegidos.	Oficial de seguridad digital	3
	12.1.2 Gestión de cambios.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la gestión de cambios.	Oficial de seguridad digital.	2
	12.1.3 Gestión de capacidades.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la gestión de capacidades.	Oficial de seguridad digital.	2
	12.1.4 Separación de entornos de desarrollo, prueba y producción.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la separación de entornos de desarrollo, pruebas y producción.	Oficial de seguridad digital.	2
	12.2 Protección contra código malicioso.					
	12.2.1 Controles contra el código malicioso.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a los controles contra el código malicioso.	Oficial de seguridad digital.	3
	12.3 Copias de seguridad.					
	12.3.1 Copias de seguridad de la información.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	3
	12.4 Registro de actividad y supervisión.					

	12.4.1 Registro y gestión de eventos de actividad.	Auditoria de eventos.	Verificación de auditorías de eventos.	N° de eventos registrados	Oficial de seguridad digital.	3
	12.4.2 Protección de los registros de información.	Ejecución de copias de seguridad.	Verificación de cumplimiento de respaldos de seguridad.	N° de respaldos de seguridad	Oficial de seguridad digital.	3
	12.4.3 Registros de actividad del administrador y operador del sistema.	Auditoria de eventos.	Verificación de auditorías de eventos.	N° de eventos registrados	Oficial de seguridad digital.	3
	12.4.4 Sincronización de relojes.	Sincronización de relojes de los activos de información.	Sincronización de reloj	N° de sincronización de reloj a activos de información.	Oficial de seguridad digital.	3
	12.5 Control del software en explotación.					
	12.5.1 Instalación del software en sistemas en producción.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la instalación del software en sistemas en producción.	Oficial de seguridad digital.	4
	12.6 Gestión de la vulnerabilidad técnica.					
	12.6.1 Gestión de las vulnerabilidades técnicas.	Actualización de software y gestión de riesgos.			Oficial de seguridad digital.	4
	12.6.2 Restricciones en la instalación de software.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a las restricciones en la instalación de software.	Oficial de seguridad digital.	4

	12.7 Consideraciones de las auditorías de los sistemas de información.					
	12.7.1 Controles de auditoría de los sistemas de información.	Auditoria de eventos.	Verificación de controles de auditoria de los sistemas de información.	N° de auditoría de eventos.	Oficial de seguridad digital.	3
A.13 Seguridad de las Comunicaciones.						
	13.1 Gestión de la seguridad en las redes.					
	13.1.1 Controles de red.	Seguridad tecnológica perimetral.	Verificación de implementación de seguridad perimetral	N° de equipos, dispositivos o programas implementados en seguridad perimetral.	Oficial de seguridad digital	3
	13.1.2 Mecanismos de seguridad asociados a servicios en red.	Gestión de control de accesos.	Verificación de mecanismos de seguridad asociados a servicios en red.	N° de controles de acceso.	Oficial de seguridad digital	3
	13.1.3 Segregación de redes.	Segmentación de redes VLAN	Verificación de segmentación de red	N° de VLAN administradas	Oficial de seguridad digital	3
	13.2 Intercambio de información con partes externas.					
	13.2.1 Políticas y procedimientos de intercambio de información.					
	13.2.2 Acuerdos de intercambio.					

	13.2.3 Mensajería electrónica.					
	13.2.4 Acuerdos de confidencialidad y secreto.					
A.14 Adquisición, desarrollo y mantenimiento de sistemas.						
	14.1 Requisitos de seguridad de los sistemas de información.					
	14.1.1 Análisis y especificación de los requisitos de seguridad.	Seguridad perimetral.	Verificación de implementación de seguridad perimetral	N° de equipos, dispositivos o programas implementados en seguridad perimetral.	Oficial de seguridad digital	**2**
	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	Seguridad perimetral.	Verificación de implementación de seguridad perimetral	N° de equipos, dispositivos o programas implementados en seguridad perimetral.	Oficial de seguridad digital	**2**
	14.1.3 Protección de las transacciones por redes telemáticas.	Seguridad perimetral.	Verificación de implementación de seguridad perimetral	N° de equipos, dispositivos o programas implementados en seguridad perimetral.	Oficial de seguridad digital	**2**
	14.2 Seguridad en los procesos de desarrollo y soporte.					

	14.2.1 Política de desarrollo seguro de software.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	3
	14.2.2 Procedimientos de control de cambios en los sistemas.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	3
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	3
	14.2.4 Restricciones a los cambios en los paquetes de software.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	2
	14.2.5 Uso de principios de ingeniería en protección de sistemas.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	2
	14.2.6 Seguridad en entornos de desarrollo.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	3
	14.2.7 Externalización del desarrollo de software.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	3
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	3
	14.2.9 Pruebas de aceptación.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	3

	14.3 Datos de prueba.					
	14.3.1 Protección de los datos utilizados en pruebas.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	**3**
A.15 Relaciones con los proveedores.						
	15.1 Seguridad de la información en las relaciones con suministradores.					
	15.1.1 Política de seguridad de la información para suministradores.	Política de seguridad de la información.	Verificación de las políticas de seguridad de información	N° de políticas de SGSI	Oficial de seguridad digital	**3**
	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	Contrato de servicios.	Verificación de controles de servicio.	N° de controles de servicio	Oficial de seguridad digital	**3**
	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	Contrato de servicios	Verificación de controles de servicio.	N° de controles de servicio	Oficial de seguridad digital	**3**
	15.2 Gestión de la prestación del servicio por suministradores.					
	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Informe mensual de servicio.	Verificación de informes mensual de servicios.	N° de informes de servicio.	Oficial de seguridad digital	**3**
	15.2.2 Gestión de cambios en los servicios prestados por terceros.	Gestión de cambios.	Verificación de gestión de cambios.	N° de gestión de cambios en los servicios.	Oficial de seguridad digital	**3**

A.16 Gestión de incidentes de seguridad de la información.						
	16.1 Gestión de incidentes de seguridad de la información y mejoras.					
	16.1.1 Responsabilidades y procedimientos.	Gestión de incidentes de seguridad de la información	Verificación de plan de gestión de incidentes de seguridad de la información.	N° de responsabilidad y procedimientos.	Oficial de seguridad digital	3
	16.1.2 Notificación de los eventos de seguridad de la información.	Gestión de incidentes de seguridad de la información	Verificación de plan de gestión de incidentes de seguridad de la información.	N° de notificaciones de eventos de seguridad de la información.	Oficial de seguridad digital	3
	16.1.3 Notificación de puntos débiles de la seguridad.	Gestión de incidentes de seguridad de la información	Verificación de plan de gestión de incidentes de seguridad de la información.	N° de notificaciones de puntos débiles de seguridad de la información.	Oficial de seguridad digital	3
	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	Gestión de incidentes de seguridad de la información	Verificación de plan de gestión de incidentes de seguridad de la información.	N° de valoración de eventos de seguridad de la información y toma de decisiones.	Oficial de seguridad digital	3
	16.1.5 Respuesta a los incidentes de seguridad.	Gestión de incidentes de seguridad de la información	Verificación de plan de gestión de incidentes de seguridad de la información.	N° de respuestas ante incidentes de seguridad.	Oficial de seguridad digital	3
	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	Gestión de incidentes de seguridad de la información	Verificación de plan de gestión de incidentes de seguridad de la información.	% de aprendizaje de los incidentes de	Oficial de seguridad digital	3

				seguridad de la información.		
	16.1.7 Recopilación de evidencias.	Gestión de incidentes de seguridad de la información	Verificación de plan de gestión de incidentes de seguridad de la información.	% de recopilación de evidencias.	Oficial de seguridad digital	3
A.17 Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio						
	17.1 Continuidad de la seguridad de la información.					
	17.1.1 Planificación de la continuidad de la seguridad de la información.	Plan de contingencia.	Verificación de plan de contingencia.	% de cumplimiento del plan de continuidad.	Oficial de seguridad digital	3
	17.1.2 Implantación de la continuidad de la seguridad de la información.	Plan de contingencia.	Verificación de plan de contingencia.	% de cumplimiento del plan de continuidad.	Oficial de seguridad digital	3
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Informe de pruebas de contingencia.	Verificación de plan de contingencia.	% de cumplimiento del plan de continuidad.	Oficial de seguridad digital	3
	17.2 Redundancias.					
	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	Centro de datos.	Verificación de disponibilidad de instalaciones para el procesamiento de la información.	% de tiempo de disponibilidad.	Oficial de seguridad digital	3
A.18 Cumplimiento.						

	18.1 Cumplimiento de los requisitos legales y contractuales.					
	18.1.1 Identificación de la legislación aplicable.	Leyes peruanas.	Verificación del cumplimiento de las leyes peruanas	% de cumplimiento de las leyes peruanas.	Oficial de seguridad digital	**3**
	18.1.2 Derechos de propiedad intelectual (DPI).	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a los derechos de propiedad intelectual.	Oficial de seguridad digital.	**3**
	18.1.3 Protección de los registros de la organización.	Control de documentos.	Verificación del cumplimiento del SGSI	% de cumplimiento del SGSI	Oficial de seguridad digital.	**3**
	18.1.4 Protección de datos y privacidad de la información personal.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la protección de datos y privacidad de la información personal.	Oficial de seguridad digital.	**3**
	18.1.5 Regulación de los controles criptográficos.	Directiva de TI y seguridad de la información.	Verificación de cumplimiento de directiva	N° de artículos orientados a la regulación de los controles criptográficos.	Oficial de seguridad digital.	**3**
	18.2 Revisiones de la seguridad de la información.					
	18.2.1 Revisión independiente de la seguridad de la información.	Auditoría interna.	Verificación del cumplimiento del SGSI	% de cumplimiento del SGSI	Oficial de seguridad digital	**3**

	18.2.2 Cumplimiento de las políticas y normas de seguridad.	Medición del SGSI	Verificación del cumplimiento del SGSI	% de cumplimiento del SGSI	Oficial de seguridad digital	3
	18.2.3 Comprobación del cumplimiento.	Informes	Verificación del cumplimiento del SGSI	% de cumplimiento del SGSI	Oficial de seguridad digital	3

Fuente: Elaboración Propia

4.1.8.2. Auditoría interna.

La siguiente auditoria permite verificar el cumplimento del sistema de gestión de seguridad digital, los mismos que deben de cumplir con los siguientes aspectos:

- La auditoría externa deberá de ser liderada por un auditor interno certificado con las habilidades demostradas, de la misma manera el equipo auditor deberá de tener experiencia auditando sistemas de gestión de seguridad de la información.
- La información recolectada a partir de la auditoria deberá ser reportada al comité de transformación digital.
- Los informes de la auditoria deberán de ser claras y precisas con la finalidad de que cualquier persona con acceso a ella la comprenda.
- El informe o reporte final de auditoria deberá de ser enviado en un plazo no mayor de 7 días calendario.

De la misma manera la auditoría interna deberá de seguir el siguiente proceso:

- Diseñar el plan de auditoría.
- Selección del auditor.
- Elaborar el cronograma de actividades.
- Realizar el proceso de auditoría.
- Recabar la información de todo el equipo auditor.
- Elaborar informe o reporte final.

4.1.9. Mejora.

4.1.9.1. Acciones correctivas.

Los escenarios de no conformidad pueden ser por distintos motivos los mismo que se enlistan a continuación:

- Falta en los requisitos legales o de contrato.
- Falta contra las políticas de seguridad de la información.
- Incumplimiento de los objetivos de seguridad de la información.
- Auditorias.
- Investigación de incidentes.
- Monitoreo.
- Revisión por el comité de transformación digital.
- Resultado de las acciones correctivas.

Para la corrección de una no conformidad, se deberá de seguir el siguiente proceso:

- Solicitar la acción correctiva.
- Identificar la raíz o causa de la no conformidad.
- Rellenar correctamente el formato sugerido para la corrección de una no conformidad.

4.1.9.2. Mejora continua.

El presente apartado pretende la mejora continua a través de la constante verificación del sistema de gestión de seguridad de la información cumpliendo los siguientes procesos:

- **Identificar las oportunidades de mejora.** Las oportunidades de mejora continua se identificarán de distinta manera entre las cuales pueden ser:
  - Auditoria.
  - Encuestas.
  - Incidentes.
  - Sugerencias.

Posterior a la identificación de las oportunidades se deberá de realizar una selección de las oportunidades de mejora y asignarlas a un representante, los mismo que se asignaran mediante un plazo límite de elaboración.

- **Realizar una propuesta de plan de acción.** Se deberá de proponer un plan de acción basado en la experiencia, los mismo que se analizarán de acuerdo al costo, beneficio y tiempo para la organización. Posterior al análisis se procede a crear el plan de acción proponiendo un cronograma, áreas involucradas, actividades, entre otras.
- **Aprobación del plan de acción.** El comité de transformación digital deberá de realizar la revisión, retroalimentación y aprobación del plan de acción.
- **Ejecutar el plan de acción.** En este proceso se debe de realizar la ejecución del plan propuesto, de la misma manera se deberá realizar el seguimiento y acompañamiento en cada una de las etapas del plan de acción.
- **Medir la mejora continua.** Se deberá realizar una medición del antes y después de la aplicación de la acción propuesta.

4.2. Presentación, análisis e interpretación de resultados

En el presente apartado se presentan los resultados obtenidos a partir de la aplicación del instrumento de investigación.

a. Análisis estadístico descriptivo.

Con la finalidad de conocer un poco más acerca del cumplimiento del SGSI se realizó una encuesta dentro de la sub gerencia de

racionalización y sistemas TIC, es por ello que a continuación, se presenta el análisis estadístico de los datos recopilados.

Tabla 22. *Resultados de la interrogante ¿Ud. es conocedor de las políticas de seguridad de la información de su institución?*

¿Ud. es conocedor de las políticas de seguridad de la información de su institución?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**No**	1	8,3	8,3
	SI	11	91,7	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 9. *Resultados de la interrogante ¿Ud. es conocedor de las políticas de seguridad de la información de su institución?*

Fuente: Elaboración Propia

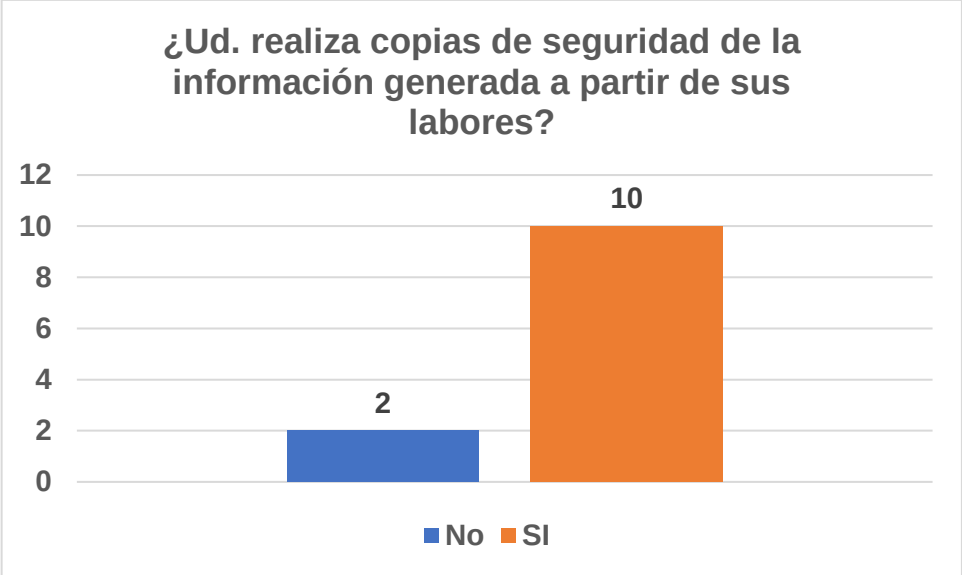
Con respecto a la pregunta 1 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. es conocedor de las políticas de seguridad de la información de su institución? Se obtuvo un porcentaje de 91.7% (11 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 8.3% (1 colaborador) no conoce acerca de las mismas. Estos resultados se observan en la tabla 22 y figura 9 antecesoras al presente párrafo.

Tabla 23. *Resultados de la interrogante ¿Ud. realiza copias de seguridad de la información generada a partir de sus labores?*

¿Ud. realiza copias de seguridad de la información generada a partir de sus labores?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**No**	2	16,7	16,7
	Sl	10	83,3	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 10. *Resultados de la interrogante ¿Ud. realiza copias de seguridad de la información generada a partir de sus labores?*



Fuente: Elaboración Propia

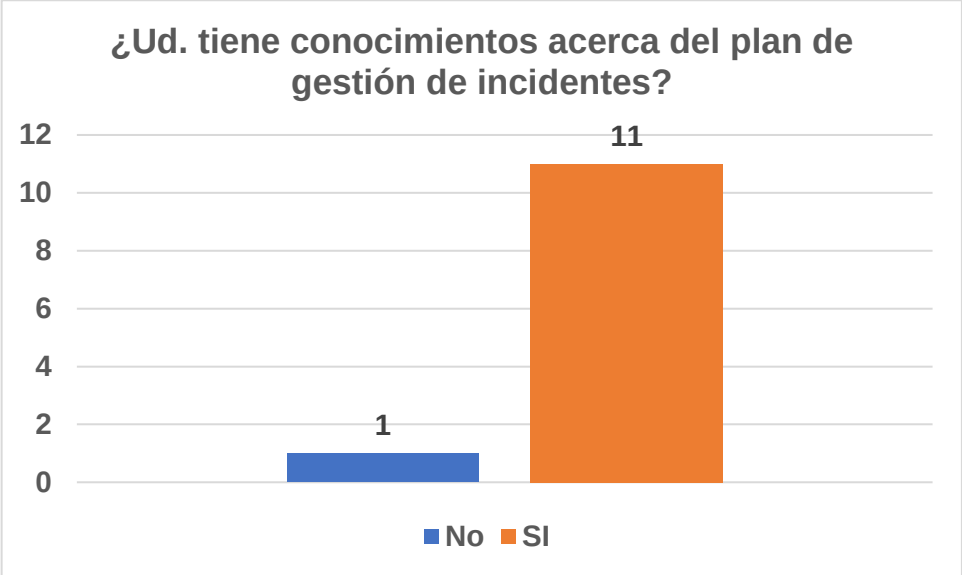
Con respecto a la pregunta 2 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. realiza copias de seguridad de la información generada a partir de sus labores? Se obtuvo un porcentaje de 83,3% (10 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 16,7% (2 colaborador) no conoce acerca de las mismas. Estos resultados se observan en la tabla 23 y figura 10 antecesoras al presente párrafo.

Tabla 24. *Resultados de la interrogante ¿Ud. tiene conocimientos acerca del plan de gestión de incidentes?*

¿Ud. tiene conocimientos acerca del plan de gestión de incidentes?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**No**	1	8,3	8,3
	SI	11	91,7	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 11. *Resultados de la interrogante ¿Ud. tiene conocimientos acerca del plan de gestión de incidentes?*



Fuente: Elaboración Propia

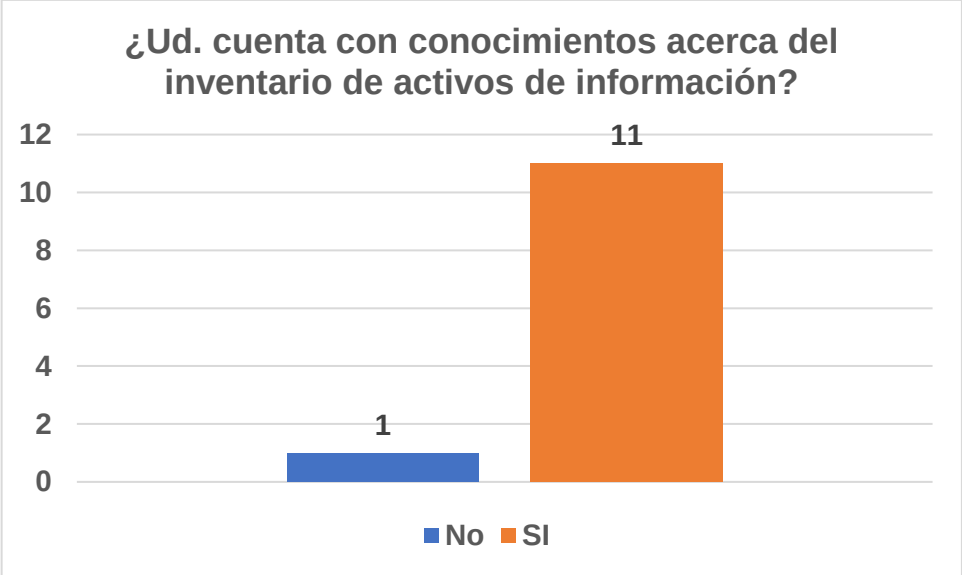
Con respecto a la pregunta 3 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. tiene conocimientos acerca del plan de gestión de incidentes? Se obtuvo un porcentaje de 91,7% (11 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 8,3% (1 colaborador) no conoce acerca de las mismas. Estos resultados se observan en la tabla 24 y figura 11 antecesoras al presente párrafo.

Tabla 25. *Resultados de la interrogante ¿Ud. cuenta con conocimientos acerca del inventario de activos de información?*

¿Ud. cuenta con conocimientos acerca del inventario de activos de información?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**No**	1	8,3	8,3
	SI	11	91,7	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 12. *Resultados de la interrogante ¿Ud. cuenta con conocimientos acerca del inventario de activos de información?*



Fuente: Elaboración Propia

Con respecto a la pregunta 4 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. cuenta con conocimientos acerca del inventario de activos de información? Se obtuvo un porcentaje de 91,7% (11 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 8,3% (1 colaborador) no conoce acerca de las mismas. Estos resultados se observan en la tabla 25 y figura 12 antecesoras al presente párrafo.

Tabla 26. *Resultados de la interrogante ¿Ud. al momento de abandonar su espacio de trabajo bloquea con contraseña su estación de trabajo?*

¿Ud. al momento de abandonar su espacio de trabajo bloquea con contraseña su estación de trabajo?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**No**	1	8,3	8,3
	Sl	11	91,7	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 13. *Resultados de la interrogante ¿Ud. al momento de abandonar su espacio de trabajo bloquea con contraseña su estación de trabajo?*

Fuente: Elaboración Propia

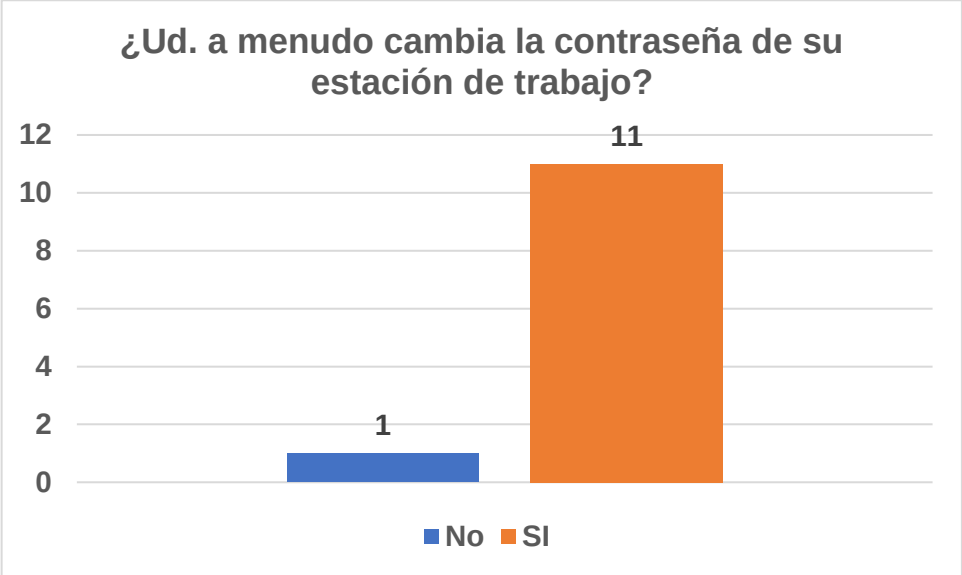
Con respecto a la pregunta 5 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. al momento de abandonar su espacio de trabajo bloquea con contraseña su estación de trabajo? Se obtuvo un porcentaje de 91,7% (11 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 8,3% (1 colaborador) no conoce acerca de las mismas. Estos resultados se observan en la tabla 26 y figura 13 antecesoras al presente párrafo.

Tabla 27. *Resultados de la interrogante ¿Ud. a menudo cambia la contraseña de su estación de trabajo?*

¿Ud. a menudo cambia la contraseña de su estación de trabajo?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**No**	1	8,3	8,3
	SI	11	91,7	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 14. *Resultados de la interrogante ¿Ud. a menudo cambia la contraseña de su estación de trabajo?*



Fuente: Elaboración Propia

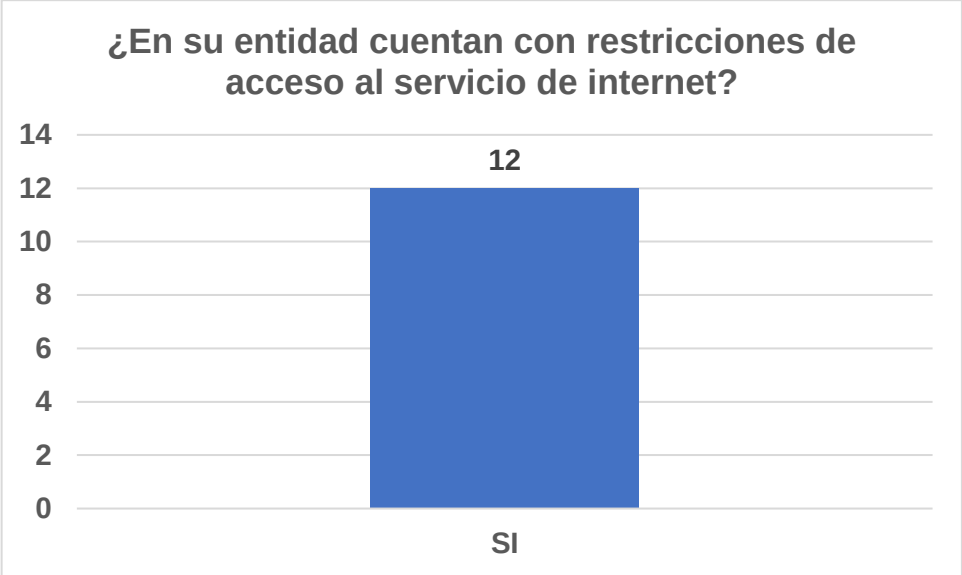
Con respecto a la pregunta 6 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. a menudo cambia la contraseña de su estación de trabajo? Se obtuvo un porcentaje de 91,7% (11 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 8,3% (1 colaborador) no conoce acerca de las mismas. Estos resultados se observan en la tabla 27 y figura 14 antecesoras al presente párrafo.

Tabla 28. *Resultados de la interrogante ¿En su entidad cuentan con restricciones de acceso al servicio de internet?*

¿En su entidad cuentan con restricciones de acceso al servicio de internet?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**SI**	12	100,0	100,0

Fuente: Elaboración Propia

Figura 15. *Resultados de la interrogante ¿En su entidad cuentan con restricciones de acceso al servicio de internet?*



Fuente: Elaboración Propia

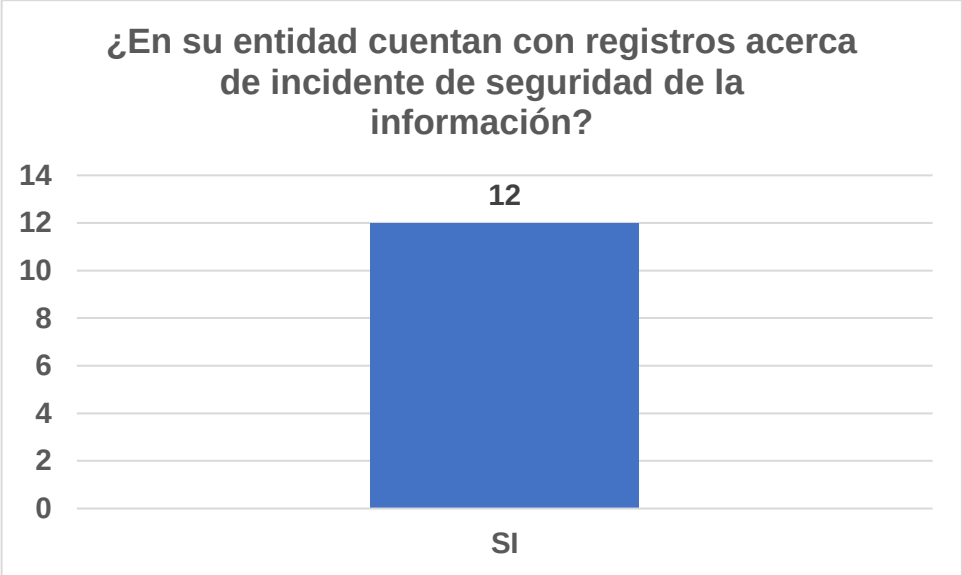
Con respecto a la pregunta 7 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. a menudo cambia la contraseña de su estación de trabajo? Se obtuvo un porcentaje de 100% (12 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 0% (0 colaboradores) no conoce acerca de las mismas. Estos resultados se observan en la tabla 28 y figura 15 antecesoras al presente párrafo.

Tabla 29. *Resultados de la interrogante ¿En su entidad cuentan con registros acerca de incidente de seguridad de la información?*

¿En su entidad cuentan con registros acerca de incidente de seguridad de la información?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**SI**	12	100,0	100,0

Fuente: Elaboración Propia

Figura 16. *Resultados de la interrogante ¿En su entidad cuentan con registros acerca de incidente de seguridad de la información?*



Fuente: Elaboración Propia

Con respecto a la pregunta 8 del instrumento de investigación utilizado en la presente investigación la cual es: ¿En su entidad cuentan con registros acerca de incidente de seguridad de la información? Se obtuvo un porcentaje de 100% (12 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 0% (0 colaboradores) no conoce acerca de las mismas. Estos resultados se observan en la tabla 29 y figura 16 antecesoras al presente párrafo.

Tabla 30. *Resultados de la interrogante ¿Ud. tiene conocimiento que su entidad cuenta con seguridad perimetral?*

¿Ud. tiene conocimiento que su entidad cuenta con seguridad perimetral?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**No**	1	8,3	8,3
	Sl	11	91,7	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 17. *Resultados de la interrogante ¿Ud. tiene conocimiento que su entidad cuenta con seguridad perimetral?*

Fuente: Elaboración Propia

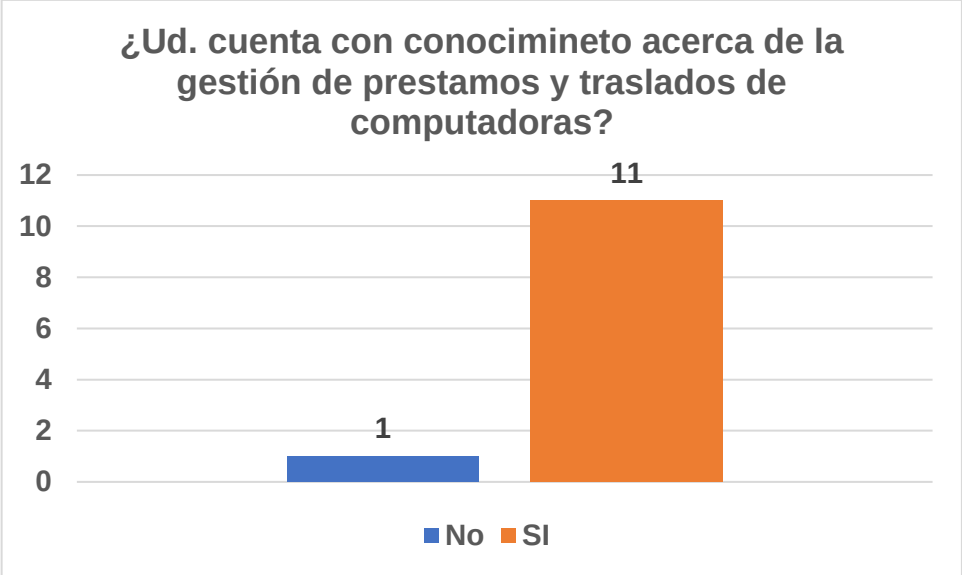
Con respecto a la pregunta 9 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. tiene conocimiento que su entidad cuenta con seguridad perimetral? Se obtuvo un porcentaje de 91,7% (11 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 8.3% (1 colaborador) no conoce acerca de las mismas. Estos resultados se observan en la tabla 30 y figura 17 antecesoras al presente párrafo.

Tabla 31. *Resultados de la interrogante ¿Ud. cuenta con conocimiento acerca de la gestión de préstamos y traslados de computadoras?*

¿Ud. cuenta con conocimiento acerca de la gestión de préstamos y traslados de computadoras?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**No**	1	8,3	8,3
	Sl	11	91,7	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 18. *Resultados de la interrogante ¿Ud. cuenta con conocimiento acerca de la gestión de préstamos y traslados de computadoras?*



Fuente: Elaboración Propia

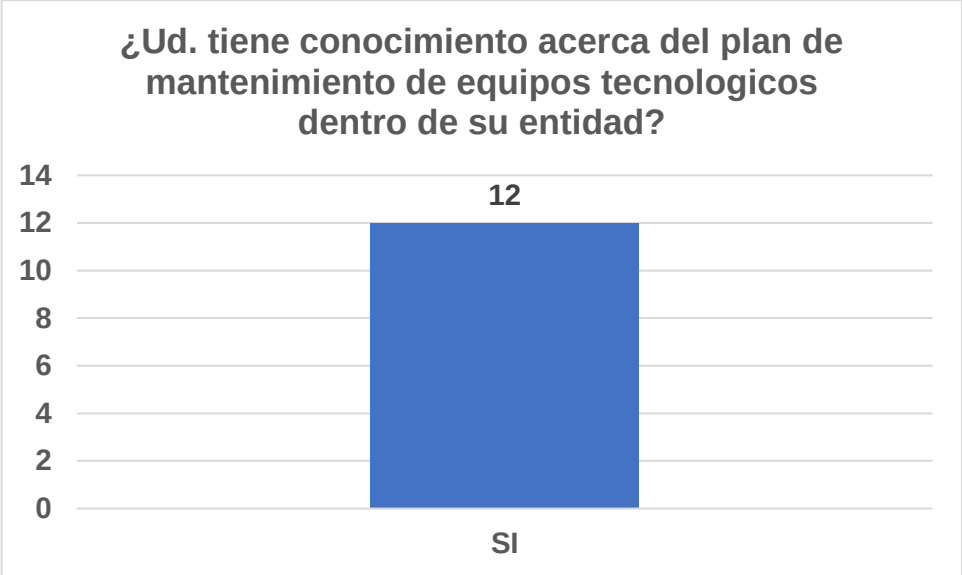
Con respecto a la pregunta 10 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. cuenta con conocimiento acerca de la gestión de préstamos y traslados de computadoras? Se obtuvo un porcentaje de 91,7% (11 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 8.3% (1 colaborador) no conoce acerca de las mismas. Estos resultados se observan en la tabla 31 y figura 18 antecesoras al presente párrafo.

Tabla 32. *Resultados de la interrogante ¿Ud. tiene conocimiento acerca del plan de mantenimiento de equipos tecnológicos dentro de su entidad?*

¿Ud. tiene conocimiento acerca del plan de mantenimiento de equipos tecnológicos dentro de su entidad?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**SI**	12	100,0	100,0

Fuente: Elaboración Propia

Figura 19. *Resultados de la interrogante ¿Ud. tiene conocimiento acerca del plan de mantenimiento de equipos tecnológicos dentro de su entidad?*



Fuente: Elaboración Propia

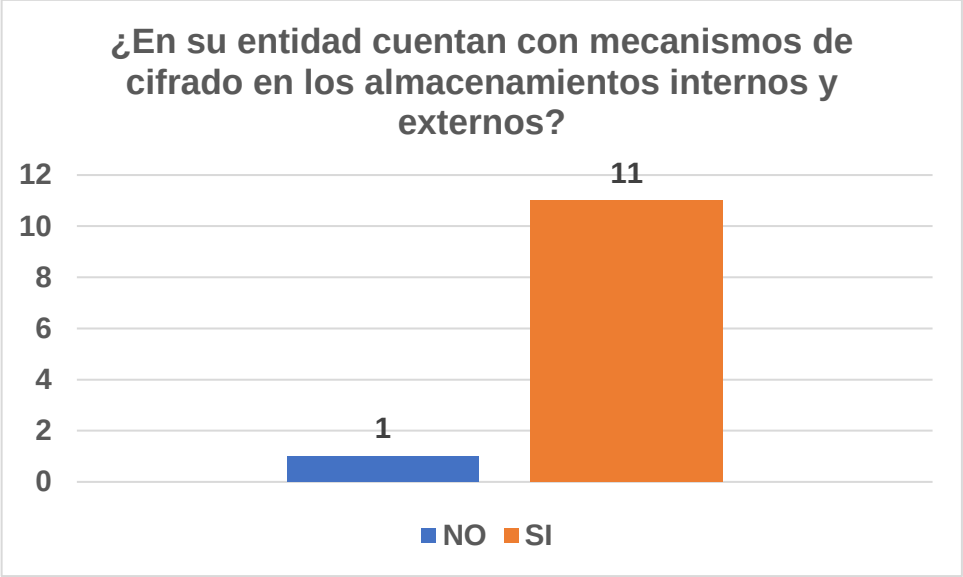
Con respecto a la pregunta 11 del instrumento de investigación utilizado en la presente investigación la cual es: ¿Ud. tiene conocimiento acerca del plan de mantenimiento de equipos tecnológicos dentro de su entidad? Se obtuvo un porcentaje de 100% (12 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 0% (0 colaboradores) no conoce acerca de las mismas. Estos resultados se observan en la tabla 32 y figura 19 antecesoras al presente párrafo.

Tabla 33. *Resultados de la interrogante ¿En su entidad cuentan con mecanismos de cifrado en los almacenamientos internos y externos?*

¿En su entidad cuentan con mecanismos de cifrado en los almacenamientos internos y externos?				
		Frecuencia	**Porcentaje**	**Porcentaje acumulado**
Válido	**NO**	1	8,3	8,3
	SI	11	91,7	100,0
	Total	12	100,0	

Fuente: Elaboración Propia

Figura 20. *Resultados de la interrogante ¿En su entidad cuentan con mecanismos de cifrado en los almacenamientos internos y externos?*



Fuente: Elaboración Propia

Con respecto a la pregunta 11 del instrumento de investigación utilizado en la presente investigación la cual es: ¿En su entidad cuentan con mecanismos de cifrado en los almacenamientos internos y externos? Se obtuvo un porcentaje de 91,7% (11 colaboradores) que si conocen las políticas de seguridad de la información mientras que el 8.3% (1 colaboradores) no conoce acerca de las mismas. Estos resultados se observan en la tabla 33 y figura 20 antecesoras al presente párrafo.

b. Estadística de confiabilidad.

Para determinar la confiabilidad del instrumento aplicado en la presente investigación se hace uso de la estadística de fiabilidad de Cronbach, es por ello que a continuación se presentan los resultados:

Tabla 34. *Estadística de fiabilidad – Resumen de procesamiento de casos.*

		N	%
Casos	**Válido**	12	100,0
	Excluido	0	,0
	Total	12	100,0

Fuente: Elaboración Propia

Tabla 35. *Estadística de fiabilidad.*

Alfa de Cronbach	N de elementos
0,708	12

Fuente: Elaboración Propia

Posterior a la obtención de los resultados procedemos al análisis es por ello que basado en las sugerencias de Frías (2019) quien menciona que "coeficiente alfa >.7 es aceptable" (p.7) entonces podemos mencionar que el instrumento de recolección de datos utilizado en la presente investigación es confiable.

c. Análisis estadístico inferencial.

El análisis de estadística inferencial se hará uso para la prueba de hipótesis, la misma que se hará uso mediante el uso del procedimiento de la estadística de T de Student para muestras relacionadas haciendo uso de una evaluación de pre test y post test las mismas que se aplican previa a la implementación del SGSI y posterior a ella.

Para el mencionado análisis se establece como nivel de significancia a 5% y por ende la confiabilidad será de 95%. Todo este análisis se

presentará en el apartado 4.3 prueba de hipótesis, la misma que se encuentra posterior a este apartado.

4.3. Prueba de hipótesis

Para la prueba de hipótesis se realiza el análisis previo a la implementación del sistema de gestión de seguridad de la información; para ello se realiza la evaluación de los controles evaluando el nivel encontrado con el resultado posterior a la implementación. Los mismo que se presentan a continuación.

Tabla 36. *Análisis de brechas (pre test y post test).*

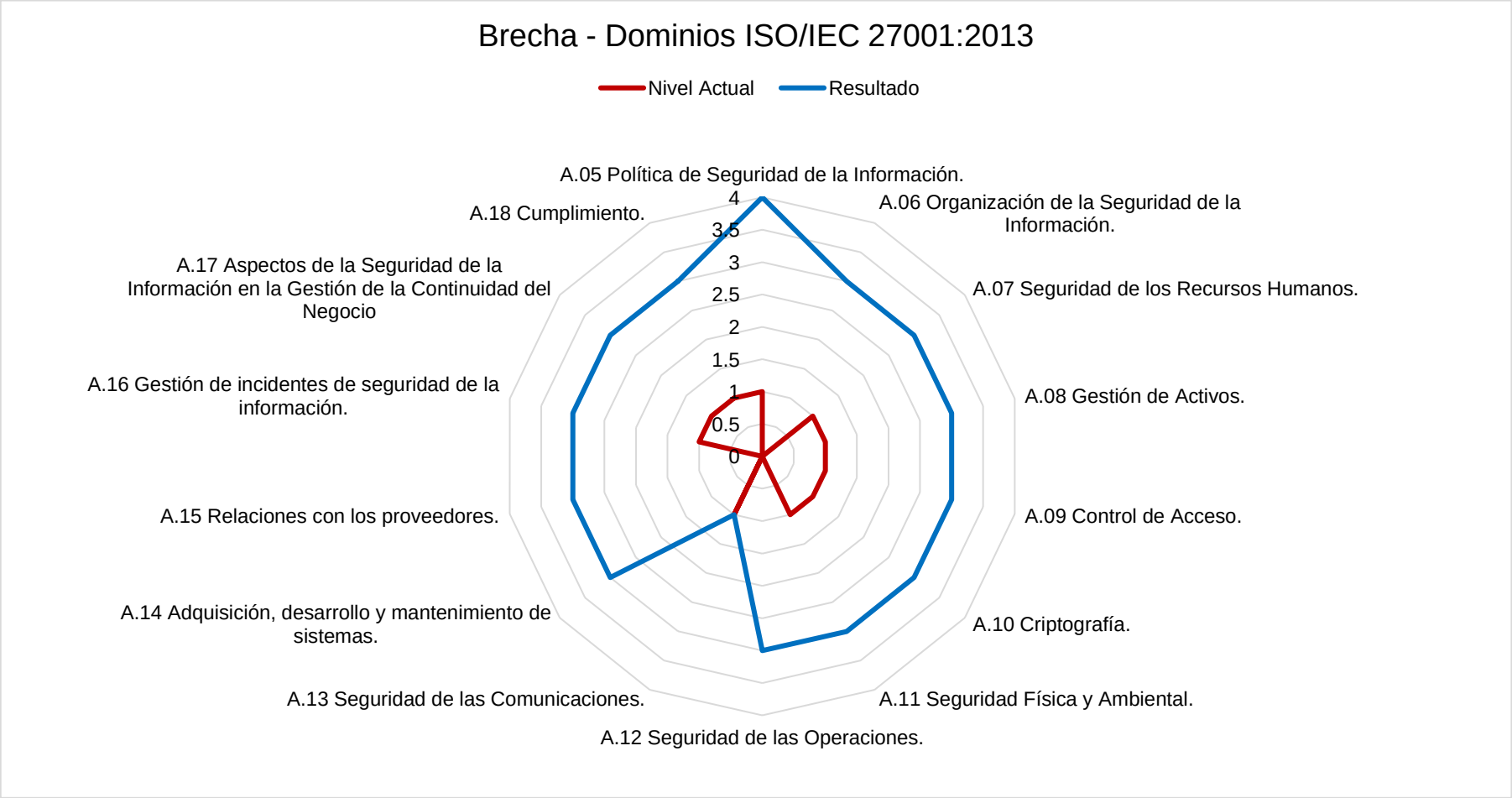
Controles	Nivel Inicial	Reusltado Final
5.1.1 Conjunto de políticas para la seguridad de la información.	1	4
5.1.2 Revisión de las políticas para la seguridad de la información	1	4
6.1.1 Asignación de responsabilidades para la seguridad de la información.	1	4
6.1.2 Segregación de tareas.	0	4
6.1.3 Contacto con las autoridades.	1	3
6.1.4 Contacto con grupos de interés especial.	1	3
6.1.5 Seguridad de la información en la gestión de proyectos.	0	3
6.2.1 Política de uso de dispositivos para movilidad.	0	3
6.2.2 Teletrabajo.	0	3
7.1.1 Investigación de antecedentes.	1	3
7.1.2 Términos y condiciones de contratación.	1	4
7.2.1 Responsabilidades de gestión.	0	3
7.2.2 Concienciación, educación y capacitación en seguridad de la información	0	4
7.3 Cese o cambio de puesto de trabajo.	1	3
7.3.1 Cese o cambio de puesto de trabajo.	1	3
8.1.1 Inventario de activos.	0	4
8.1.2 Propiedad de los activos.	0	2
8.1.3 Uso aceptable de los activos.	1	3
8.1.4 Devolución de activos.	3	4
8.2.1 Directrices de clasificación.	2	3
8.2.2 Etiquetado y manipulado de la información.	1	3
8.2.3 Manipulación de activos.	1	3
8.3.1 Gestión de soportes extraíbles.	0	3
8.3.2 Eliminación de soportes.	0	3
8.3.3 Soportes físicos en tránsito.	0	3
9.1.1 Política de control de accesos.	2	3
9.1.2 Control de acceso a las redes y servicios asociados.	1	2
9.2.1 Gestión de altas/bajas en el registro de usuarios.	0	3
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	1	3
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	0	3
9.2.4 Gestión de información confidencial de autenticación de usuarios.	1	3
9.2.5 Revisión de los derechos de acceso de los usuarios.	1	3
9.2.6 Retirada o adaptación de los derechos de acceso	1	3

9.3.1 Uso de información confidencial para la autenticación.	1	3
9.4.1 Restricción del acceso a la información.	1	3
9.4.2 Procedimientos seguros de inicio de sesión.	1	3
9.4.3 Gestión de contraseñas de usuario.	1	3
9.4.4 Uso de herramientas de administración de sistemas.	1	3
9.4.5 Control de acceso al código fuente de los programas.	1	3
10.1.1 Política de uso de los controles criptográficos.	1	3
10.1.2 Gestión de claves	1	3
11.1.1 Perímetro de seguridad física.	1	3
11.1.2 Controles físicos de entrada.	1	3
11.1.3 Seguridad de oficinas, despachos y recursos.	1	3
11.1.4 Protección contra las amenazas externas y ambientales.	1	3
11.1.5 El trabajo en áreas seguras.	1	3
11.1.6 Áreas de acceso público, carga y descarga.	0	3
11.2.1 Emplazamiento y protección de equipos.	1	3
11.2.2 Instalaciones de suministro.	1	3
11.2.3 Seguridad del cableado.	0	3
11.2.4 Mantenimiento de los equipos.	1	3
11.2.5 Salida de activos fuera de las dependencias de la empresa.	1	3
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	0	3
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	1	3
11.2.8 Equipo informático de usuario desatendido.	1	3
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	1	3
12.1.1 Documentación de procedimientos de operación.	0	3
12.1.2 Gestión de cambios.	0	2
12.1.3 Gestión de capacidades.	0	2
12.1.4 Separación de entornos de desarrollo, prueba y producción.	0	2
12.2.1 Controles contra el código malicioso.	0	3
12.3.1 Copias de seguridad de la información.	2	3
12.4.1 Registro y gestión de eventos de actividad.	0	3
12.4.2 Protección de los registros de información.	1	3
12.4.3 Registros de actividad del administrador y operador del sistema.	1	3
12.4.4 Sincronización de relojes.	0	3
12.5.1 Instalación del software en sistemas en producción.	0	4
12.6.1 Gestión de las vulnerabilidades técnicas.	0	4
12.6.2 Restricciones en la instalación de software.	0	4
12.7.1 Controles de auditoría de los sistemas de información.	1	3
13.1.1 Controles de red.	1	3
13.1.2 Mecanismos de seguridad asociados a servicios en red.	1	3
13.1.3 Segregación de redes.	2	3
14.1.1 Análisis y especificación de los requisitos de seguridad.	1	2
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	1	2
14.1.3 Protección de las transacciones por redes telemáticas.	0	2
14.2.1 Política de desarrollo seguro de software.	0	3
14.2.2 Procedimientos de control de cambios en los sistemas.	0	3
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	0	3
14.2.4 Restricciones a los cambios en los paquetes de software.	0	2
14.2.5 Uso de principios de ingeniería en protección de sistemas.	0	2
14.2.6 Seguridad en entornos de desarrollo.	0	3
14.2.7 Externalización del desarrollo de software.	0	3
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	1	3

14.2.9 Pruebas de aceptación.	0	3
14.3.1 Protección de los datos utilizados en pruebas.	0	3
15.1.1 Política de seguridad de la información para suministradores.	0	3
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	0	3
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	0	3
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	0	3
15.2.2 Gestión de cambios en los servicios prestados por terceros.	1	3
16.1.1 Responsabilidades y procedimientos.	1	3
16.1.2 Notificación de los eventos de seguridad de la información.	1	3
16.1.3 Notificación de puntos débiles de la seguridad.	1	3
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	1	3
16.1.5 Respuesta a los incidentes de seguridad.	1	3
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	1	3
16.1.7 Recopilación de evidencias.	1	3
17.1.1 Planificación de la continuidad de la seguridad de la información.	1	3
17.1.2 Implantación de la continuidad de la seguridad de la información.	1	3
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	1	3
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	0	3
18.1.1 Identificación de la legislación aplicable.	2	3
18.1.2 Derechos de propiedad intelectual (DPI).	1	3
18.1.3 Protección de los registros de la organización.	1	3
18.1.4 Protección de datos y privacidad de la información personal.	2	3
18.1.5 Regulación de los controles criptográficos.	1	3
18.2.1 Revisión independiente de la seguridad de la información.	1	3
18.2.2 Cumplimiento de las políticas y normas de seguridad.	1	3
18.2.3 Comprobación del cumplimiento.	1	3

Fuente: Elaboración Propia.

Figura 21. *Análisis de brechas (pre test y post test).*



Fuente: Elaboración Propia

Tal y como se puede observar en la figura 21 podemos observar cómo evoluciona los controles de seguridad de la información, los mismo que fueron evaluados antes de la implementación la misma que está de color rojo y los resultados obtenidos posterior a la implementación del SGSI.

Posterior al análisis presentamos los resultados obtenidos a partir de la prueba de hipótesis mediante la aplicación de la distribución T de Student para muestras relacionadas.

Tabla 37. *Análisis de brechas (pre test y post test).*

	t	Gl	Sig. (bilateral)
Brechas Inicial – Brechas resultado	-33,942	109	,000

Fuente: Elaboración Propia.

Antes de realizar el análisis estableceremos la hipótesis nula y la hipótesis alterna los cuales son:

- **Hipótesis nula (H0):** El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 no mitiga los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.
- **Hipótesis alterna (H1):** El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021**.**

Mediante el análisis podemos obtener que el grado de significancia es de 0% y el establecido para la investigación fue de 5% por lo tanto al ser menor se aprueba la hipótesis alterna y se rechaza la hipótesis nula.

4.4. Discusión de resultados.

En el transcurso del desarrollo de la investigación se obtuvieron datos de vital importancia los cuales se relacionan con los objetivos planteados como parte de la investigación; tal cual es: *"Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco – 2021".* El objetivo principal de la investigación en curso; y que posterior a la implementación del sistema de gestión de seguridad de la información la misma que está basada en la NTP ISO/IEC 27001 el cual propone dominios y controles con la única finalidad de incrementar la seguridad de la información dentro de la organización y con la finalidad de cumplir el objetivo trazado se realizó la declaración de aplicabilidad seleccionando los controles y dominios que se aplicaran dentro de la organización. Del mismo modo después de haber realizado la implementación del SGSI se realizó un análisis de medición de cada uno de los controles y brechas del SGSI los mismo que se pueden observar en la tabla 36 y figura 21, los mismo que muestran resultados positivos con respecto a la seguridad de la información dentro de la institución debido a que el cumplimiento de cada uno de los controles del SGSI significa que se construye de a pocos una organización con conciencia y disciplina en seguridad de la información.

De la misma manera se coincide con las conclusiones de Vásquez & Delgado (2019) quienes mencionan que "Al implementar el modelo adaptado en base a la norma ISO/IEC 27001 se estableció políticas de seguridad que ayudaron a mejorar la falta de seguridad que había en a la empresa, e establecieron sanciones se incumplan las normas establecidas" (p.86) Asimismo Ccesa (2017) menciona que "los controles de seguridad de la ISO 27002,

permiten establecer métricas, que ayuden a medir la eficacia y eficiencia del SGSI una vez implementados” (p.114).

De la misma manera la gestión de riesgos vistos en los apartados 4.1.7.2. y 4.1.7.3 ayudó a la institución a gestionar de una mejor manera los riesgos asociados a sus activos de información los mismos que se deben de realizar periódicamente con la finalidad de tratar adecuadamente los riesgos; tal y como menciona Castillo (2016) la identificación de los riesgos “permite a la empresa tomar medidas preventivas y correctivas en los procesos que necesitan ser atendidos con mayor brevedad a nivel de seguridad para el mejor funcionamiento de los mismos”(p.130).

CONCLUSIONES

Mediante el diseño del sistema de gestión de la información basa en la NTP ISO/IEC 27001:2014 en el Gobierno Regional Pasco, se obtuvieron resultados positivos los mismo que conllevan a las siguientes conclusiones:

- El análisis de brechas permite tener una mejor adaptación de los niveles de cumplimiento de cada uno de los controles basados en la ISO 27002 los cuales forman parte del anexo A, con ello podemos identificar el estado de madurez de la organización en un nivel inicial del proyecto de implementación del sistema de gestión de seguridad de la información SGSI y poder determinar un nivel deseado de alcance posterior a la implementación del SGSI.
- La aplicación correcta de cada una de las etapas de implementación basadas en la metodología PHVA (planificar, hacer, verificar y actuar); permite tener identificador cada uno de los activos de información de la institución, así como también realizar una gestión adecuada de los riesgos relacionados a los activos de información con la finalidad de tratarlos oportunamente.
- Contar con unas políticas de seguridad de la información bien definidas y difundidas a todos los funcionarios públicos del Gobierno Regional Pasco permite tener una organización con cultura, consciente y disciplinada en seguridad de la información; de la misma manera contribuyen a la mejora continua del sistema de gestión de seguridad de la información.
- Posteriormente a la identificación de los riesgos relacionados a los activos de información de la institución. Se elaboró los controles de seguridad de la información con la finalidad de realizar un tratamiento correcto y disminuir el umbral de riesgo en los cuales se encuentren cada uno de ellos.
- La información generada a partir de la implementación de la NTP ISO/IEC 27001:2014 debe de ser resguardada de manera correcta y usada solo con para los fines para los cuales fueron creados.

- Se encontraron resistencias en todo nivel jerárquicos del Gobierno Regional Pasco a la implementación del presente proyecto, es por ello que se plantearon reuniones de concientización a los directivos con la finalidad de que el proyecto se haga realidad.

RECOMENDACIONES

- El avance acelerado de las tecnologías de la información puede representar oportunidades de mejora contante para el Gobierno Regional Pasco, es por ello que se debe de realizar una revisión periódica de cada uno de los controles aplicados mediante el SGSI; pero ello también conlleva a que se presenten nuevas amenazas es por ello que se debe de realizar análisis periódicos de riesgos con la finalidad de realizar el tratamiento pertinente.
- Se deberá de realizar una campaña de concientización, capacitación y entrenamiento a cada funcionario público del Gobierno Regional Pasco con la finalidad de crear conciencia y fortaleza en seguridad de la información en la institución.
- Se recomienda a la institución a ampliar el presupuesto a todos los niveles de gestión tecnológica con la finalidad de obtener mejores resultados a nivel de seguridad de la información.
- Toda contratación de personal deberá de contemplar dentro de su termino de referencia capacitaciones en computación e informática y seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

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 Pasco Perú*. Universidad Nacional Daniel Alcides Carrión.

Bernal Torres, C. A. (2010). *Metodología de la investigación* (O. Fernández Palma (ed.); Tercera).

Cajusol Torres, L. (2020). *Diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2013 para una empresa de producción y comercialización de productos de consumo masivo*. Universidad Tecnológica del Perú.

Calderon, L. (2018). *Seguridad informática y seguridad de la información*. http://polux.unipiloto.edu.co:8080/00002658.pdf

Carrasco Díaz, S. (2005). *Metodología de la investigación científica* (San Marco (ed.); Primera).

Castillo Collazos, R. E. (2016). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE PIRA APLICANDO LA NORMA ISO/IEC 27001:2013*. Universidad Católica Los Ángeles de Chimbote.

Ccesa, M. (2017). *"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*. UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA.

Cruz Diaz, M. A., & Fukusaki Infantas, S. (2017). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERÚ SAC*. Universidad Sam Martin de Porras.

De Buen, O. (2017). *Sobre la importancia de los trabajos de la Comisión Electrotécnica Internacional (IEC) | Comisión Nacional para el Uso Eficiente de la Energía | Gobierno | gob.mx*. https://www.gob.mx/conuee/articulos/sobre-la-importancia-de-los-trabajos-de-la-comision-electrotecnica-internacional-iec

Estélia, F., Coelho Luiz, S., Segadas, G., & Kowask Bezerra, A. E. (2014). *Gestión de la seguridad de la información* (ESR Colombia (ed.)). REDCEDIA.

Frías, D. (2019). *APUNTES DE CONSISTENCIA INTERNA DE LAS PUNTUACIONES DE UN INSTRUMENTO DE MEDIDA Análisis de la consistencia interna de las puntuaciones de un instrumento de medida*. https://www.uv.es/friasnav/AlfaCronbach.pdf

Fundación Iberoamericana para la Gestión de la Calidad. (2012). *¿Qué es ISO?* https://www.fundibeq.org/informacion/infoiso/que-es-iso

Giraldo Valencia, K. L., & Villalobos Rojas, K. V. (2017). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE GESTIÓN DE INFORMACIÓN, GESTIÓN DE RECURSOS FÍSICOS Y GESTIÓN HUMANA DE LA EMPRESA ACCESO DIRECTO ASOCIADOS LIMITADA, BASADO EN LA NORMA ISO 27001:2013* [Universidad Piloto de Colombia]. http://polux.unipiloto.edu.co:8080/00004102.pdf

Gobierno Regional Pasco. (2017). *Organigrama - Gobierno Regional Pasco*.

http://www.regionpasco.gob.pe/wps/institucional/organigrama

Guardia Palacios, F. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN AJUSTADO A LAS NECESIDADES DE LA CORPORACIÓN MÉDICA CLÍNICA VIDA DE QUIBDÓ.* [UNIVERSIDAD PONTIFICIA'BOLIVARIANA]. https://repository.upb.edu.co/bitstream/handle/20.500.11912/3567/Diseño de un sistema de gestión de seguridad de la información.....pdf?sequence=1&isAllowed=y

Hernández, R., Fernández, C., & Baptista, P. (2013). *Metodología de la investigación* (S. . McGRAW-HILL / INTERAMERICANA EDITORES (ed.); 6°, Vol. 53, Issue 9). https://doi.org/10.1017/CBO9781107415324.004

IBM. (2021). *Política y objetivos de seguridad - Documentación de IBM*. https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

INCIBE, E. (2019). Protección de la información. In *Coleccion: Protege tu empresa*.

Instituto Nacional de Calidad, P. (2022). *Listado de Normas Técnicas Peruanas*. https://cdn.www.gob.pe/uploads/document/file/3241618/NORMAS OBLIGATORIAS 2022.pdf.pdf

ISO. (2013). *ISO - ISO/IEC 27001 — Information security management*. https://www.iso.org/isoiec-27001-information-security.html

ISO Tools Excellence. (2004, April 29). *Desarrollo de la familia de normas ISO 27000*. https://www.pmg-ssi.com/2014/04/desarrollo-de-la-familia-de-normas-iso-27000/

Lopez Alvarado, R. L. (2018). *Guía del investigador*.

Ministerio de Desarrollo Agrario y Riego. (2015). *Normas Técnicas Peruanas*. https://www.midagri.gob.pe/portal/193-exportaciones/importancia-de-la-calidad-en-las-agroexportaciones/695-normas-tecnicas-peruanas

Nieves, A. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA ISO/IEC 27001:2013* [INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO]. https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo Final.pdf?sequence=1&isAllowed=y

Precidencia de Consejo de Ministros. (2016, January 8). *El Peruano - Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición", en todas las entidades integrant*. https://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/

Uso de la NTP ISO/IEC 27001:2014 en las entidaddes integrantes del Sistemas Nacional de Informática, 1 (2015) (testimony of Perú Presidencia del Consejo de Ministros). https://cdn.www.gob.pe/uploads/document/file/357224/Resolución_Ministerial_N__004-2016-PCM20190902-25578-19siyuu.pdf

Rivas Plata, C. E. (2019). *EVALUACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN DISAV SAC APLICANDO LINEAMIENTOS ISO 27001*. UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS.

Solarte, F. (2016). *Modelo PHVA | Sistema de gestión de seguridad informática -*

SGSI. http://blogsgsi.blogspot.com/2016/07/v-behaviorurldefaultvmlo.html

Vásquez, J., & Delgado, M. (2019). *MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN S.R.L.* UNIVERSIDAD DE LAMBAYEQUE.

Vega Briceño, E. (2021). *Seguridad de la información* (Primera Ed, Vol. 1).

ANEXOS

Instrumentos de Recolección de datos.

Universidad Nacional Daniel Alcides Carrión

FACULTAD DE INGENIERIA

ESCUELA DE FORMACION PROFESIONAL DE INGENIERIA DE SISTEMAS

CUESTIONARIO

Estas preguntas forman parte de la evaluación del “Diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021”.

Sexo de la persona encuestada.

Masculino ( ) Femenino ( )

INSTRUCCIONES: Marque solo una alternativa con la que se identifique:

1. **¿Ud. es conocedor de las políticas de seguridad de la información de su institución?**

   Si ( ) No ( )

2. **¿Ud. realiza copias de seguridad de la información generada a partir de sus labores?**

   Si ( ) No ( )

3. **¿Ud. tiene conocimientos acerca del plan de gestión de incidentes?**

   Si ( ) No ( )

4. **¿Ud. cuenta con conocimientos acerca del inventario de activos de información?**

   Si ( ) No ( )

5. **¿Ud. al momento de abandonar su espacio de trabajo bloquea con contraseña su estación de trabajo?**

   Si ( ) No ( )

6. **¿Ud. a menudo cambia la contraseña de su estación de trabajo?**

   Si ( ) No ( )

7. **¿En su entidad cuentan con restricciones de acceso al servicio de internet?**

   Si ( ) No ( )

8. **¿En su entidad cuentan con registros acerca de incidente de seguridad de la información?**

   Si ( ) No ( )

9. **¿Ud. tiene conocimiento que su entidad cuenta con seguridad perimetral?**

   Si ( ) No ( )

10. **¿Ud. cuenta con conocimiento acerca de la gestión de préstamos y traslados de computadoras?**

    Si ( ) No ( )

11. **¿Ud. tiene conocimiento acerca del plan de mantenimiento de equipos tecnológicos dentro de su entidad?**

    Si ( ) No ( )

12. **¿En su entidad cuentan con mecanismos de cifrado en los almacenamientos internos y externos?**

    Si ( ) No ( )

Procedimiento de validez y confiabilidad

Juicio de Experto: Experto 1

Universidad Nacional Daniel Alcides Carrión

FACULTAD DE INGENIERIA

ESCUELA DE FORMACION PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO "JUICIO DE EXPERTOS"

I. DATOS PERSONALES.

a. **APELLIDOS Y NOMBRES DEL EXPERTO:** VICENTE CRISTOBAL, Johannes Avilio

b. **GRADO ACADÉMICO:** INGENIERO DE SISTEMAS Y COMPUTACIÓN.

c. **CARGO E INSTITUCIÓN DONDE LABORA:** INGENIERO DE SEGURIDAD INFORMÁTICA / GOBIERNO REGIONAL PASCO

d. **TITULO DE LA INVESTIGACIÓN:** Diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001 2014 en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco – 2021.

e. **AUTOR DEL INTRUMENTO:** RAMIREZ PARRA, Joel Jaime.

f. **NOMBRE DEL INSTRUMENTO:** CUESTIONARIO.

II. **ASPECTOS DE EVALUACIÓN.**

Después de haber leído las matrices de consistencia y de contrastación de variables; y analizado los ítems del instrumento correspondiente lea Ud. Las siguientes preguntas, dándole un puntaje para su validación marcando los números de puntaje del cuadro según considere (1. Completamente en desacuerdo. 2. En desacuerdo. 3. De acuerdo. 4. Completamente de acuerdo)

N°	Indicadores / Criterios: Preguntas	1	2	3	4	Observaciones
1	**Coherencia:** ¿Las preguntas elaboradas tienen relación con el título y con las variables en estudio?				X	
2	**Claridad:** ¿La redacción de las preguntas y la instrucción del instrumento son adecuadas y se entienden?				X	
3	**Suficiencia:** ¿El instrumento elaborado responde al objetivo de la investigación?				X	
4	**Metodología:** ¿El instrumento elaborado responde al objetivo de la investigación?				X	
5	**Experticia:** ¿Existe una relación del conocimiento de los autores con el contenido de los instrumentos, basado en aspectos teóricos – científicos?				X	
6	**Intencionalidad:** ¿existe intencionalidad expresada en conductas observables en la organización?				X	
7	**Organización:** ¿Existe secuencia lógica y ordenada en las preguntas?				X	
8	**Pertinencia:** ¿Considera usted que las opciones empleadas son correctas para medir las diversas unidades?				X	
9	**Coherencia:** ¿Hay coherencia entre preguntas, en cuanto a forma y estructura?				X	
10	**Actualidad:** ¿Es adecuado el avance de la ciencia y tecnología y la experiencia del tesista?				X	
	TOTAL				40	
	TOTAL GENERAL				40	

Opinión de aplicabilidad: El instrumento planteado por el investigador Ramirez Parra, Joel Jaime Cumple con la coherencia, claridad, experticie y pertinencia y por ello es que se aprueba y sugiere la aplicabilidad del instrumento para los fines pertinentes.

Vicente

Firma del Experto
DNI: 72647100
CIP: 258778
N° Telefónico: 935784094

Juicio de Experto: Experto 2

Universidad Nacional Daniel Alcides Carrión

FACULTAD DE INGENIERIA

ESCUELA DE FORMACION PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO "JUICIO DE EXPERTOS"

I. **DATOS PERSONALES.**

a. **APELLIDOS Y NOMBRES DEL EXPERTO:** PAREDES LOPEZ, ELVIS JESUS

b. **GRADO ACADÉMICO:** INEGNIERO DE SISTEMAS Y COMPUTACION

c. **CARGO E INSTITUCIÓN DONDE LABORA:** UNDAC

d. **TITULO DE LA INVESTIGACIÓN:** Diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.

e. **AUTOR DEL INTRUMENTO:** Bach. Joel Jaime RAMIREZ PARRA

f. **NOMBRE DEL INSTRUMENTO:** Cuestionario

II. **ASPECTOS DE EVALUACIÓN.**

Después de haber leído las matrices de consistencia y de contrastación de variables; y analizado los ítems del instrumento correspondiente lea Ud. Las siguientes preguntas, dándole un puntaje para su validación marcando los números de puntaje del cuadro según considere (1. Completamente en desacuerdo. 2. En desacuerdo. 3. De acuerdo. 4. Completamente de acuerdo)

N°	Indicadores / Criterios: Preguntas	1	2	3	4	Observaciones
1	**Claridad:** Está formulado con lenguaje apropiado				X	
2	**Objetividad:** Está expresado en conductas observadas				X	
3	**Actualidad:** ¿El instrumento de recolección de datos mide correctamente los indicadores?				X	
4	**Organización:** ¿Existe una organización lógica entre (variables e indicadores)?				X	
5	**Suficiencia:** ¿Los instrumentos son suficientes para las mediciones de todos los indicadores?				X	
6	**Intencionalidad:** Es adecuado para valorar aspectos sobre la compresión espacial en relación a las capacidades de define, identifica, señala y ubica.				X	
7	**Consistencia:** ¿Los objetivos y variables están formulados de forma que puedan ser medibles y comprobados?				X	
8	**Coherencia:** ¿Hay coherencia entre las variables, dimensiones e indicadores?				X	
9	**Metodología:** ¿La estrategia responde al propósito de la investigación?				X	
10	**actualidad:** ¿Es adecuado el avance de la ciencia y tecnología y la experiencia del tesista?				X	
	TOTAL				40	
	TOTAL GENERAL				40	

Opinión de aplicabilidad: Ninguno

PAREDES LOPEZ ELVIS JESUS

Juicio de Experto: Experto 3

Universidad Nacional Daniel Alcides Carrión

FACULTAD DE INGENIERIA

ESCUELA DE FORMACION PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO "JUICIO DE EXPERTOS"

I. DATOS PERSONALES.

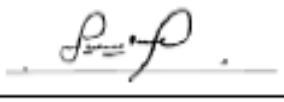
a. **APELLIDOS Y NOMBRES DEL EXPERTO: RAMON VICENTE, LILIANA MADELEINE**
b. **GRADO ACADÉMICO: INGENIERO**
c. **CARGO E INSTITUCIÓN DONDE LABORA: INDEPENDIENTE**
d. **TITULO DE LA INVESTIGACIÓN:** Diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.
e. **AUTOR DEL INTRUMENTO:** Bach. Joel Jaime RAMIREZ PARRA
f. **NOMBRE DEL INSTRUMENTO:** Cuestionario

II. ASPECTOS DE EVALUACIÓN.

Después de haber leído las matrices de consistencia y de contrastación de variables; y analizado los ítems del instrumento correspondiente lea Ud. Las siguientes preguntas, dándole un puntaje para su validación marcando los números de puntaje del cuadro según considere (1. Completamente en desacuerdo. 2. En desacuerdo. 3. De acuerdo. 4. Completamente de acuerdo)

N°	Indicadores / Criterios: Preguntas	1	2	3	4	Observaciones
1	**Claridad:** Está formulado con lenguaje apropiado				X	
2	**Objetividad:** Está expresado en conductas observadas				X	
3	**Actualidad:** ¿El instrumento de recolección de datos mide correctamente los indicadores?				X	
4	**Organización:** ¿Existe una organización lógica entre (variables e indicadores)?				X	
5	**Suficiencia:** ¿Los instrumentos son suficientes para las mediciones de todos los indicadores?			X		
6	**Intencionalidad:** Es adecuado para valorar aspectos sobre la compresión espacial en relación a las capacidades de define, identifica, señala y ubica.			X		
7	**Consistencia:** ¿Los objetivos y variables están formulados de forma que puedan ser medibles y comprobados?				X	
8	**Coherencia:** ¿Hay coherencia entre las variables, dimensiones e indicadores?				X	
9	**Metodología:** ¿La estrategia responde al propósito de la investigación?				X	
10	**actualidad:** ¿Es adecuado el avance de la ciencia y tecnología y la experiencia del tesista?				X	
	TOTAL			8	32	
	TOTAL GENERAL				40	

Opinión de aplicabilidad: El instrumento es aplicable para el trabajo realizado.



RAMON VICENTE, Liliana M.

Alfa de Cronbach	N de elementos
0,708	12

Posterior a la obtención de los resultados procedemos al análisis es por ello que basado en las sugerencias de Frías (2019) quien menciona que “coeficiente alfa >.7 es aceptable” (p.7) entonces podemos mencionar que el instrumento de recolección de datos utilizado en la presente investigación es confiable.

Matriz de Consistencia

“Diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021”

PROBLEMA	OBJETIVO	HIPOTESIS	VARIABLES
GENERAL	**GENERAL**	**GENERAL**	**INDEPENDIENTE**
¿De qué manera el diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021?	Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.	El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de los pilares de la seguridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.	NTP ISO/IEC 27001:2014.
ESPECIFICOS	**ESPECIFICOS**	**ESPECIFICOS**	**DEPENDIENTE**
¿De qué manera el diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la confidencialidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021?	Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de la confidencialidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.	El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la confidencialidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.	Sistema de gestión de seguridad de la información.
¿De qué manera el diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la integridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021?	Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar los riesgos de la integridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.	El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la integridad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.	
¿De qué manera el diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la disponibilidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021?	Diseñar un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para mitigar de la disponibilidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021.	El diseño de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 mitiga los riesgos de la disponibilidad de la información en la Sub Gerencia de Racionalización y Sistemas TIC del Gobierno Regional Pasco - 2021	