UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

FACULTAD DE INGENIERÍA

ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TRABAJO DE SUFICIENCIA PROFESIONAL

Estudio evaluativo para la implementación de un sistema de gestión de seguridad de la información en las Oficinas Departamentales de Estadística e Informática bajo el lineamento NTP-ISO/IEC 27001:2014: caso de estudio ODEI Pasco

Para optar el título profesional de:
Ingeniero de Sistemas y Computación

Autor:
Bach. Jose Antonio MENDOZA MAURICIO
Asesor:
Mg. Teodoro ALVARADO RIVERA

Cerro de Pasco - Perú - 2025

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

FACULTAD DE INGENIERÍA

ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TRABAJO DE SUFICIENCIA PROFESIONAL

Estudio evaluativo para la implementación de un sistema de gestión de seguridad de la información en las Oficinas Departamentales de Estadística e Informática bajo el lineamento NTP-ISO/IEC 27001:2014: caso de estudio ODEI Pasco

Sustentada y aprobada ante los miembros del jurado:

_____	_____
Dr. Percy RAMIREZ MEDRANO	Mg. Oscar Clevorio CAMPOS SALVATIERRA
PRESIDENTE	MIEMBRO

_____

Mg. Williams Antonio MUÑOZ ROBLES

MIEMBRO

Universidad Nacional Daniel Alcides

Carrión Facultad de Ingeniería

Unidad de Investigación

INFORME DE ORIGINALIDAD N° 236-2024-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, El Trabajo de suficiencia Profesional ha sido evaluado por el software antiplagio Turnitin Similarity, que a continuación se detalla:

TRABAJO DE SUFICIENCIA PROFESIONAL

"Estudio evaluativo para la implementación de un sistema de gestión de seguridad de la información en las Oficinas Departamentales de Estadística e Informática bajo el lineamento NTP-ISO/IEC 27001:2014: caso de estudio ODEI Pasco"

Apellidos y nombres del tesista:

Bach. MENDOZA MAURICIO, José Antonio

Apellidos y nombres del Asesor:

Mg. ALVARADO RIVERA, Teodoro

Escuela de Formación Profesional

Ingeniería de Sistemas y Computación

Índice de Similitud

9 %

APROBADO

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

Cerro de Pasco, 16 de diciembre del 2024

Firmado digitalmente por MEJIA CACERES Reynaldo FAU 20154605046 soft
Motivo: Soy el autor del documento
Fecha: 16.12.2024 22:16:25 -05:00

DEDICATORIA

El presente trabajo se lo dedico a mi Señora Madre, quien gracias a su paciencia y dedicación ahora soy lo que soy una persona de bien.

A mi familia por ser mis verdaderos amigos y confidentes, y lo más valioso que Dios me dio.

RESUMEN

El presente Trabajo de Suficiencia Profesional realiza un estudio evaluativo sobre la seguridad de la información en la ODEI de Pasco bajo el marco normativo NTP-ISO/IEC 27001:2014, se realizó con el objetivo de proponer su implantación alineados a la Política General de la Seguridad de la Información del INEI para ello se identificaron los activos de información en diferentes grados de importancia de cada área de la entidad en estudio, estas se valoraron por su nivel de importancia considerando las dimensiones básicas establecidas por la norma; cuales son disponibilidad, integridad y confidencialidad. Posteriormente se realizó el análisis de riesgos utilizando la metodología MAGERIT V.3 la cual permite identificar las amenazas potenciales en el manejo de los activos de información identificando el origen, el riesgo y las vulnerabilidades en los diferentes aspectos involucrados tales como la organización, la información, el software, el hardware, las comunicaciones, los elementos auxiliares, las instalaciones y los recursos humanos. Como siguiente paso se realizó la Declaración de Aplicabilidad considerando el estado actual de la implementación de la Norma NTP-ISO/IEC 27001:2014 en la ODEI Pasco para ello se usó la tabla de requerimientos descritos en la norma identificando el estado de implementación de los controles de seguridad en la ODEI Pasco en relación a los riesgos ya descritos anteriormente; realizando su respectivo análisis. Finalmente se declararon los hallazgos encontrados y las recomendaciones para que en base a ellos la alta dirección defina decisiones y en lo posterior determinar un SGSI para las ODEI a nivel nacional.

Palabras clave: seguridad de la Información, activo de la Información, riesgo, MAGERIT, controles de seguridad.

ABSTRACT

This Professional Sufficiency Work carries out an evaluative study on information security at the ODEI of Pasco under the regulatory framework NTP-ISO / IEC 27001: 2014, it was carried out with the objective of proposing its implementation aligned with the General Policy of Information Security of the INEI for this, the information assets were identified in different degrees of importance of each area of the entity under study, these were valued by their level of importance considering the basic dimensions established by the standard; which are availability, integrity and confidentiality. Subsequently, the risk analysis was carried out using the MAGERIT V.3 methodology, which allows to identify potential threats in the management of information assets by identifying the origin, risk and vulnerabilities in the different aspects involved such as the organization, information, software, hardware, communications, auxiliary elements, facilities and human resources. The next step was to prepare a Declaration of Applicability, considering the current status of implementation of the NTP-ISO/IEC 27001:2014 Standard at the Pasco ODEI. To do this, the table of requirements described in the standard was used to identify the status of implementation of security controls at the Pasco ODEI in relation to the risks described above, and to conduct their respective analysis. Finally, the findings and recommendations were presented so that senior management could use them to make decisions and subsequently develop an ISMS for the ODEIs nationwide.

Keywords: information security, information asset, risk, MAGERIT, security controls.

INTRODUCCIÓN

Actualmente, los sistemas usados en el almacenamiento, procesamiento y envió de información están presentes en una amplia gama de instituciones de diversos rubros y funciones. Los sistemas de información son cada día más complejos debido a la globalización, lo que implica que las distancias geográficas no son una dificultad. Así, existe un número cada vez mayor de personas que pueden acceder a información que podría ser básica para las distintas organizaciones y entidades en las que trabajan. No obstante, se añade el riesgo que supone la fuga de datos delicados, ya sea por personas que tienen acceso a tal información, bien por extraños que han llegado a ella a través de un sistema de ataque.

En la actualidad, la seguridad de la información es de gran relevancia en las instituciones públicas y privadas, ya que asegura el almacenamiento, procesamiento y cambio de información, manteniendo las bases de la confidencialidad, integridad y accesibilidad de la información. Por otra parte, la calidad del servicio es una auténtica ventaja competitiva de una organización, reflejando la responsabilidad de las personas que componen un organismo encaminado al servicio del usuario o de la población en general, donde las particularidades más significativas son la tangibilidad, confianza y capacidad de respuesta.

La seguridad de la información resulta esencial para las organizaciones en la era de la información, diversos aspectos están implicados para su confidencialidad, pues la sociedad depende de la información almacenada para toma de decisiones en las empresas y entes gubernamentales. Es así como, la seguridad de la información juega un papel muy importante en las instituciones públicas es el caso del Instituto Nacional de Estadística e Informática en adelante INEI quien tiene el encargo de generar y manejar información estadística vital para la toma de decisiones la cual debe ser resguardada y protegida por ende las oficinas departamentales deben custodiar dichos activos de la información, para nuestro caso la Oficina Departamental de Estadística e Informática Pasco.

El presente informe de suficiencia profesional consta de cuatro capítulos:

En el capítulo I se describen los datos generales incluyendo para ello el título del trabajo de suficiencia profesional, su delimitación y fechas de inicio y termino.

En el capítulo II se describe la planificación del trabajo de suficiencia profesional realizando una breve descripción, se realiza la justificación de trabajo de suficiencia profesional determinando los objetivos tanto el objetivo general como los objetivos específicos.

En el capítulo III se describe el marco teórico con el fin de ubicar el presente trabajo de suficiencia profesional y se definen los antecedentes, las bases teóricas científicas y se definen los términos básicos.

En el capítulo IV se describe el desarrollo de la experiencia siendo la parte modular del trabajo de suficiencia profesional es aquí donde se realiza el marco normativo del INEI, posteriormente la Política General del INEI, se define la organización estructural del INEI y se desarrolla la intervención motivo del trabajo de suficiencia profesional.

Por último, se realizaron las conclusiones y recomendaciones generales y su respectivo anexo.

EL AUTOR

ÍNDICE

INDICE DE TABLAS

INDICE DE FIGURAS

CAPITULO I

DATOS GENERALES

1.1. Título del trabajo de suficiencia profesional

Estudio evaluativo para la implementación de un sistema de gestión de seguridad de la información en las Oficinas Departamentales de Estadística e Informática bajo el lineamento NTP-ISO/IEC 27001:2014: caso de estudio ODEI Pasco.

1.2. Delimitación del trabajo de suficiencia profesional

El presente trabajo de suficiencia profesional se desarrolló en la Oficina Departamental de Estadística e Informática de Pasco en adelante ODEI Pasco.

1.3. Fecha de inicio y fecha de término

Fecha de inicio: 1 de noviembre del 2023

Fecha de término: 1 de marzo del 2024

CAPITULO II

PLANIFICACIÓN DEL TRABAJO

2.1. Descripción del trabajo de suficiencia profesional

El trabajo de suficiencia profesional se desarrolló en las instalaciones de la ODEI Pasco, realizando en primer lugar entrevistas al Oficial de Seguridad de la Información del INEI con el fin de conocer la Política General de la Seguridad de la Información del INEI; marco normativo y sus avances, posteriormente al encargado del Área de Informática de la ODEI Pasco con el fin de recopilar información para identificar los activos información relevantes, analizando su nivel de seguridad identificando amenazas y vulnerabilidades.

Para el estudio evaluativo de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se realizaron los procedimientos según la metodología MAGERIT V.3 con la finalidad de proponer la implementación de un SGSI y así asegurar los activos de información en este caso de la ODEI de Pasco cumpliendo con la Política General Seguridad de la Información del INEI para lo cual se realizaron las siguientes actividades:

- Identificación de Activos en la ODEI Pasco; resultando de la entrevista al encargado del Área de Informática de la ODEI Pasco e inventario de activos tangibles e intangibles.

- Análisis de riesgos en la ODEI Pasco; se identificaron y evaluaron las amenazas y vulnerabilidades de los activos; y se calcularon los riesgos y definieron los niveles de riesgo definiendo la probabilidad de ocurrencia e impacto.
- Declaración de Aplicabilidad; se elaboró la declaración de aplicabilidad de controles (SOA) en la ODEI Pasco realizando la comparativa con los controles de seguridad de la Política General de la Seguridad de la Información del INEI.
- Hallazgos encontrados; definición de propuestas para la implementación de un SGSI; contemplando todos los factores de la institución tales como recursos humanos, gestión de activos, gestión de incidentes, uso de internet entre otros.

2.2. Justificación

El presente trabajo de suficiencia profesional se justifica ya que el INEI está llegando a manejar una gran cantidad de información sensible para la toma de decisiones por lo que se requiere que esta política de seguridad de la información se replique en todos sus niveles de organización en este caso las ODEI pues la falta de protección de esa información puede conllevar a su uso indebido. Es así como el presente trabajo podrá servir como un indicador para su implantación en todos sus niveles de organización y de base para futuras investigaciones en el marco de implementación de sistemas de gestión de seguridad de la información en las entidades públicas bajo la norma NTP-ISO/IEC 27001:2014.

De igual manera el presente trabajo de suficiencia profesional presenta una implicancia social pues el cumplimiento es obligatorio por parte de todos los trabajadores del INEI y de la ODEI de Pasco y los beneficiarios serán los usuarios o personas que necesiten de los servicios de información que ofrece el INEI y la ODEI de Pasco.

Las implicaciones prácticas resultan significativas pues se establecerán propuestas que ayuden a solucionar un problema real, teniendo en cuenta criterios necesarios para la alineación de la ODEI Pasco a la Política General de la Seguridad de la Información del INEI de la ODEI.

El beneficio metodológico brindado se evidenciará en poder evaluar la seguridad de la información y el control de riesgos en la ODEI de Pasco bajo los lineamientos de la norma NTP-ISO/IEC 27001:2014; es así como la contribución vendrá dada por una ruta metodológica seguida por quien investiga para obtener el análisis deseado.

2.3. Objetivos del trabajo de suficiencia profesional

2.3.1. Objetivo general

Realizar el estudio evaluativo de seguridad de la información en la ODEI de Pasco proponer recomendaciones para su implantación bajo los lineamientos de la Política General de la Seguridad de la Información del INEI según la norma NTP-ISO/IEC 27001:2014.

2.3.2. Objetivos específicos

Realizar un inventario de activos para determinar sus vulnerabilidades y riesgos en la ODEI de Pasco según la norma NTP-ISO/IEC 27001:2014.

Identificar los riesgos y vulnerabilidades de los activos informáticos y de información definiendo su probabilidad de ocurrencia e impacto en la ODEI de Pasco.

Identificar y jerarquizar los problemas de la seguridad de la información en la ODEI de Pasco bajo el lineamiento de la norma NTP-ISO/IEC 27001:2014.

CAPITULO III

MARCO TEÓRICO

3.1. Antecedentes

3.1.1. Internacionales

Espinel (2017); “Proyecto de investigación estrategia para implementar un sistema de gestión de la seguridad de la información basado en la norma ISO 27001 en el área de TI para la empresa Market Mix”. En el estudio se planteó como objetivo principal establecer la mejor estrategia para implantar un Sistema de Gestión de Seguridad de la Información basada en la norma ISO 27001. La investigación se basó en un enfoque mixto cualitativo y cuantitativo el tipo de estudio fue descriptivo, la población se compuso por 200 trabajadores de la empresa Market Mix, el instrumento y técnica empleada fue la encuesta/cuestionario. Los resultados muestran que el 7% de su personal presenta un conocimiento excelente, el 29% su conocimiento es bueno, el 32% su conocimiento es regular, el 13% su conocimiento es muy deficiente y el 20% no tiene conocimiento. Se deduce que gran parte de los trabajadores siendo un 65% que labora en el área de TI posee niveles de conocimiento de seguridad de la información muy bajos o carece de ellos; resulta bastante significativo crear labores o acciones que lleven a que los trabajadores se nivelen con respecto a

los conocimientos de seguridad informática. La investigación guarda relación con el presente estudio porque se pretende realizar un sistema de gestión de la seguridad de la información basado en las normas ISO 27001.

Jácome (2019); en su investigación titulada “Diseño de una política de gestión de seguridad de la información para el área de imagenología del hospital general docente de Calderón utilizando los estándares ISO 27001 e ISO 27799”. El objetivo principal de su investigación era el de plantear una política de gestión de seguridad de la Información analizando las normas ISO 27001 e ISO/ 27799, para así resguardar la información como los activos fijos informáticos, en el estudio se utilizó la metodología mixta usando el cuestionario y la entrevista para recoger los datos. El autor concluye que se pudo establecer un antes y un después en la administración de la información de dicho centro hospitalario; no siendo necesario gastos adicionales, pues el área de la salud en la nación está creciendo y enmarcado legalmente de una manera no muy bien definida. Dicho marco legal debe aplicarse para garantizar la confidencialidad, integridad y disponibilidad de la información del paciente generado al momento de aplicar el tratamiento por parte de los médicos. Se logró corroborar que la implementación de controles para cada uno de los procesos informáticos existentes es necesaria.

3.1.2. Nacionales

Diaz & Infantas (2017); estudiaron el “Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Peru SAC”. Se plantearon como propósito general aminorar los riesgos a los que se encuentran expuestos los activos de información de la clínica aludida para ello se usó el método Plan-Do-Check-Act o Ciclo de Deming propuesto por la ISO/27001:2005. Los investigadores concluyen que ejecutar un Sistema de Gestión de Seguridad de la Información fue la premisa para conseguir el objetivo fundamental su ejecución fue

desarrollada mediante el plan y puesta en práctica de estrategias para supervisar eficazmente el acceso a la información, tratando de garantizar la confidencialidad, integridad y disponibilidad de los activos de información limitando los riesgos de seguridad de estos. El desarrollo y la ejecución de la Política de Seguridad de la Información resultó significativa, pues mostró la obligación de la organización con la seguridad de los datos, aparte de establecer trabajos y obligaciones, estableció las reglas de como la organización debe ser supervisada. Se logró inferir que implementando controles se hace un mejor tratamiento de riesgos para Medcam Perú SAC; los mismos que se planificaron en función de algunas variables como el costo de la implementación, la efectividad para la mitigación del riesgo identificado y el análisis costo-beneficio. La sensibilización del personal respecto a la seguridad es imprescindible para que el Sistema de Gestión de Seguridad de la Información pueda llevarse a cabo con éxito en la organización. Sensibilizar sobre los problemas de seguridad de la información refuerza el sistema ejecutado y crea una mejora constante.

La presente investigación guarda relación con el estudio de Diaz & Infantas (2017) pues propone el diseñar e implementar un Sistema de Gestión de Seguridad de la Información para proteger los activos de información en la clínica Medcam Perú SAC.

Mendoza (2018); en su tesis titulada, “Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018”. Se planteó mejorar los niveles de seguridad de la información en el gobierno local para ello se utilizó como metodología del método hipotético-deductivo con un enfoque cuantitativo con un diseño preexperimental del tipo de estudio aplicada, el instrumento y técnica para recoger los datos fue la encuesta/cuestionario. El autor de esta investigación concluye que en los gobiernos locales es necesario alinear con la gerencia de TI las estrategias del negocio igualmente es preciso conservar información de calidad para apoyar las

decisiones por lo que se requiere que el ente tenga mapeado la totalidad de sus activos y cada activo gestionar sus riesgos a los que conlleva para que así sea posible ejecutar un apropiado control y conservar los riesgos en un nivel aceptable; asimismo se sugiere efectuar evaluaciones reiteradas de los niveles de riesgo, para monitorear apropiadamente la efectividad de los controles aplicados.

3.2. Bases teóricas científicas

3.2.1. Seguridad de la Información

La seguridad de la información es básica para que las organizaciones consigan sobrevivir en la era de la información ya que la sociedad cada vez más incluye en su día a día información almacenada en sistemas informáticos para la toma de decisiones. Es importante no confundir el término seguridad de la información, con el termino seguridad informática, puesto que si bien el primero engloba al segundo no son sinónimos. Según Gui S. G. (s.f.):

> Es importante no confundir el término seguridad informática, con el término seguridad informática, puesto que si bien el primero engloba al segundo no son sinónimos. La seguridad informática se ocupa únicamente de la seguridad de los sistemas de información y, por tanto, queda circunscrita al ámbito de la información automatizada, siendo por ello un término mucho más restrictivo que el de seguridad de la información, que se ocupa de la información en todas sus formas (oral, escrita, impresa, electrónica, óptica, electro-magnética…) y en cualquier momento de su ciclo de vida (creación o captura, mantenimiento, distribución y uso, y almacenamiento, archivo y destrucción), para protegerla de cualquier amenaza que pudiera suponer pérdida o disminución del valor de la misma. (p. 7)

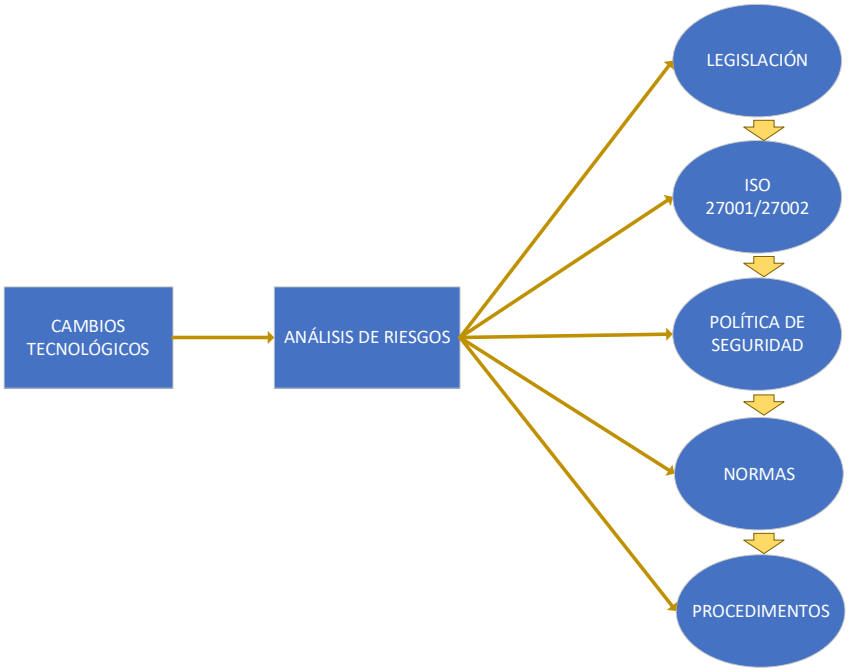
Actualmente existe una creciente atención por parte de las organizaciones del valor total y el conocimiento de las vulnerabilidades de sus activos en relación con la seguridad, la seguridad de la información es

fundamental para garantizar la competitividad, la rentabilidad, el cumplimiento de las exigencias legales y la imagen de la organización en el mercado empresarial tanto en la sociedad en general como en el ámbito privado. En dichos entornos la seguridad de la información es una parte que empodera a las organizaciones por ejemplo en el e-government (gobierno electrónico) y el e-commerce (comercio electrónico).

La seguridad de la información incorpora la garantía de datos, sistemas, activos y diferentes recursos contra debacles, errores (deliberados o no) y manipulación no autorizada. Como lo indica la norma ISO/IEC 27002: 2007, la seguridad de la información es el seguro de los datos contra diferentes tipos de peligros para garantizar la continuidad empresarial, limitar los riesgos, aumentar el retorno sobre la inversión y las oportunidades de negocio. La seguridad de la información se adquiere mediante la ejecución de una serie de controles que abarcan políticas, medidas, sistemas, estructuras organizacionales y funciones de hardware y software. Específicamente, los controles deben establecerse, llevarse a cabo, verificarse, evaluarse y trabajarse de forma continua para cumplir con los objetivos del negocio y de seguridad de la organización.

Figura 1:

Visión general de la seguridad de la información



Los cambios tecnológicos siempre están presentes en el día a día en las organizaciones por lo que se evidenciaran vulnerabilidades y riesgos, requiriéndose por ello una evaluación de riesgos eficiente y actualizada esto permitirá que los niveles de riesgos y la forma de tratarlos sean levantados simultáneamente se precisa conocer las leyes que la organización está obligada a seguir y recopilar los requerimientos de seguridad precisos para cumplir con ella; luego es necesario ubicar los controles obligatorios y determinados por el análisis de riesgos con la utilización de las normas de seguridad, partiendo de los controles registrados se requiere crear políticas, normas y procedimientos para su aplicación.

Los principales objetivos de la seguridad de la información son los siguientes:

- **Confidencialidad.** Es un estado de disponibilidad de información usado únicamente por los usuarios en los procesos y dispositivos autorizados.

- **Integridad.** Se refiere a la modificación de información no autorizada como en el caso de información agregada o destruida es de vital importancia garantizar su integridad, en los casos donde la información sea de gran valor para evitar que se pierda y de igual manera cuando los datos se quieran cambiar de forma intencional para desinformar al destinatario.
- **Accesibilidad.** Es el acceso oportuno y confiable a la información y los servicios de información. Ahora bien, las características de una infracción de accesibilidad puede **ser** una falla de software/hardware o un ataque de denegación de servicio distribuido (DDoS).
- **Autenticidad.** Es la capacidad de ubicar exclusivamente al autor fuente de información, la autenticidad de datos electrónicos es verificada por medios como una firma digital electrónica.
- **No repudio.** El no repudio permite establecer la autoría de la información donde el emisor no puede negar el hecho de su envío o recepción. Se puede garantizar por medio de una firma digital o protocolos criptográficos.

3.2.2. Sistema de Gestión de Seguridad de la Información (SGSI)

Según la Plataforma del Estado Peruano (s.f.):

Un Sistema de Gestión de Seguridad de la Información (SGSI) consta de políticas, procedimientos, directrices y recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. El análisis de los requisitos para la protección de los activos de información y la aplicación de los controles adecuados para garantizar la protección de estos

activos de información, según sea necesario, contribuye a la implementación exitosa de un SGSI.

Este sistema ha evolucionado con la norma ISO-17799 del año 2000, convirtiéndose de esta manera en la familia ISO 27000 desde el 2005 pretende ser una norma internacional que brinda sugerencias para ejecutar la gestión de la seguridad de la información, se encuentra orientada a comenzar, instaurar y conservar la seguridad de la información de una organización.

La norma ISO 27001:2005 es de suma importancia ya que se encuentra encaminada a crear, efectuar, maniobrar, supervisar, examinar, conservar y optimizar un Sistema de Gestión de Seguridad de la Información (SGSI) y se encuentra alineada con la norma ISO 9001 con el objetivo permitir la implementación y operación permanente compuesta con sistemas de gestión relacionados. En octubre del 2022 fue actualizada la norma de requisitos del SGSI designada ISO27001:2022, y de igual manera la norma del Código de Práctica del Sistema de Gestión de Seguridad de la Información llamada ISO27002:2022.

3.2.3. ISO 27001

Según ISOTools Excellence (2014):

La norma ISO 27001 es una solución y la mejora continua la cual puede desarrollarse mediante un SGSI. La norma ISO 27001 permite evaluar los riesgos capaces de poner en peligro la información de una organización tanto propia como datos de terceros. Por otro lado, ayuda a instituir los controles y estrategias más apropiadas para eliminar o disminuir tales riesgos. En otras palabras, es un estándar que permite desarrollar un SGSI en un contexto empresarial o institucional y como todos los principios proporciona los procedimientos más idóneos en este ámbito. El ISO 27001 es un sistema que depende del ciclo de mejora continua o Deming denominado ciclo PHVA (Planificar, Hacer, Verificar y Actuar). El ISO 27001 ayuda a establecer las

exigencias de un SGSI y hacer la correlación con el ciclo PHVA propuesto por ISO 27001, se dividiría en estos pasos, cada uno de ellos conectado a una progresión de actividades. (p. 4)

El ISO 27001 se puede llevar a cabo en cualquier organización impulsada por los ingresos, privada o pública, pequeña o grande. Dicha norma está redactada por los mejores expertos en la materia y da un procedimiento para llevar a cabo la gestión de seguridad de la información en el interior de una organización. Asimismo, permite asegurar la organización.

Las actividades necesarias para la implementación del ISO 27001 son las siguientes:

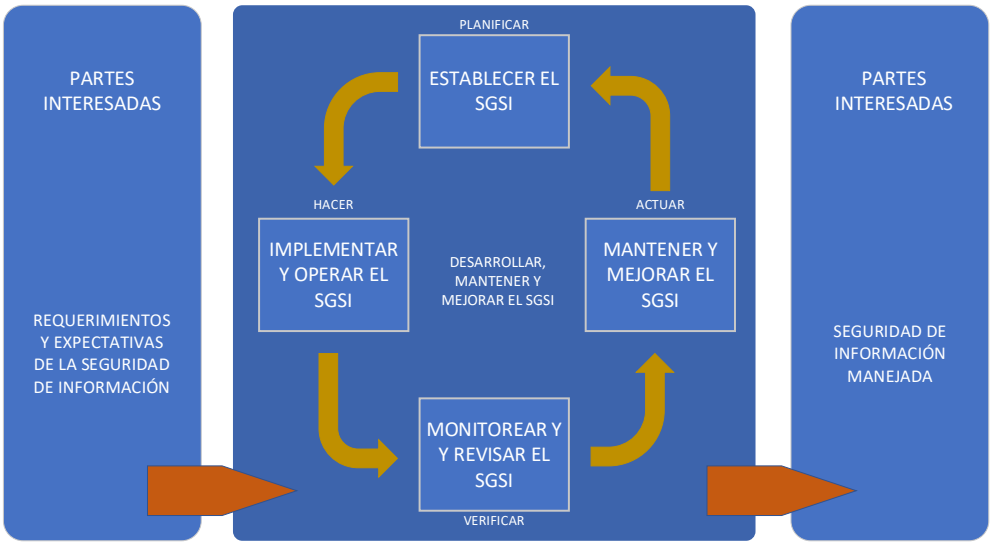
- Definición del alcance del SGSI
- Definición de las políticas de seguridad
- Análisis y gestión de riesgos
- Identificación de riesgos
- Realizar un tratamiento de los riesgos
- Elaboración de la declaración de aplicabilidad de controles
- Desarrollo del plan de tratamiento de riesgos
- Definir un sistema de métricas
- Generar un programa para generar conciencia en la organización
- Gestión de recursos y operaciones
- Monitoreo de incidencias
- Elaboración de documentación asociada

3.2.4. Modelo PHVA

El modelo PHVA es de mejora continua ideal en las organizaciones y esta supervisado bajo la norma ISO 27001, aplicándose para estructurar la totalidad de los procesos del SGSI.

Figura 2:

Modelo PHVA



Nota: La figura muestra la secuencia del modelo PHVA. Fuente: https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

Este modelo abarca una serie de acciones en la secuencia señalada por las letras que combinan las siglas: P (plan: planear), H (Hacer, ejecutar), V (verificar, controlar) y finalmente A (actuar, actuar de manera correctiva). A continuación, se definirá cada uno una de estas fases:

- **Planear.** En esta etapa se crean las políticas, objetivos, procesos y procedimientos del SGSI importantes para la gestión del riesgo y la mejora de la seguridad de información para así poder conseguir resultados conforme a las políticas y objetivos generales de una organización.
- **Hacer.** Aquí se implementan y manejar las políticas, controles y procesos del SGSI, en esta etapa se implementan los cambios planteados en la fase anterior.
- **Verificar.** En esta fase se evalúa y mide el desempeño de un proceso con base en la política y los objetivos en determinados periodos de tiempo para revisar si se cumplen con los cambios previstos en la planificación.

- **Actuar.** Realizadas las mediciones y verificaciones se pone en práctica las acciones correctivas y preventivas basándose en los resultados de la auditoría interna del SGSI para así poder conseguir la mejora continua en los procesos del SGSI.

3.2.5. Metodología MAGERIT

Acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información mayormente utilizado por entidades públicas para minimizar y gestionar el riesgo de implantación y uso de tecnologías de información actualmente se encuentra en la Versión 3, esta metodología implementa el proceso de gestión de riesgos bajo el marco de trabajo del ISO 31000 ubicándose en contexto en la planificación de los SGSI del ISO 27001.

En MAGERIT se formalizan las actividades para realizar una correcta gestión de riesgos, estas son:

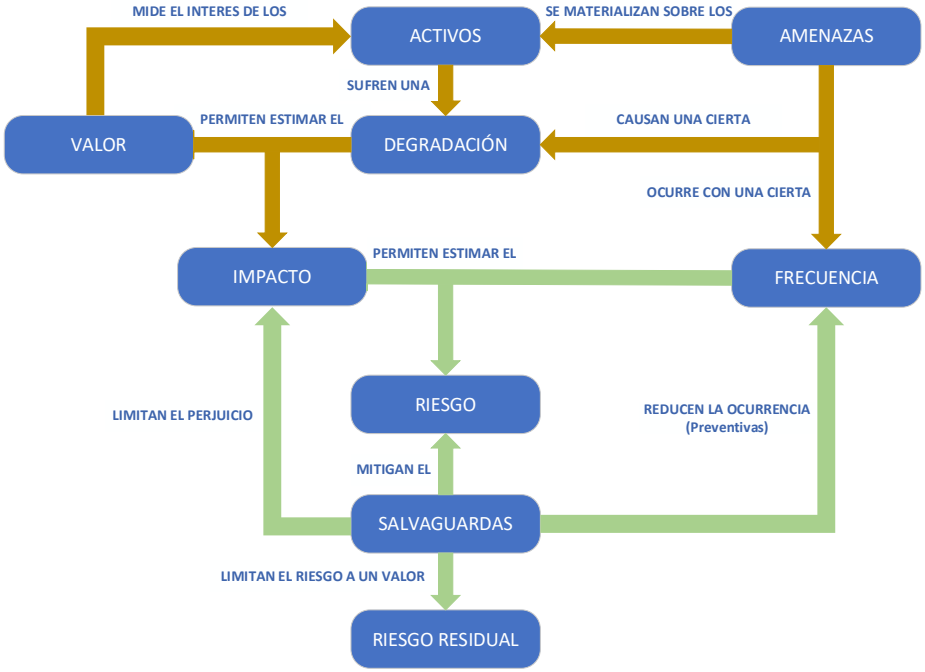
- El Método de Análisis de Riesgos (MAR)
- El Proyecto de Análisis de Riesgos (PAR)
- El Plan de Seguridad (PS)

Las dos grandes tareas que se realizan mediante esta metodología son la de analizar el riesgo y dar el tratamiento respectivo considerando para ello tres elementos básicos cuales son los activos, las amenazas y los salvaguardas cuyo tratamiento estiman el impacto y el riesgo.

En el proceso de gestión de riesgos de MAGERIT se realiza en primer lugar la determinación del contexto con el fin de determinar los parámetros y condiciones internas y externas posteriormente se realiza la identificación, análisis y evaluación de riesgos para tener en cuenta puntos de peligro cuantificando y cualificando sus posibles consecuencias para así determinar si se va a aceptar o trabajar en su tratamiento, también se realiza la comunicación y consulta a las partes interesadas y por último hacer un adecuado seguimiento y revisión.

Figura 3

Metodología MAGERIT



Nota: La figura muestra los elementos y el ciclo de la metodología MAGERIT V.3. Fuente: http://calidadtic.blogspot.com/2014/02/gestion-del-riesgo.html

A continuación, se definen los elementos de la metodología MAGERIT V.3:

- **Activos.** Se refiere al componente de un sistema de información necesario para su correcto funcionamiento y cumplimiento de objetivos en la organización puede ser atacado accidentalmente o deliberadamente; lo constituyen los datos, información, recursos tangibles e intangibles, equipos, aplicaciones, servicios entre otros. La relación de tipos de activos se encuentra en el Capítulo 2 del “Catalogo de Elementos” del Libro II de MARGERIT.
- **Amenazas. Causa** potencial de un incidente que puede ocasionar daños a un sistema de información o a una organización (UNE 71504:2008). Siendo el activo el que puede sufrir el daño o incidente, la relación de amenazas se

encuentra en el Capítulo 5 del “Catalogo de Elementos” del Libro II de MARGERIT.

- **Salvaguardas.** Son las medidas que se toman para reducir el riesgo pueden consistir en procedimientos o soluciones tecnológicas dependiendo del tipo de activo, la relación de salvaguardas se encuentra en el Capítulo 6 del “Catalogo de Elementos” del Libro II de MARGERIT.
- **Impacto.** Consecuencia de la materialización de una amenaza sobre un activo, conociendo el valor del activo y la degradación que conlleva la amenaza se obtiene el nivel de impacto que se obtendrá en el sistema.
- **Riesgo.** Según la norma ISO 27001 es el efecto de la incertidumbre, el riesgo viene hacer el grado de exposición a una amenaza de uno o más activos si estos no se llegaran a proteger adecuadamente.
- **Riesgo residual.** Es el resultado de implementar una salvaguarda donde se modifica un riesgo potencial en uno residual.

3.3. Definición de términos básicos

3.3.1. Confidencialidad:

Es aquella que abarca el resguardo de los datos transmitidos contra ataques pasivos o sea al acceso no autorizado que contendrá medidas tales como el control de acceso y encriptación. La pérdida de la confiabilidad es generada al momento que existe una transgresión de la confiabilidad de algún dato, como la contraseña de un usuario o administrador del sistema permitiendo de esta manera que esté expuesta la información restringida y la cual se encontraba disponible solamente a un específico grupo de usuarios (Organización Internacional de Normalización/Comisión Electrotécnica Internacional [ISO/IEC] 13335-1, 2004).

3.3.2. Autenticidad:

Es la que se encarga de garantizar que la comunicación sea genuina en otras palabras el origen y destino pueden comprobar la identidad de la otra parte involucrada en la comunicación con el objetivo de corroborar que la otra parte es quien dice ser; hay que tener en cuenta que el origen y el destino por lo general son usuarios, dispositivos o procesos (ISO/IEC 13335-1, 2004).

3.3.3. Integridad:

Es la garantía contra ataques activos mediante los cambios o remociones no autorizadas; es de gran importancia usar un esquema que ayude a verificar la integridad de la información almacenada y su transmisión. La integridad puede ser considerada como servicio sin y con recuperación; por otro lado, una vez que los ataques activos son considerados en su contexto, interesara más el descubrimiento que la prevención de esa manera, si es detectado un peligro para la integridad es posible reportarlo y el mecanismo de recuperación es activado de forma inmediata (ISO/IEC 13335-1, 2004).

La integridad es igualmente un requisito para otros servicios de seguridad, por ejemplo, si la integridad de un sistema de control de acceso a un sistema operativo es violada, igualmente se viola la confidencialidad de sus archivos. La pérdida de la integridad es generada cuando alguna información se encuentra expuesta a la manipulación por personal no autorizado, que realiza cambios no aprobados y no se encuentran bajo el control del propietario de la información (corporativo o privado).

3.3.4. Conformidad:

Es cumplir y hacer cumplir las regulaciones internas y externas asignadas a los trabajos de la organización. Estar en conformidad es estar de acuerdo, continuando y haciendo cumplir las leyes y reglamentos internos y externos (Normaiso27001, 2024).

3.3.5. Disponibilidad:

Establece que los recursos se encuentren disponibles para el acceso de entidades autorizadas mientras así lo soliciten, lo que representa protección contra la pérdida o degradación; la pérdida de disponibilidad ocurre cuando la información ya no es accesible para quienes la necesitan vendría a ser el caso de pérdida de comunicación con un sistema significativo para la organización que sucedió al momento de caerse un servidor o una aplicación crítica para el negocio que exteriorizó una falla por un error ocasionado por causas internas o externas al equipo o por la acción de individuos no autorizados, con o sin mala intención (ISO/IEC 13335-1, 2004).

3.3.6. Control:

Son los medios de gestión de riesgos contenidos en políticas, operaciones, pautas, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o naturaleza jurídica (ISO/IEC 27002, 2005).

3.3.7. Información:

Se encuentra compuesta por una serie de datos ya inspeccionados y estructurados, que permiten crear un mensaje asentado en algún fenómeno o ente (Porto & Gardey, 2008).

3.3.8. Vulnerabilidad:

Debilidad de un activo o control que puede ser aprovechado por un peligro. A largo plazo la seguridad de la información ha adquirido un significado más prominente atrayendo consigo una serie de expertos en asuntos vinculados con seguridad, peligros y similares; que fomentan diferentes enfoques, normas, buenas prácticas y varios modelos para planificar un SGSI (ISO/IEC 27000, 2014).

3.3.9. Seguridad:

Una idea relacionada con la seguridad es la ausencia de peligro o contingencia; se puede comprender como seguridad una condición de cualquier sistema o tipo de información (informático o no) que muestre que este sistema o información se encuentra libre de riesgo, daño o peligro. El riesgo o daño se percibe como cualquier cosa que consigue afectar su funcionamiento directo o los resultados conseguidos (Vega Briceño, 2021).

3.3.10. Seguridad de la información:

Resguardo de la información y de los accesos a los sistemas de información, control de su empleo, divulgación, cambio, alteración, lectura, registro o destrucción (ISO/IEC 27000, 2016).

CAPITULO IV

DESARROLLO DE LA EXPERIENCIA

4.1. Intervención

4.1.1. Marco normativo

- Norma NTP-ISO/IEC 27001:2014
- Resolución Ministerial N°004-2016-PCM que aprueba el uso obligatorio de la Norma NTP-ISO/IEC 27001:2014.
- Resolución Ministerial N°166-2017-PCM que dispone que el titular de la entidad deba designar un Oficial de Seguridad de la Información; responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la entidad.
- Resolución Jefatural N°429-2017-INEI que aprueba la conformación del Comité de Gestión de Seguridad de la Información del INEI y la designación del Oficial de Seguridad de la Información.
- Resolución Jefatural N°200-2020-INEI que aprueba la conformación del Comité de Gobierno Digital del INEI.
- Resolución Jefatural N°335-2023-INEI que aprueba el Mapa de Procesos del Instituto Nacional de Estadística e Informática - INEI

- Resolución Jefatural N°133-2023-INEI que aprueba la Política General de Seguridad de la Información del Instituto Nacional de Estadística e Informática – INEI.

4.1.2. Política general del INEI

Teniendo en consideración que actualmente la implementación del SGSI se realiza en el Proceso: Administración del Centro de Datos de la Sede Central del INEI.

Se desarrollo el documento dirigido a establecer un marco general de gestión que tiene como objetivo la protección de la información del INEI con directrices generales para un tratamiento adecuado de riesgos y su protección de posibles pérdidas o modificación no autorizada, adoptando para ello la norma NTP-ISO/IEC 27001:2014; Norma Técnica Peruana vigente la cual es una adopción de la norma ISO/IEC 27001:2013.

Este documento incluye objetivos de seguridad de la información, los compromisos con los requisitos relacionados a la seguridad de la información y los compromisos de mejora continua del sistema de gestión de la seguridad de la información de la institución.

Al igual que los roles y responsabilidades de los entes involucrados para el aseguramiento del sistema de gestión de seguridad de la información y el reporte de su desempeño según cargos y funciones.

Se rige bajo los siguientes principios:

- **Acceso autorizado.** todos los usuarios deben ser identificados, autenticados y su nivel de permiso deben ser concedidos de acuerdo al nivel de responsabilidad.
- **Auditabilidad.** los sistemas informáticos deben de registrar cada evento para su control y auditoria **relacionada** dicho evento.

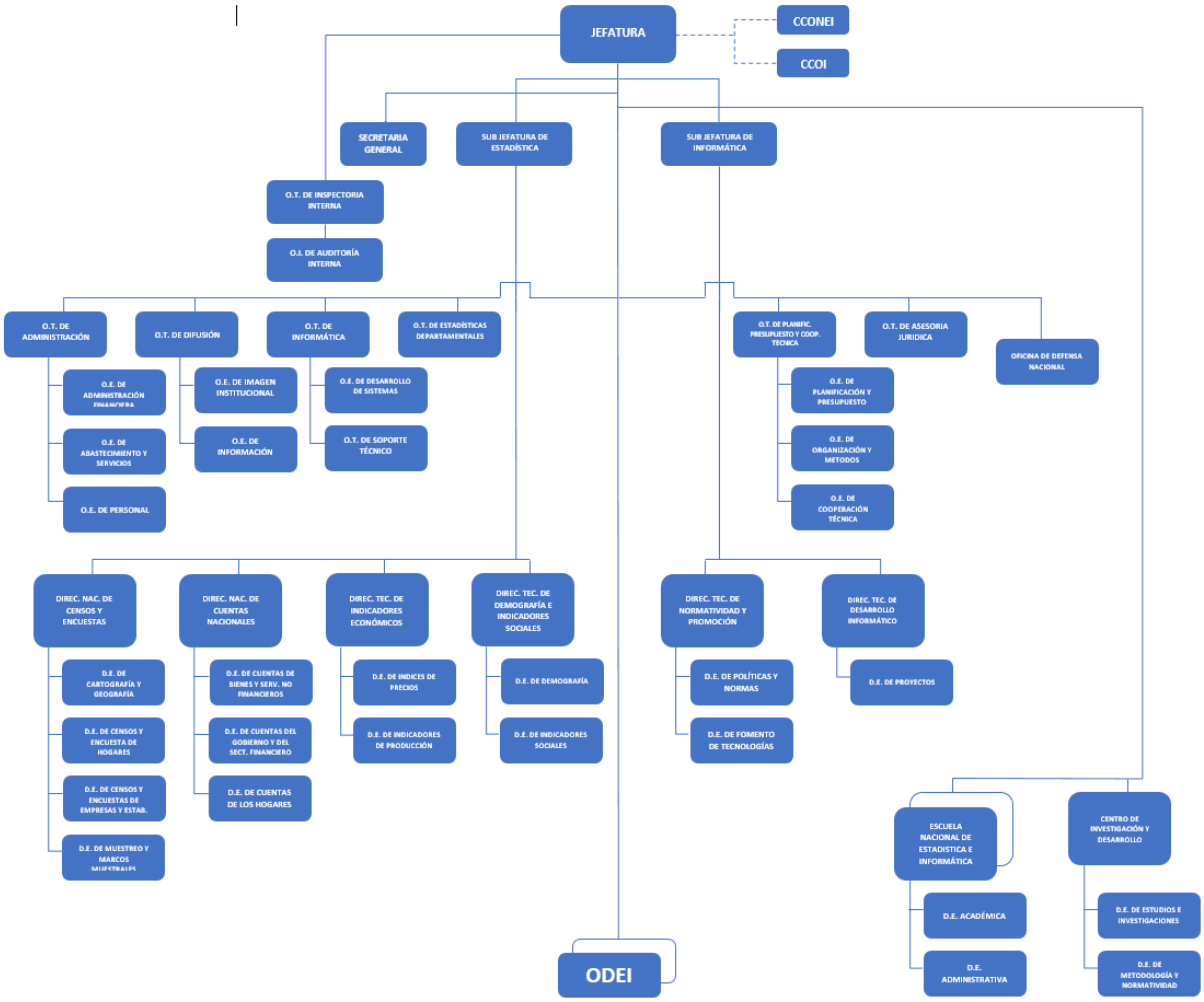
- **Colaboración.** la seguridad de la información viene hacer un trabajo colaborativo de los **trabajadores** de la institución y de terceros que hacen uso de los activos de la información.
- **Confidencialidad.** los activos de la información se deben mantener protegidos para asegurar **la** privacidad y confidencialidad.
- **Disponibilidad.** los activos de información deben estar disponibles solo para usuarios **autorizados**.
- **Integridad.** los activos de información deben estar protegidos para preservar su integridad detectando su modificación, adulteración o eliminación.
- **Propiedad.** la información ingresada, registrada, almacenada y procesada es propiedad exclusiva de la institución.
- **Protección.** los activos de información deben ser protegidos aplicando un sistema de gestión de seguridad de la información.
- **Supervisión.** los sistemas informáticos tangibles e intangibles deben ser verificados periódicamente para establecer el cumplimiento de las políticas de seguridad.
- **Uso apropiado**. los activos de información deben ser utilizados en forma adecuada, eficiente para el desarrollo de las actividades propias de la institución.

4.1.3. Organización estructural del INEI

Según la Decreto Supremo N°043-2001-PCM que aprueba el reglamento de organización y funciones, define el organigrama estructural del INEI.

Figura 4

Organigrama Estructural INEI

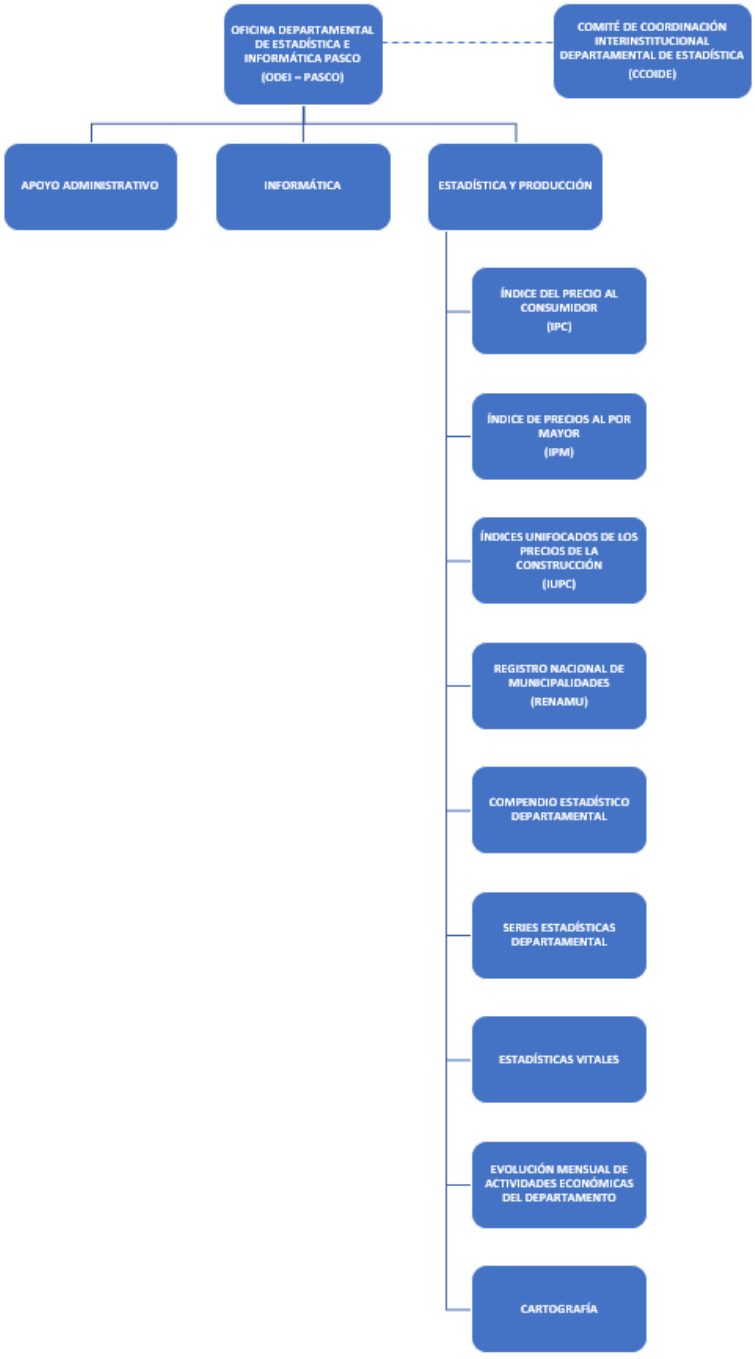


Nota: La figura muestra el organigrama estructural del Instituto Nacional de Estadística e Informática. Fuente: D.S. N°043-2001-PCM

4.1.4. Organigrama Funcional de ODEI Pasco

Figura 5:

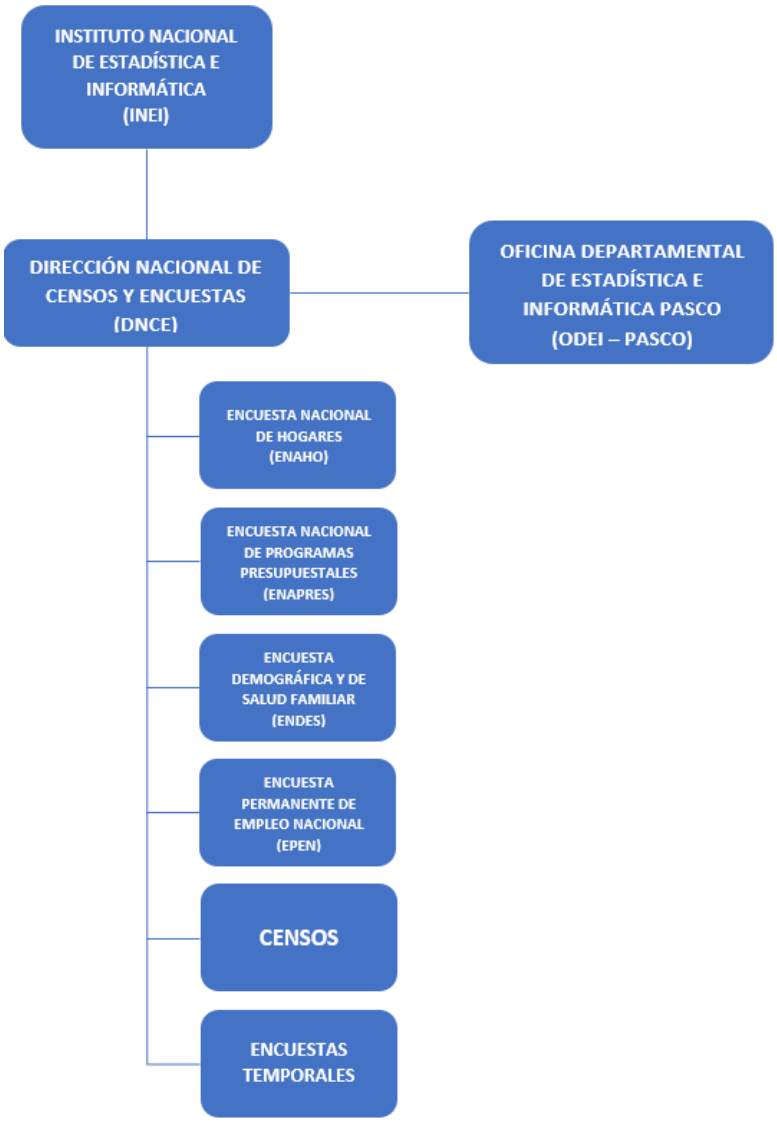
Organigrama Funcional ODEI Pasco



Nota: La figura muestra el organigrama funcional de la Oficina Departamental de Estadística e Informática Pasco

Figura 6

Organigrama Funcional ODEI Pasco



Nota: La figura muestra el organigrama funcional de la Oficina Departamental de Estadística e Informática Pasco

4.1.5. Identificación de activos de información de la ODEI Pasco

Teniendo en cuenta que el identificar un activo de información viene a constituir un paso crucial para dar inicio a la construcción de un SGSI, ya que el activo de información es el recurso que utiliza el SGSI para realizar el proceso y conseguir así los objetivos de la entidad. Según el Ítem A.8 Gestión de Activos

del Anexo A, de la Norma NTP-ISO/IEC 27001:2014 para su implementación en la entidad se debe dar cumplimiento a los siguientes puntos:

- Que la entidad cuente con un inventario de activos.
- Se debe definir la propiedad de activos y su propietario.
- Se debe realizar la clasificación de información en relación a sus características y el uso que se les da en la entidad.
- Se debe realizar un etiquetado para su manipulación de la información.

Siendo los activos de información de la ODEI Pasco los siguientes:

Tabla 1

Inventario de Activos – ODEI Pasco

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
100-1	INFORMACIÓN	NORMAS INTERNAS	Custodiar bajo los lineamientos de las normas internas los activos de información bajo responsabilidad	Director Departamental
100-2	INFORMACIÓN	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ASIGNADOS	Supervisar los controles de seguridad asignados a la ODEI	Director Departamental
100-3	INFORMACIÓN	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	Difundir la Política General de Seguridad de la Información al personal a cargo	Director Departamental
100-4	INFORMACIÓN	ACTA	Actas desarrolladas en las reuniones desarrolladas por el CCOIDE	Director Departamental
100-5	INFORMACIÓN	SESIONES ORDINARIAS	Reuniones programadas vía plataforma Zoom	Director Departamental
100-6	INFORMACIÓN	INFORMES DE GESTIÓN DE CCOIDE	Informes realizados por la presidente y secretaria técnica de la CCOIDE	Director Departamental

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
100-7	INFORMACIÓN	COORDINACIONES CON LAS OFICINAS ESTADÍSTICAS	Reuniones de coordinación con los responsables de las oficinas estadísticas de las direcciones regionales miembros de la CCOIDE con la finalidad de continuar con la producción estadísticas en tiempos establecidos	Director Departamental
100-8	INFORMACIÓN	INFORMES DE CCOIDE A CEPLAN	Informes programados sobre los avances concernientes a la producción estadística de los diferentes sectores regionales	Director Departamental
100-9	INFORMACIÓN	INFORMES DE GESTIÓN	Informe programado realizado a Sede Central	Director Departamental
100-10	INFORMACIÓN	INFORMES DE RESPUESTA	Informe a solicitud de los diferentes sectores, organismos públicos o privados	Director Departamental
100-11	INFORMACIÓN	CONCEPTOS INTERNOS	Conceptos internos dados por las distintas áreas de Sede Central	Director Departamental
100-12	INFORMACIÓN	INFORMES DE ENAHO A CEPLAN	Solicitud de Informes programados sobre los avances de la encuesta	Coordinador Departamental 2
100-13	INFORMACIÓN	INFORMES DE GESTIÓN DE ENAHO	Solicitud de Informe realizado por la coordinadora departamental del proyecto	Coordinador Departamental 2
100-14	ELEMENTOS AUXILIARES	LÓGISTICA ENAHO	Apoyo logístico para la recopilación de información	Coordinador Departamental 2
100-15	INFORMACIÓN	COORDINACIONES ENAHO	Coordinaciones con autoridades para la realización de la encuesta	Coordinador Departamental 2

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
100-16	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN ENAHO	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Coordinador Departamental 2
100-17	COMUNICACIONES	ENVIO DE INFORMACIÓN ENAHO	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Coordinador Departamental 2
100-18	INFORMACIÓN	SEGUIMIENTO Y SUPERVISIÓN ENAHO	Seguimiento y supervisión al cumplimiento con respecto a la consistencia de la información	Coordinador Departamental 2
100-19	INFORMACIÓN	INFORMES DE ENAPRES A CEPLAN	Solicitud de Informes programados sobre los avances de la encuesta	Coordinador Departamental 1
100-20	INFORMACIÓN	INFORMES DE GESTIÓN DE ENAPRES	Solicitud de Informe realizado por la coordinadora departamental del proyecto	Coordinador Departamental 1
100-21	ELEMENTOS AUXILIARES	LÓGISTICA ENAPRES	Apoyo logístico para la recopilación de información	Coordinador Departamental 1
100-22	INFORMACIÓN	COORDINACIONES ENAPRES	Coordinaciones con autoridades para la realización de la encuesta	Coordinador Departamental 1
100-23	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Coordinador Departamental 1
100-24	COMUNICACIONES	ENVIO DE INFORMACIÓN ENAPRES	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Coordinador Departamental 1

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
100-25	INFORMACIÓN	SEGUIMIENTO Y SUPERVISIÓN ENAPRES	Seguimiento y supervisión al cumplimiento con respecto a la consistencia de la información	Coordinador Departamental 1
100-26	INFORMACIÓN	INFORMES DE ENDES A CEPLAN	Solicitud de Informes programados sobre los avances de la encuesta	Supervisor Local
100-27	INFORMACIÓN	INFORMES DE GESTIÓN DE ENDES	Solicitud de Informe realizado por la coordinadora departamental del proyecto	Supervisor Local
100-28	ELEMENTOS AUXILIARES	LÓGISTICA ENDES 1	Apoyo logístico para la recopilación de información	Supervisor Local
100-29	INFORMACIÓN	COORDINACIONES ENDES	Coordinaciones con autoridades para la realización de la encuesta	Supervisor Local
100-30	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Supervisor Local
100-31	COMUNICACIONES	ENVIO DE INFORMACIÓN ENDES 1	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Supervisor Local
100-32	INFORMACIÓN	SEGUIMIENTO Y SUPERVISIÓN ENDES 1	Seguimiento y supervisión al cumplimiento con respecto a la consistencia de la información	Supervisor Local
100-33	ELEMENTOS AUXILIARES	LÓGISTICA ENDES 2	Apoyo logístico para la recopilación de información	Actualizador Cartográfico
100-34	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Recopilación de información de acuerdo a los conglomerados	Coordinador Departamental 3

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
			designados en su programación de trabajo	
100-35	COMUNICACIONES	ENVIO DE INFORMACIÓN ENDES 2	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Coordinador Departamental 3
100-36	INFORMACIÓN	INFORMES DE EPEN A CEPLAN	Solicitud de Informes programados sobre los avances de la encuesta	Coordinador Departamental 3
100-37	INFORMACIÓN	INFORMES DE GESTIÓN DE EPEN	Solicitud de Informe realizado por la coordinadora departamental del proyecto	Coordinador Departamental 3
100-38	ELEMENTOS AUXILIARES	LÓGISTICA EPEN 1	Apoyo logístico para la recopilación de información	Coordinador Departamental 3
100-39	INFORMACIÓN	COORDINACIONES EPEN	Coordinaciones con autoridades para la realización de la encuesta	Coordinador Departamental 3
100-40	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Coordinador Departamental 3
100-41	COMUNICACIONES	ENVIO DE INFORMACIÓN EPEN 1	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Coordinador Departamental 3
100-42	INFORMACIÓN	SEGUIMIENTO Y SUPERVISIÓN EPEN 1	Seguimiento y supervisión al cumplimiento con respecto a la consistencia de la información	Coordinador Departamental 3
100-43	ELEMENTOS AUXILIARES	LÓGISTICA EPEN 2	Apoyo logístico para la recopilación de información	Coordinador Departamental 3

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
100-44	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Coordinador Departamental 4
100-45	COMUNICACIONES	ENVIO DE INFORMACIÓN EPEN 2	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Coordinador Departamental 4
100-46	INFORMACIÓN	INFORMES DE CENSOS 1 A CEPLAN	Solicitud de Informes programados sobre avances de operación de campo	Coordinador Departamental 4
100-47	INFORMACIÓN	INFORMES DE GESTIÓN DE CENSOS 1	Solicitud de Informe realizado por la coordinadora departamental del proyecto	Coordinador Departamental 4
100-48	ELEMENTOS AUXILIARES	LÓGISTICA CENSO 1	Apoyo logístico para la recopilación de información	Coordinador Departamental 4
100-49	INFORMACIÓN	COORDINACIONES CENSOS 1	Coordinaciones con autoridades para la realización de la encuesta	Coordinador Departamental 4
100-50	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Coordinador Departamental 4
100-51	COMUNICACIONES	ENVIO DE INFORMACIÓN CENSO 1	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Coordinador Departamental 4
100-52	INFORMACIÓN	SEGUIMIENTO Y SUPERVISIÓN CENSOS 1	Seguimiento y supervisión al cumplimiento con respecto a la consistencia de la información	Coordinador Departamental 4

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
100-53	INFORMACIÓN	INFORMES DE CENSOS 2 A CEPLAN	Solicitud de Informes programados sobre avances de operación de campo	Coordinador Departamental 4
100-54	INFORMACIÓN	INFORMES DE GESTIÓN DE CENSOS 2	Solicitud de Informe realizado por la coordinadora departamental del proyecto	Coordinador Departamental 4
100-55	ELEMENTOS AUXILIARES	LÓGISTICA CENSO 2	Apoyo logístico para la recopilación de información	Coordinador Departamental 4
100-56	INFORMACIÓN	COORDINACIONES CENSOS 2	Coordinaciones con autoridades para la realización de la encuesta	Coordinador Departamental 4
100-57	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Coordinador Departamental 4
100-58	COMUNICACIONES	ENVIO DE INFORMACIÓN CENSO 2	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Coordinador Departamental 4
100-59	INFORMACIÓN	SEGUIMIENTO Y SUPERVISIÓN CENSOS 2	Seguimiento y supervisión al cumplimiento con respecto a la consistencia de la información	Coordinador Departamental 4
100-60	INFORMACIÓN	INFORMES DE CENSOS A CEPLAN	Solicitud de Informes programados sobre avances de operación de campo	Coordinador Departamental 4
100-61	INFORMACIÓN	INFORMES DE GESTIÓN DE CENSO	Solicitud de Informe realizado por la coordinadora departamental del proyecto	Coordinador Departamental 4
100-62	ELEMENTOS AUXILIARES	LÓGISTICA CENSO	Apoyo logístico para la recopilación de información	Coordinador Departamental 4

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
100-63	INFORMACIÓN	COORDINACIONES CENSOS	Coordinaciones con autoridades para la realización de la encuesta	Coordinador Departamental 4
100-64	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN CENSOS	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Coordinador Departamental 4
100-65	COMUNICACIONES	ENVIO DE INFORMACIÓN CENSO	Seguimiento y supervisión al cumplimiento con respecto al envío de información	Coordinador Departamental 4
100-66	INFORMACIÓN	SEGUIMIENTO Y SUPERVISIÓN CENSOS	Seguimiento y supervisión al cumplimiento con respecto a la consistencia de la información	Coordinador Departamental 4
100-67	INFORMACIÓN	INFORMES DE ENCUESTAS TEMPORALES A CEPLAN	Solicitud de Informes programados sobre avances de operación de campo	Coordinador Departamental 5
100-68	INFORMACIÓN	INFORMES DE GESTIÓN DE ENCUESTAS TEMPORALES	Solicitud de Informe realizado por la coordinadora departamental del proyecto	Coordinador Departamental 5
100-69	ELEMENTOS AUXILIARES	LÓGISTICA ENCUESTAS TEMPORALES	Apoyo logístico para la recopilación de información	Coordinador Departamental 5
100-70	INFORMACIÓN	COORDINACIONES ENCUESTAS TEMPORALES	Coordinaciones con autoridades para la realización de la encuesta	Coordinador Departamental 5
100-71	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Recopilación de información de acuerdo a los conglomerados designados en su programación de trabajo	Coordinador Departamental 5
100-72	COMUNICACIONES	ENVIO DE INFORMACIÓN	Seguimiento y supervisión al cumplimiento con	Coordinador Departamental 5

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
		ENCUESTAS TEMPORALES	respecto al envío de información	
100-73	INFORMACIÓN	SEGUIMIENTO Y SUPERVISIÓN ENCUESTAS TEMPORALES	Seguimiento y supervisión al cumplimiento con respecto a la consistencia de la información	Coordinador Departamental 5
100-74	RECURSOS HUMANOS	TÉRMINOS DE CONTRATACIÓN	Incluir en la contratación de terceros lo referente a la seguridad de la información	Director Departamental
100-75	INSTALACIONES	DESPACHO DE JEFATURA	Oficina donde se encuentra el Director de ODEI Pasco	N/A
100-76	RECURSOS HUMANOS	DIRECTOR	Lidera la ODEI Pasco	N/A
200-77	INFORMACIÓN	RENDICIONES PROYECTOS PREMANENTES	Rendición de cuentas de fondos otorgados por encargo	Apoyo Administrativo
200-78	INFORMACIÓN	RENDICIONES PROYECTOS TEMPORALES	Rendición de cuentas de fondos otorgados por encargo	Apoyo Administrativo
200-79	INFORMACIÓN	RENDICIONES ODEI	Rendición de cuentas de fondos otorgados a ODEI	Apoyo Administrativo
200-80	INFORMACIÓN	REGISTRO DE COMPRAS Y VENTAS	Registro mensual de compras y ventas en ODEI	Apoyo Administrativo
200-81	INFORMACIÓN	INFORMES	Apoyo administrativo para la realización de informes de ODEI	Apoyo Administrativo
200-82	COMUNICACIONES	INFORMES SEDE CENTRAL	Envío de informes realizados en la ODEI a Sede Central	Apoyo Administrativo
200-83	INFORMACIÓN	CORREOS	Apoyo administrativo para la redacción de correos institucionales y su envío a Sede Central	Apoyo Administrativo
200-84	SOFTWARE	CORREO INSTITUCIONAL	Uso del correo institucional	Apoyo Administrativo
200-85	SOFTWARE	MENSAJERÍA	Uso del Sistema de Documentación y Mensajería SGD	Apoyo Administrativo

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
300-86	INFORMACIÓN	INFORME PLAN OPERATIVO	Informe de seguimiento y evaluación del Plan Operativo en ODEI	Analista Estadístico Departamental 1
300-87	INFORMACIÓN	GESTIÓN DE ACTIVOS TIC	Documento donde se específica los datos del equipo, fechas de mantenimiento y responsable	Analista Estadístico Departamental 1
300-88	INFORMACIÓN	DIRECTIVAS	Documento de gestión de cumplimiento como ente ejecutor	Analista Estadístico Departamental 1
300-89	INFORMACIÓN	POLÍTICAS	Documento de gestión de cumplimiento como ente ejecutor	Analista Estadístico Departamental 1
300-90	INFORMACIÓN	SEGUIMIENTO SISTEMAS DE INFORMACIÓN	Seguimiento de la gestión de los sistemas de información desarrollados en Sede Central	Analista Estadístico Departamental 1
300-91	INFORMACIÓN	MANUAL DE USUARIO	Seguimiento del cumplimiento de los manuales de usuario	Analista Estadístico Departamental 1
300-92	INFORMACIÓN	MANUAL TÉCNICO	Seguimiento del cumplimiento de los manuales técnicos elaborados por OTIN	Analista Estadístico Departamental 1
300-93	SOFTWARE	UNETE	Sistema para las convocatorias de personal por Locación de Servicios de acuerdo con las necesidades y a solicitud de los proyectos de la institución y sus procesos de evaluación	Analista Estadístico Departamental 1
300-94	SOFTWARE	RENAMU	Sistema para el monitoreo, la recepción, procesamiento y consistencia del Registro Nacional de Municipalidades con	Analista Estadístico Departamental 1

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
			la finalidad de integrar información estadística de las Municipalidades Provinciales, Distritales y de Centros Poblados	
300-95	SOFTWARE	SGD	Sistema de documentación y mensajería	Analista Estadístico Departamental 1
300-96	SOFTWARE	SIIP	Sistema integrado de indicadores de precios	Analista Estadístico Departamental 1
300-97	SOFTWARE	FTP	Extranet institucional para intercambio de archivos	Analista Estadístico Departamental 1
300-98	SOFTWARE	INTRANET	Intranet institucional para comunicación interna	Analista Estadístico Departamental 1
300-99	SOFTWARE	OWA	Aplicación utilizada en el manejo del correo institucional	Analista Estadístico Departamental 1
300-100	SOFTWARE	SISTEMA LÓGISTICO	Aplicación institucional utilizado para control de bienes y materiales recepcionados por la ODEI	Analista Estadístico Departamental 1
300-101	SERVICIOS	PETICIÓN	Solicitud de atención de peticiones de servicios TIC a la OTIN	Analista Estadístico Departamental 1
300-102	SERVICIOS	SEGUIMIENTO PETICIONES	Solución de incidencia de petición de servicios TIC	Analista Estadístico Departamental 1
300-103	ELEMENTOS AUXILIARES	RESPALDO DE INFORMACIÓN	Necesidad de realizar respaldos de información por equipo asignado	Analista Estadístico Departamental 1
300-104	INFORMACIÓN	INFORME DE INCIDENCIAS	Informe de incidencias con respecto a la	Analista Estadístico Departamental 1

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
			seguridad de la información en ODEI	
300-105	INFORMACIÓN	MANTENIMIENTO DE EQUIPOS	Mantenimiento de equipos según cronograma especificado por OTIN	Analista Estadístico Departamental 1
300-106	INFORMACIÓN	MONITOREO DE SISTEMAS Y APLICACIONES	Monitoreo de los sistemas, aplicaciones, portal web institucional	Analista Estadístico Departamental 1
300-107	INFORMACIÓN	REPORTE	Reporte programado de funcionamiento de servidor y redes	Analista Estadístico Departamental 1
300-108	INFORMACIÓN	MONITOREO CONEXIONES	Monitoreo programado de calidad de conexión internet	Analista Estadístico Departamental 1
300-109	INFORMACIÓN	INFORME DE SERVICIOS	Informe programado de servicios ofrecidos por la ODEI a Sede Central	Analista Estadístico Departamental 1
300-110	HARDWARE	ACTIVOS INFORMÁTICOS	Inventario de equipos asignados a ODEI	Analista Estadístico Departamental 1
400-111	INFORMACIÓN	INFORMES DE IPC A CEPLAN	Informe programado sobre las actividades realizadas	Analista Estadístico Departamental 2
400-112	INFORMACIÓN	FORMATO A1	Formato usado para la recolección de datos referentes a mercados de acuerdo al directorio de informantes	Analista Estadístico Departamental 2
400-113	INFORMACIÓN	FORMATO A26	Formato usado para la recolección de datos referentes a establecimientos de acuerdo al directorio de informantes	Analista Estadístico Departamental 2
400-114	INFORMACIÓN	FORMATO A32	Formato usado para la recolección de datos referentes a alquiler de viviendas de acuerdo al	Analista Estadístico Departamental 2

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
			directorio de informantes	
400-115	INFORMACIÓN	INGRESO DE DATOS IPC A SIIP	Ingreso de datos recolectados al SIIP	Analista Estadístico Departamental 2
400-116	INFORMACIÓN	ANÁLISIS DE INFORMACIÓN DE IPC	Revisión y análisis de la información ingresada en el SIIP	Analista Estadístico Departamental 2
400-117	INFORMACIÓN	CONSISTENCIA DE INFORMACIÓN DE IPC	Proceso de consistencia de la información ingresada en el SIIP	Analista Estadístico Departamental 2
400-118	INFORMACIÓN	CUADRO FINAL DEL IPC DEPARTAMENTAL	Cuadro final obtenido del cálculo del IPC departamental	Analista Estadístico Departamental 2
400-119	INFORMACIÓN	INFORME DE IPC A DTIE	Envió de informe con el resultado del IPC departamental a la oficina técnica para su aprobación	Analista Estadístico Departamental 2
400-120	INFORMACIÓN	INFORME DE IUPC A CEPLAN	Informe programado sobre las actividades realizadas	Analista Estadístico Departamental 2
400-121	INFORMACIÓN	FORMATO IUPC	Formato usado para la recolección de datos de acuerdo al directorio de informantes	Analista Estadístico Departamental 2
400-122	INFORMACIÓN	INGRESO DE DATOS IUPC A SIIP	Ingreso de datos recolectados al SIIP	Analista Estadístico Departamental 2
400-123	INFORMACIÓN	ANÁLISIS DE INFORMACIÓN DE IUPC	Revisión y análisis de la información ingresada en el SIIP	Analista Estadístico Departamental 2
400-124	INFORMACIÓN	CONSISTENCIA DE INFORMACIÓN DE IUPC	Proceso de consistencia de la información ingresada en el SIIP	Analista Estadístico Departamental 2
400-125	INFORMACIÓN	CUADRO FINAL DEL IUPC DEPARTAMENTAL	Cuadro final obtenido del cálculo del IUPC departamental	Analista Estadístico Departamental 2

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
400-126	INFORMACIÓN	INFORME DE IUPC A DTIE	Envió del informe con el resultado del IUPC departamental a la oficina técnica para su aprobación y consolidación	Analista Estadístico Departamental 2
400-127	INFORMACIÓN	INFORME DE IPM A CEPLAN	Informe programado sobre las actividades realizadas	Analista Estadístico Departamental 2
400-128	INFORMACIÓN	FORMATO IPM	Formato usado para la recolección de datos de acuerdo al directorio de informantes	Analista Estadístico Departamental 2
400-129	INFORMACIÓN	INGRESO DE DATOS IPM A SIIP	Ingreso de datos recolectados al SIIP	Analista Estadístico Departamental 2
400-130	INFORMACIÓN	ANÁLISIS DE INFORMACIÓN DE IPM	Revisión y análisis de la información ingresada en el SIIP	Analista Estadístico Departamental 2
400-131	INFORMACIÓN	CONSISTENCIA DE INFORMACIÓN DE IPM	Proceso de consistencia de la información ingresada en el SIIP	Analista Estadístico Departamental 2
400-132	INFORMACIÓN	INFORME DE IPM DTIE	Envió del informe con el resultado del IPM departamental a la oficina técnica para su aprobación y consolidación	Analista Estadístico Departamental 2
400-133	INFORMACIÓN	INFORME EVOLUCIÓN MENSUAL A CEPLAN	Informe programado sobre las actividades realizadas	Analista Estadístico Departamental 3
400-134	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Recopilación de información de los diferentes sectores gubernamentales	Analista Estadístico Departamental 3
400-135	INFORMACIÓN	AVANCE ECONÓMICO Y SOCIAL REGIONAL MENSUAL	Elaboración de la nota mensual sobre Avance Económico y Social Regional Mensual	Analista Estadístico Departamental 3
400-136	INFORMACIÓN	DOCUMENTO ECONÓMICO Y	Elaboración del Avance Económico y	Analista Estadístico

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
		SOCIAL REGIONAL MENSUAL	Social Regional Mensual	Departamental 3
400-137	INFORMACIÓN	INFORME A OTED	Envío de informe a OTED para su verificación, inclusión y publicación en el portal del INEI, Perú: Panorama Económico Departamental	Analista Estadístico Departamental 3
500-138	INFORMACIÓN	INFORME DE COMPENDIO A CEPLAN	Informe programado sobre las actividades realizadas	Analista Estadístico Departamental 3
500-139	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Recopilación de información de los diferentes sectores gubernamentales	Analista Estadístico Departamental 3
500-140	INFORMACIÓN	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Actualizar la información de acuerdo a la información proporcionada por los sectores	Analista Estadístico Departamental 3
500-141	INFORMACIÓN	EDICIÓN	Ordenar y clasificar por Capítulos la información remitida en Excel	Analista Estadístico Departamental 3
500-142	INFORMACIÓN	REVISIÓN COMPENDIO	Revisión de la información editada para su posterior publicación	Analista Estadístico Departamental 3
500-143	INFORMACIÓN	INFORME DE SERIES A CEPLAN	Informe programado sobre las actividades realizadas	Analista Estadístico Departamental 3
500-144	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN SERIES	Recopilación de información de los diferentes sectores gubernamentales	Analista Estadístico Departamental 3
500-145	INFORMACIÓN	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Actualizar la información de acuerdo a la información proporcionada por los sectores	Analista Estadístico Departamental 3

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
500-146	INFORMACIÓN	REVISIÓN SERIES	Revisión de la información para su posterior publicación	Analista Estadístico Departamental 3
500-147	INFORMACIÓN	INFORME DE ESTADÍSTICAS VITALES A CEPLAN	Informe programado sobre las actividades realizadas	Analista Estadístico Departamental 1
500-148	INFORMACIÓN	INFORME MENSUAL ESTADÍSTICAS VITALES 1	Recepción de informes mensuales de las Municipalidades Provinciales y Distritales	Analista Estadístico Departamental 1
500-149	INFORMACIÓN	INFORME MENSUAL ESTADÍSTICAS VITALES 2	Recepción de informes mensuales de las Municipalidades Provinciales y Distritales	Analista Estadístico Departamental 1
500-150	INFORMACIÓN	FORMATO 2 - MATRIMONIOS Y DIVORCIOS	Recopilación de información de las municipalidades provinciales y distritales	Analista Estadístico Departamental 1
500-151	INFORMACIÓN	FORMATO 2 - NACIMIENTOS Y DEFUNCIONES	Recopilación de información de las municipalidades provinciales y distritales	Analista Estadístico Departamental 1
500-152	INFORMACIÓN	INFORME DE RENAMU A CEPLAN	Informe programado sobre las actividades realizadas	Analista Estadístico Departamental 1
500-153	COMUNICACIONES	OFICIO 1	Oficio dirigido a las Municipalidades Provinciales y Distritales	Analista Estadístico Departamental 1
500-154	COMUNICACIONES	OFICIO 2	Oficio dirigido a las Municipalidades de Centros Poblados	Analista Estadístico Departamental 1
500-155	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Auto diligenciamiento, donde el alcalde designa a un responsable para el diligenciamiento del formulario, quien	Analista Estadístico Departamental 1

Identificador	Tipo	Nombre	Descripción	Nombre del responsable de la Información (Custodio del Activo)
			recopilará la información de las diferentes áreas u oficinas de la municipalidad	
500-156	INFORMACIÓN	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Auto diligenciamiento, donde el alcalde designa a un responsable para el diligenciamiento del formulario, quien recopilará la información de las diferentes áreas u oficinas de la municipalidad	Analista Estadístico Departamental 1
500-157	INFORMACIÓN	TABULACIÓN DE INFORMACIÓN	Se realiza una tabla con los resultados obtenidos tras la recopilación de datos	
500-158	INFORMACIÓN	CONSISTENCIA DE INFORMACIÓN DE RENAMU	Proceso de consistencia de la información ingresada en el RENAMU	Analista Estadístico Departamental 1
500-159	INFORMACIÓN	INFORMES DE CARTOGRAFÍA A CEPLAN	Informe programado sobre las actividades realizadas	Especialista Cartográfico
500-160	INFORMACIÓN	OFICIO	Oficio dirigido a las Municipalidades Provinciales y Distritales	Especialista Cartográfico
500-161	INFORMACIÓN	CONSISTENCIA DE INFORMACIÓN CARTOGRÁFICA	Proceso de consistencia de la información ingresada	Especialista Cartográfico
500-162	INFORMACIÓN	INFORME A DECG	Envío de informe a DECG para su verificación	Especialista Cartográfico
600-163	RECURSOS HUMANOS	COLABORADORES CAS	Personas con contrato administrativo de servicios	N/A
600-164	RECURSOS HUMANOS	COLABORADORES CON LOCACIÓN DE SERVICIOS	Personas con contrato por locación de servicios	N/A

Luego de identificar los activos de información y realizar su respectivo inventario, estos se tienen que valorar para determinar su nivel de importancia en las tres dimensiones básicas: disponibilidad, integridad y confidencialidad.

De acuerdo a las dimensiones establecidas se realiza una valoración para cada una de ellas:

- **De acuerdo a la Dimensión de la Confidencialidad.** Se establecieron 3 niveles:
- **Información *Pública Reservada (3).*** información disponible para un proceso y de ser conocida por terceros puede tener efectos negativos en la entidad.
- ***Información Pública Clasificada (2).*** información disponible para varios procesos y de ser **conocida** por terceros puede tener efectos negativos en la entidad.
- **Información *Pública (1).*** información disponible a terceros sin restricciones.
- ***No clasificada (3).*** activos de información que deben ser incluidos en el inventario, pero aun sin **clasificación** se tratará como Información Pública Reservada.
- **De *acuerdo* a la Dimensión de la Disponibilidad.** Se establecieron 3 niveles:
- ***Alta (3).*** la no disponibilidad de la información conlleva a resultados negativos severos **que** perjudican a la entidad.
- ***Media (2).*** la no disponibilidad de la información conlleva a resultados negativos moderados que perjudican a la entidad.
- ***Baja (1).*** la no disponibilidad de la información puede afectar a la entidad, pero no conlleva a resultados negativos que perjudican a la entidad.

- ***No clasificada (3).*** activos de información que deben ser incluidos en el inventario, pero aun sin clasificación se tratará como Alta.
- **De *acuerdo* a la Dimensión de la Integridad.** Se establecieron 3 niveles:
- ***Alta (3).*** la pérdida de exactitud y completitud de la información conlleva a resultados negativos severos que perjudican a la entidad.
- ***Media (2).*** la pérdida de exactitud y completitud de la información conlleva a resultados negativos moderados que perjudican a la entidad.
- ***Baja (1).*** la pérdida de exactitud y completitud de la información puede afectar a la entidad, pero no conlleva a resultados negativos que perjudican a la entidad.
- ***No clasificada (3).*** activos de información que deben ser incluidos en el inventario, pero aun sin clasificación se tratará como Alta.

Tabla 2

Valoración de Activos - ODEI Pasco

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
100-1	INFORMACIÓN PÚBLICA RESERVADA	ALTA	MEDIA	ALTA
100-2	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-3	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-4	INFORMACIÓN PÚBLICA	BAJA	BAJA	BAJA
100-5	INFORMACIÓN PÚBLICA	BAJA	MEDIA	MEDIO
100-6	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-7	NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA	ALTA
100-8	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
100-9	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
100-10	INFORMACIÓN PÚBLICA	MEDIA	BAJA	MEDIO
100-11	INFORMACIÓN PÚBLICA	BAJA	BAJA	BAJA
100-12	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
100-13	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-14	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-15	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-16	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-17	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-18	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-19	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
100-20	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-21	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-22	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-23	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-24	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-25	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-26	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
100-27	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-28	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-29	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
100-30	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-31	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-32	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-33	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-34	INFORMACIÓN PÚBLICA RESERVADA	ALTA	MEDIA	ALTA
100-35	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-36	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
100-37	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-38	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-39	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-40	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-41	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-42	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-43	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-44	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-45	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-46	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
100-47	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-48	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
100-49	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-50	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-51	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-52	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-53	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
100-54	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-55	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-56	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-57	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-58	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-59	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-60	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
100-61	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-62	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-63	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-64	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-65	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
100-66	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-67	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
100-68	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-69	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-70	NO CLASIFICADA	NO CLASIFICADA	BAJA	MEDIO
100-71	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-72	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-73	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
100-74	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
100-75	NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA	ALTA
100-76	NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA	ALTA
200-77	INFORMACIÓN PÚBLICA	BAJA	BAJA	BAJA
200-78	INFORMACIÓN PÚBLICA	BAJA	BAJA	BAJA
200-79	INFORMACIÓN PÚBLICA	BAJA	BAJA	BAJA
200-80	INFORMACIÓN PÚBLICA	BAJA	BAJA	BAJA
200-81	INFORMACIÓN PÚBLICA	BAJA	BAJA	BAJA
200-82	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
200-83	NO CLASIFICADA	MEDIA	MEDIA	MEDIO
200-84	NO CLASIFICADA	MEDIA	MEDIA	MEDIO
200-85	INFORMACIÓN PÚBLICA RESERVADA	BAJA	BAJA	MEDIO
300-86	NO CLASIFICADA	MEDIA	MEDIA	MEDIO
300-87	INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA	MEDIA	MEDIO
300-88	INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA	MEDIA	MEDIO
300-89	INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA	MEDIA	MEDIO

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
300-90	INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA	ALTA	MEDIO
300-91	INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA	ALTA	MEDIO
300-92	INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA	ALTA	MEDIO
300-93	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-94	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-95	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-96	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-97	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	MEDIA	MEDIO
300-98	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	MEDIA	MEDIO
300-99	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-100	INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA	MEDIA	MEDIO
300-101	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-102	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-103	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-104	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-105	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	MEDIA	MEDIO
300-106	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	MEDIA	MEDIO

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
300-107	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	MEDIA	MEDIO
300-108	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
300-109	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
300-110	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-111	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
400-112	INFORMACIÓN PÚBLICA RESERVADA	ALTA	MEDIA	ALTA
400-113	INFORMACIÓN PÚBLICA RESERVADA	ALTA	MEDIA	ALTA
400-114	INFORMACIÓN PÚBLICA RESERVADA	ALTA	MEDIA	ALTA
400-115	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-116	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-117	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-118	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
400-119	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
400-120	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
400-121	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-122	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-123	INFORMACIÓN PÚBLICA RESERVADA	ALTA	MEDIA	ALTA

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
400-124	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-125	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
400-126	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
400-127	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
400-128	INFORMACIÓN PÚBLICA RESERVADA	ALTA	MEDIA	ALTA
400-129	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-130	INFORMACIÓN PÚBLICA RESERVADA	ALTA	MEDIA	ALTA
400-131	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-132	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
400-133	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
400-134	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-135	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
400-136	INFORMACIÓN PÚBLICA	ALTA	ALTA	MEDIO
400-137	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
500-138	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
500-139	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-140	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
500-141	NO CLASIFICADA	NO CLASIFICADA	MEDIA	ALTA
500-142	NO CLASIFICADA	NO CLASIFICADA	MEDIA	ALTA
500-143	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
500-144	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-145	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-146	NO CLASIFICADA	MEDIA	ALTA	ALTA
500-147	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
500-148	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
500-149	INFORMACIÓN PÚBLICA	MEDIA	MEDIA	MEDIO
500-150	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-151	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-152	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
500-153	INFORMACIÓN PÚBLICA	MEDIA	BAJA	MEDIO
500-154	INFORMACIÓN PÚBLICA	MEDIA	BAJA	MEDIO
500-155	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-156	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-157	INFORMACIÓN PÚBLICA CLASIFICADA	ALTA	ALTA	ALTA
500-158	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-159	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo
500-160	NO CLASIFICADA	BAJA	BAJA	MEDIO
500-161	INFORMACIÓN PÚBLICA RESERVADA	ALTA	ALTA	ALTA
500-162	INFORMACIÓN PÚBLICA RESERVADA	MEDIA	MEDIA	MEDIO
600-163	NO CLASIFICADA	NO CLASIFICADA	MEDIA	ALTA
600-164	NO CLASIFICADA	NO CLASIFICADA	MEDIA	ALTA

4.1.6. Análisis de riesgos ODEI Pasco

- **Identificación de Amenazas.** Para realizar el análisis de riesgos se deben identificar las amenazas para los activos de información de la ODEI Pasco y así identificar las amenazas que se pueden presentar con dichos activos. Para ello se identifica el tipo de amenaza de acuerdo al tipo de activo de información teniendo como referencia el catálogo de elementos del libro 2 de la metodología MAGERIT V.3.

La clasificación de amenazas propuesta por la metodología, son las siguientes:

- ***Desastres naturales.*** relacionados a los fenómenos o eventos naturales.
- ***De origen industrial.*** relacionados a los eventos producidos por la acción humana ocurridos de forma accidental tales como averías de tipo físico o lógico, malas condiciones ambientales o degradación de medios de almacenamiento.
- ***Errores y fallo no intencionados.*** relacionados a errores por descuido o desconocimiento de las personas.
- ***Ataques intencionados.*** relacionados a daños ocasionados por personas inescrupulosas con objetivos de alterar o sustraer algún activo de la entidad.

En la ODEI Pasco se identificaron las siguientes amenazas relacionadas a los activos de información:

Tabla 3

Identificación de Amenazas – ODEI Pasco

ORIGEN		RIESGO		VULNERABILIDAD
ORGANIZACIÓN				
DESASTRES NATURALES	N	Tormentas eléctricas		Debido a la falta de infraestructura apropiada podría ocasionar daños a los equipos informáticos utilizados en la ODEI Pasco
INFORMACIÓN				
ORIGEN INDUSTRIAL	I	Avería de origen físico o lógico	I.5	Los fallos en los equipos y/o fallos en los aplicativos para recojo de información, puede ser debida a un defecto de fábrica o por el funcionamiento del sistema o aplicativos utilizados
		Cortes de suministro eléctrico	I.6	Debido a las fluctuaciones o sobrecargas de energía provocan que los UPS se sobrecarguen lo cual podría provocar daños o pérdidas de información
		Fallo de servicios de comunicaciones	I.8	Interrupción en el envío de información a la Sede Central del INEI por fallas en el servidor
		Degradación de los soportes de almacenamiento de la información	I.10	no hay controles de seguridad para mantener la disponibilidad de los soportes de información y que estos no se deterioren con el uso y el paso del tiempo
ERRORES Y FALLOS NO INTENCIONADOS	E	Alteración accidental de la Información	E.15	La información puede ser alterada por error humano, se necesita realizar un respaldo para su recuperación (afecta su integridad)
		Destrucción de la Información	E.18	La información puede ser eliminada por error humano, se necesita realizar un respaldo para su recuperación (afecta su disponibilidad)
		Fugas de Información	E.19	La información puede ser expuesta, por error se puede enviar a personas ajenas fuera de la institución
		Pérdida de equipos	E.25	El uso de dispositivos externos de almacenamiento como USB y tabletas, afectan la confiabilidad y confidencialidad de la información y esta pueda ser expuesta.
ATAQUES INTENSIONADOS	A	Manipulación de la configuración	A.4	La manipulación en la configuración de las tabletas necesarias para el recojo de la información pueden afectar la integridad de la información

ORIGEN		RIESGO		VULNERABILIDAD
		Suplantación de la identidad de los usuarios	A.5	Los usuarios tienen sus niveles de privilegios y un equipo desatendido, conlleva a la suplantación de identidad por lo que la información peligra en su confidencialidad, autenticidad e integridad.
		Abuso de los privilegios de acceso	A.6	Cada usuario tiene privilegios hacia un determinado propósito, cuando abusa de este privilegio para realizar tareas fuera de su competencia la información se expone en su confidencialidad, integridad y disponibilidad
		Uso no previsto	A.7	No hay un control para el uso de los recursos, equipos de la institución debido a que algunos equipos no cuentan con acceso restringido
		Modificación deliberada de información	A.15	Alteración de la información, ánimo de obtener beneficio o causar un perjuicio
		Destrucción de Información	A.18	Eliminación de información, ánimo de obtener beneficio o causar un perjuicio
		Divulgación de información	A.19	Compartir información no autorizada
		Manipulación de programas	A.22	Alteración intencionada de aplicativos y programas
		Manipulación de equipos	A.23	Alteración intencionada de equipos
		Robo de información	A.25	Sustracción de información por personal interno o contratadas en forma temporal
		Ataque destructivo	A.26	Si algún software malicioso afecte la información en sus diferentes niveles
SERVICIOS				
ORIGEN INDUSTRIAL	I	Fluctuaciones o sobrecargas eléctricas		Pueden verse afectado los servicios de impresión y escaneo de documentos
		Fallo de servicios de comunicaciones	I.8	Interrupción en el envío de información a la Sede Central del INEI por fallas en el servidor
		Interrupción de otros servicios y suministros esenciales	I.9	El servicio de impresión puede verse afectado por falta de suministros
ATAQUES INTENSIONADOS	A	Uso no previsto	A.7	El uso de páginas web no relacionadas al ámbito laboral
		Modificación deliberada de información	A.15	Falta de control en el uso de algunos equipos
		Destrucción de Información	A.18	Perdida de información o de algunas carpetas en equipos con escaso nivel de seguridad

ORIGEN		RIESGO		VULNERABILIDAD
		Divulgación de información	A.19	Usuarios no autorizados pueden hacer búsquedas en carpetas de otros usuarios
SOFTWARE				
ORIGEN INDUSTRIAL	I	Avería de origen físico o lógico	I.5	La exposición de equipos sin un adecuado almacenamiento puede derivar al deterioro del sistema
ERRORES Y FALLOS NO INTENCIONADOS	E	Errores de usuario	E.1	Falta de capacitación en el uso adecuado de los equipos
		Difusión de software dañino	E.8	Falta de capacitación sobre seguridad y prevención de amenazas de aspecto informático
		Alteraciones accidentales de información	E.15	No existe un control y monitoreo adecuado de almacenamiento de información en los equipos de la ODEI Pasco
		Destrucción de la Información	E.18	Falta establecer los niveles de seguridad de la información
		Errores de mantenimiento y actualizaciones de programas	E.21	Falta de un inventario de software y programas
ATAQUES INTENSIONADOS	A	Suplantación de la identidad de los usuarios	A.5	Los usuarios tienen sus niveles de privilegios y un equipo desatendido, conlleva a la suplantación de identidad por lo que la información peligra en su confidencialidad, autenticidad e integridad.
		Abuso de los privilegios de acceso	A.6	Cada usuario tiene privilegios hacia un determinado propósito, cuando abusa de este privilegio para realizar tareas fuera de su competencia la información se expone en su confidencialidad, integridad y disponibilidad
		Uso no previsto	A.7	No hay un control para el uso de los recursos, equipos de la institución debido a que algunos equipos no cuentan con acceso restringido
		Difusión de software dañino	A.8	Falta de control en el uso de navegadores web
		Re-encadenamiento de mensajes	A.9	Falta de control en el uso de los correos electrónicos
		Destrucción de Información	A.18	Eliminación de información, ánimo de obtener beneficio o causar un perjuicio
		Divulgación de información	A.19	Compartir información no autorizada
		Manipulación de programas	A.22	Alteración intencionada de aplicativos y programas
HARDWARE				

ORIGEN		RIESGO		VULNERABILIDAD
ORIGEN INDUSTRIAL	I	Avería de origen físico o lógico	I.5	La exposición de equipos sin un adecuado almacenamiento puede derivar a su deterioro
		Cortes de suministro eléctrico	I.6	Debido a las fluctuaciones o sobrecargas de energía provocan que los UPS se sobrecarguen lo cual podría provocar daños a los equipos
ERRORES Y FALLOS NO INTENCIONADOS	E	Errores de mantenimiento y actualización de hardware	E.23	Mantenimiento de equipos no planificados
ATAQUES INTENSIONADOS	A	Uso no previsto	A.7	Uso de equipos en actividades de ocio y asuntos personales
COMUNICACIONES				
ORIGEN INDUSTRIAL	I	Fallo de servicios de comunicaciones	I.8	La tercerización del servicio de internet puede ocasionar problemas de comunicación con los servidores de la Sede Central
ERRORES Y FALLOS NO INTENCIONADOS	E	Caída del sistema por agotamiento de recursos	E.24	La comunicación con los servidores de Sede Central para la aplicaciones y base de datos se ve afectado cuando el canal de comunicaciones se satura por la cantidad de paquetes enviados
ATAQUES INTENSIONADOS	A	Suplantación de la identidad de los usuarios	A.5	Los usuarios tienen sus niveles de privilegios y un equipo desatendido, conlleva a la suplantación de identidad por lo que la información peligra en su confidencialidad, autenticidad e integridad.
		Abuso de los privilegios de acceso	A.6	Cada usuario tiene privilegios hacia un determinado propósito, cuando abusa de este privilegio para realizar tareas fuera de su competencia la información se expone en su confidencialidad, integridad y disponibilidad
		Uso no previsto	A.7	No hay un control para el uso de los recursos, equipos de la institución debido a que algunos equipos no cuentan con acceso restringido
		Acceso no autorizado	A.11	Vulnerabilidad en los accesos al WIFI ya que no se tiene un debido control de accesos
ELEMENTOS AUXILIARES				
ORIGEN INDUSTRIAL	I	Fuego	I.1	Las instalaciones y cableado eléctrico se encuentran expuestas en alguna medida
		Avería de origen físico o lógico	I.5	Daños en los equipos auxiliares por falta de mantenimiento
		Degradación de los soportes de almacenamiento	I.10	Deterioro a largo plazo de instalaciones y cableados eléctricos

ORIGEN		RIESGO		VULNERABILIDAD
		de la información		
ERRORES Y FALLOS NO INTENCIONADOS	E	Errores de mantenimiento y actualización de hardware	E.23	Mantenimiento de equipos no planificados
ATAQUES INTENSIONADOS	A	Ataque destructivo	A.26	Al estar parte del cableado fuera de canaletas están propicias a corte o sabotaje de las mismas
INSTALACIONES				
DESASTRES NATURALES	N	Daños por agua	N.2	La infraestructura por su antigüedad y falta de mantenimiento es propensa que sufra por lluvias de goteras
ORIGEN INDUSTRIAL	I	Fluctuaciones o sobrecargas eléctricas		Las instalaciones eléctricas podrían sufrir sobrecarga de energía
RECURSOS HUMANOS				
ORIGEN INDUSTRIAL	I	Fluctuaciones o sobrecargas eléctricas		Los altibajos en el suministro eléctrico afectan el desempeño del personal
ERRORES Y FALLOS NO INTENCIONADOS	E	Deficiencias en la organización	E.7	La falta de procedimientos claros por falta de manuales e instructivos hace que el personal cometa errores
		Fuga de información	E.19	Falta de control en la manipulación de la información digital hace que esa información se ve expuesta
ATAQUES INTENSIONADOS	A	Indisponibilidad del personal	A.28	Renuncias del personal

Estas amenazas se deben valorar y para ello se consideraron los activos que obtuvieron un grado de criticidad ALTA, los activos de información se valoraron bajo los criterios:

- ***Probabilidad.*** determinado por la probabilidad de ocurrencia, por el número veces que el activo de información pueda ser afectado por una amenaza en un determinado periodo de tiempo según el siguiente rango:

Tabla 4

Valoración de la Probabilidad

PROBABILIDAD		
Frecuencia muy baja	Puede ocurrir una vez por año o mas	1
Frecuencia baja	Puede ocurrir una vez por semestre	2
Frecuencia media	Puede ocurrir en un mes	3
Frecuencia alta	Puede ocurrir una vez a la semana	4
Frecuencia muy alta	Puede ocurrir una vez al día	5

- ***Impacto.*** nivel en el cual el activo de información puede ser afectado dependiendo del nivel de ***seguridad***, utilizado para ello el siguiente rango:

Tabla 5

Valoración del Impacto

IMPACTO		
Muy bajo	5%	1
Bajo	20%	2
Medio	50%	3
Alto	75%	4
Muy alto	100%	5

- **Valoración del Riesgo.** Para realizar la valoración del riesgo se realiza mediante la siguiente formula:

Riesgo = Probabilidad * Impacto

Se definen los siguientes niveles de riesgo:

- ***Alto.*** cuando la amenaza puede ocurrir con frecuencia y el impacto es alto en los activos de información, en este punto es necesario evaluar que tipos de controles son necesarios para corregir.
- ***Medio.*** cuando la amenaza se puede presentar con frecuencia, pero el impacto es moderado en los activos de información.
- ***Bajo.*** cuando la amenaza es esporádica y el impacto es bajo en los activos de información, se registrará el evento para contenerlo en una bitácora o historial.

Tabla 6

Niveles de Riesgo

NIVELES DE RIESGO	
PROBABILIDAD: IMPACTO	NIVEL DE RIESGO
1:1	Bajo
2:1	Bajo
3:1	Bajo
4:1	Bajo
1:2	Bajo
2:2	Bajo
1:3	Bajo

5:1	Medio
5:2	Medio
4:2	Medio
3:2	Medio
3:3	Medio
2:3	Medio
2:4	Medio
1:4	Medio
1:5	Medio
5:3	Alto
4:3	Alto
5:4	Alto
4:4	Alto
3:4	Alto
5:5	Alto
4:5	Alto
3:5	Alto
2:5	Alto

Aplicando el análisis de riesgos se obtienen los siguientes resultados:

Tabla 7

Valoración de Riesgos

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Alteración accidental de la Información	NORMAS INTERNAS	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	NORMAS INTERNAS	Puede ocurrir una vez por año o mas	1:5	Medio
Alteración accidental de la Información	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ASIGNADOS	Puede ocurrir una vez por año o mas	1:2	Bajo
Destrucción de la Información	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ASIGNADOS	Puede ocurrir una vez por año o mas	1:3	Bajo
Modificación deliberada de información	CONTROLES DE SEGURIDAD DE LA INFORMACIÓN ASIGNADOS	Puede ocurrir una vez por año o mas	1:3	Bajo
Alteración accidental de la Información	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	Puede ocurrir una vez por año o mas	1:1	Bajo
Modificación deliberada de información	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	Puede ocurrir una vez por año o mas	1:1	Bajo

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Fallo de servicios de comunicaciones	COORDINACIONES CON LAS OFICINAS ESTADÍSTICAS	Puede ocurrir una vez por semestre	2:2	Bajo
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN ENAHO	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	SEGUIMIENTO Y SUPERVISIÓN ENAHO	Puede ocurrir en un mes	3:4	Alto
Destrucción de la Información	SEGUIMIENTO Y SUPERVISIÓN ENAHO	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	SEGUIMIENTO Y SUPERVISIÓN ENAHO	Puede ocurrir una vez por semestre	2:2	Bajo
Modificación deliberada de información	SEGUIMIENTO Y SUPERVISIÓN ENAHO	Puede ocurrir una vez por semestre	2:5	Alto
Destrucción de Información	SEGUIMIENTO Y SUPERVISIÓN ENAHO	Puede ocurrir una vez por año o mas	1:5	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Divulgación de información	SEGUIMIENTO Y SUPERVISIÓN ENAHO	Puede ocurrir una vez a la semana	4:1	Bajo
Manipulación de equipos	SEGUIMIENTO Y SUPERVISIÓN ENAHO	Puede ocurrir en un mes	3:2	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	SEGUIMIENTO Y SUPERVISIÓN ENAPRES	Puede ocurrir en un mes	3:4	Alto
Destrucción de la Información	SEGUIMIENTO Y SUPERVISIÓN ENAPRES	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	SEGUIMIENTO Y SUPERVISIÓN ENAPRES	Puede ocurrir una vez por semestre	2:2	Bajo
Modificación deliberada de información	SEGUIMIENTO Y SUPERVISIÓN ENAPRES	Puede ocurrir una vez por semestre	2:5	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de Información	SEGUIMIENTO Y SUPERVISIÓN ENAPRES	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	SEGUIMIENTO Y SUPERVISIÓN ENAPRES	Puede ocurrir una vez a la semana	4:1	Bajo
Manipulación de equipos	SEGUIMIENTO Y SUPERVISIÓN ENAPRES	Puede ocurrir en un mes	3:2	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	SEGUIMIENTO Y SUPERVISIÓN ENDES 1	Puede ocurrir en un mes	3:4	Alto
Destrucción de la Información	SEGUIMIENTO Y SUPERVISIÓN ENDES 1	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	SEGUIMIENTO Y SUPERVISIÓN ENDES 1	Puede ocurrir una vez por semestre	2:2	Bajo

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Modificación deliberada de información	SEGUIMIENTO Y SUPERVISIÓN ENDES 1	Puede ocurrir una vez por semestre	2:5	Alto
Destrucción de Información	SEGUIMIENTO Y SUPERVISIÓN ENDES 1	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	SEGUIMIENTO Y SUPERVISIÓN ENDES 1	Puede ocurrir una vez a la semana	4:1	Bajo
Manipulación de equipos	SEGUIMIENTO Y SUPERVISIÓN ENDES 1	Puede ocurrir en un mes	3:2	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por semestre	2:4	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por año o mas	1:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	SEGUIMIENTO Y SUPERVISIÓN EPEN 1	Puede ocurrir en un mes	3:4	Alto
Destrucción de la Información	SEGUIMIENTO Y SUPERVISIÓN EPEN 1	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	SEGUIMIENTO Y SUPERVISIÓN EPEN 1	Puede ocurrir una vez por semestre	2:2	Bajo
Modificación deliberada de información	SEGUIMIENTO Y SUPERVISIÓN EPEN 1	Puede ocurrir una vez por semestre	2:5	Alto
Destrucción de Información	SEGUIMIENTO Y SUPERVISIÓN EPEN 1	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	SEGUIMIENTO Y SUPERVISIÓN EPEN 1	Puede ocurrir una vez a la semana	4:1	Bajo
Manipulación de equipos	SEGUIMIENTO Y SUPERVISIÓN EPEN 1	Puede ocurrir en un mes	3:2	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por año o mas	1:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
almacenamiento de la información				
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por semestre	2:4	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir una vez por año o mas	1:5	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN CENSOS 1	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 1	Puede ocurrir en un mes	3:4	Alto
Destrucción de la Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 1	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 1	Puede ocurrir una vez por semestre	2:2	Bajo
Modificación deliberada de información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 1	Puede ocurrir una vez por semestre	2:5	Alto
Destrucción de Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 1	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 1	Puede ocurrir una vez a la semana	4:1	Bajo
Manipulación de equipos	SEGUIMIENTO Y SUPERVISIÓN CENSOS 1	Puede ocurrir en un mes	3:2	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir una vez por semestre	2:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN CENSOS 2	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 2	Puede ocurrir en un mes	3:4	Alto
Destrucción de la Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 2	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 2	Puede ocurrir una vez por semestre	2:2	Bajo
Modificación deliberada de información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 2	Puede ocurrir una vez por semestre	2:5	Alto
Destrucción de Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 2	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	SEGUIMIENTO Y SUPERVISIÓN CENSOS 2	Puede ocurrir una vez a la semana	4:1	Bajo
Manipulación de equipos	SEGUIMIENTO Y SUPERVISIÓN CENSOS 2	Puede ocurrir en un mes	3:2	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir una vez por semestre	2:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN CENSOS	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS	Puede ocurrir en un mes	3:4	Alto
Destrucción de la Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS	Puede ocurrir una vez por semestre	2:2	Bajo
Modificación deliberada de información	SEGUIMIENTO Y SUPERVISIÓN CENSOS	Puede ocurrir una vez por semestre	2:5	Alto
Destrucción de Información	SEGUIMIENTO Y SUPERVISIÓN CENSOS	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	SEGUIMIENTO Y SUPERVISIÓN CENSOS	Puede ocurrir una vez a la semana	4:1	Bajo
Manipulación de equipos	SEGUIMIENTO Y SUPERVISIÓN CENSOS	Puede ocurrir en un mes	3:2	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN	Puede ocurrir en un mes	3:1	Bajo

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
	ENCUESTAS TEMPORALES			
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	SEGUIMIENTO Y SUPERVISIÓN ENCUESTAS TEMPORALES	Puede ocurrir en un mes	3:4	Alto
Destrucción de la Información	SEGUIMIENTO Y SUPERVISIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	SEGUIMIENTO Y SUPERVISIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:2	Bajo
Modificación deliberada de información	SEGUIMIENTO Y SUPERVISIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:5	Alto
Destrucción de Información	SEGUIMIENTO Y SUPERVISIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	SEGUIMIENTO Y SUPERVISIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez a la semana	4:1	Bajo
Manipulación de equipos	SEGUIMIENTO Y SUPERVISIÓN ENCUESTAS TEMPORALES	Puede ocurrir en un mes	3:2	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Avería de origen físico o lógico	INFORME DE INCIDENCIAS	Puede ocurrir una vez por año o mas	1:2	Bajo
Cortes de suministro eléctrico	INFORME DE INCIDENCIAS	Puede ocurrir una vez por año o mas	1:1	Bajo
Fallo de servicios de comunicaciones	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:3	Medio
Degradación de los soportes de almacenamiento de la información	INFORME DE INCIDENCIAS	Puede ocurrir una vez por año o mas	1:2	Bajo
Alteración accidental de la Información	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de la Información	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:5	Alto
Fugas de Información	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:3	Medio
Pérdida de equipos	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:4	Medio
Manipulación de la configuración	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:4	Medio
Abuso de los privilegios de acceso	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:5	Alto
Destrucción de Información	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:5	Alto
Divulgación de información	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:3	Medio
Manipulación de programas	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:3	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Manipulación de equipos	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:4	Medio
Robo de información	INFORME DE INCIDENCIAS	Puede ocurrir una vez a la semana	4:5	Alto
Ataque destructivo	INFORME DE INCIDENCIAS	Puede ocurrir una vez por semestre	2:5	Alto
Cortes de suministro eléctrico	MONITOREO CONEXIONES	Puede ocurrir una vez por año o mas	1:4	Medio
Fallo de servicios de comunicaciones	MONITOREO CONEXIONES	Puede ocurrir una vez por año o mas	1:5	Medio
Manipulación de la configuración	MONITOREO CONEXIONES	Puede ocurrir una vez por año o mas	1:4	Medio
Suplantación de la identidad de los usuarios	MONITOREO CONEXIONES	Puede ocurrir una vez por semestre	2:5	Alto
Abuso de los privilegios de acceso	MONITOREO CONEXIONES	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	MONITOREO CONEXIONES	Puede ocurrir una vez por semestre	2:1	Bajo
Ataque destructivo	MONITOREO CONEXIONES	Puede ocurrir una vez por año o mas	1:5	Medio
Alteración accidental de la Información	FORMATO A1	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	FORMATO A1	Puede ocurrir en un mes	3:4	Alto
Fugas de Información	FORMATO A1	Puede ocurrir una vez por año o mas	1:4	Medio
Modificación deliberada de información	FORMATO A1	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	FORMATO A1	Puede ocurrir en un mes	3:5	Alto
Robo de información	FORMATO A1	Puede ocurrir una vez por semestre	2:3	Medio
Alteración accidental de la Información	FORMATO A26	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	FORMATO A26	Puede ocurrir en un mes	3:4	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Fugas de Información	FORMATO A26	Puede ocurrir una vez por año o mas	1:4	Medio
Modificación deliberada de información	FORMATO A26	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	FORMATO A26	Puede ocurrir en un mes	3:5	Alto
Robo de información	FORMATO A26	Puede ocurrir una vez por semestre	2:3	Medio
Alteración accidental de la Información	FORMATO A32	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	FORMATO A32	Puede ocurrir en un mes	3:4	Alto
Fugas de Información	FORMATO A32	Puede ocurrir una vez por año o mas	1:4	Medio
Modificación deliberada de información	FORMATO A32	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	FORMATO A32	Puede ocurrir en un mes	3:5	Alto
Robo de información	FORMATO A32	Puede ocurrir una vez por semestre	2:3	Medio
Cortes de suministro eléctrico	INGRESO DE DATOS IPC A SIIP	Puede ocurrir una vez por año o mas	1:3	Bajo
Alteración accidental de la Información	INGRESO DE DATOS IPC A SIIP	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	INGRESO DE DATOS IPC A SIIP	Puede ocurrir una vez por año o mas	1:5	Medio
Fugas de Información	INGRESO DE DATOS IPC A SIIP	Puede ocurrir en un mes	3:1	Bajo
Modificación deliberada de información	INGRESO DE DATOS IPC A SIIP	Puede ocurrir en un mes	3:5	Alto
Destrucción de Información	INGRESO DE DATOS IPC A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Divulgación de información	INGRESO DE DATOS IPC A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	INGRESO DE DATOS IPC A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	ANÁLISIS DE INFORMACIÓN DE IPC	Puede ocurrir una vez por año o mas	1:3	Bajo

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de la Información	ANÁLISIS DE INFORMACIÓN DE IPC	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	ANÁLISIS DE INFORMACIÓN DE IPC	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	ANÁLISIS DE INFORMACIÓN DE IPC	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	ANÁLISIS DE INFORMACIÓN DE IPC	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	ANÁLISIS DE INFORMACIÓN DE IPC	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	ANÁLISIS DE INFORMACIÓN DE IPC	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	CONSISTENCIA DE INFORMACIÓN DE IPC	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	CONSISTENCIA DE INFORMACIÓN DE IPC	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	CONSISTENCIA DE INFORMACIÓN DE IPC	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	CONSISTENCIA DE INFORMACIÓN DE IPC	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	CONSISTENCIA DE INFORMACIÓN DE IPC	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	CONSISTENCIA DE INFORMACIÓN DE IPC	Puede ocurrir una vez por año o mas	1:1	Bajo
Robo de información	CONSISTENCIA DE INFORMACIÓN DE IPC	Puede ocurrir una vez por año o mas	1:5	Medio
Alteración accidental de la Información	CUADRO FINAL DEL IPC DEPARTAMENTAL	Puede ocurrir una vez por año o mas	1:4	Medio
Destrucción de la Información	CUADRO FINAL DEL IPC DEPARTAMENTAL	Puede ocurrir en un mes	3:4	Alto
Fugas de Información	CUADRO FINAL DEL IPC DEPARTAMENTAL	Puede ocurrir una vez por año o mas	1:3	Bajo
Modificación deliberada de información	CUADRO FINAL DEL IPC DEPARTAMENTAL	Puede ocurrir en un mes	3:5	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de Información	CUADRO FINAL DEL IPC DEPARTAMENTAL	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	CUADRO FINAL DEL IPC DEPARTAMENTAL	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	CUADRO FINAL DEL IPC DEPARTAMENTAL	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	FORMATO IUPC	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	FORMATO IUPC	Puede ocurrir en un mes	3:4	Alto
Fugas de Información	FORMATO IUPC	Puede ocurrir una vez por año o mas	1:4	Medio
Modificación deliberada de información	FORMATO IUPC	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	FORMATO IUPC	Puede ocurrir en un mes	3:5	Alto
Robo de información	FORMATO IUPC	Puede ocurrir una vez por semestre	2:3	Medio
Cortes de suministro eléctrico	INGRESO DE DATOS IUPC A SIIP	Puede ocurrir una vez por año o mas	1:3	Bajo
Alteración accidental de la Información	INGRESO DE DATOS IUPC A SIIP	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	INGRESO DE DATOS IUPC A SIIP	Puede ocurrir una vez por año o mas	1:5	Medio
Fugas de Información	INGRESO DE DATOS IUPC A SIIP	Puede ocurrir en un mes	3:1	Bajo
Modificación deliberada de información	INGRESO DE DATOS IUPC A SIIP	Puede ocurrir en un mes	3:5	Alto
Destrucción de Información	INGRESO DE DATOS IUPC A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Divulgación de información	INGRESO DE DATOS IUPC A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	INGRESO DE DATOS IUPC A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	ANÁLISIS DE INFORMACIÓN DE IUPC	Puede ocurrir una vez por año o mas	1:3	Bajo

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de la Información	ANÁLISIS DE INFORMACIÓN DE IUPC	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	ANÁLISIS DE INFORMACIÓN DE IUPC	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	ANÁLISIS DE INFORMACIÓN DE IUPC	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	ANÁLISIS DE INFORMACIÓN DE IUPC	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	ANÁLISIS DE INFORMACIÓN DE IUPC	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	ANÁLISIS DE INFORMACIÓN DE IUPC	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	CONSISTENCIA DE INFORMACIÓN DE IUPC	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	CONSISTENCIA DE INFORMACIÓN DE IUPC	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	CONSISTENCIA DE INFORMACIÓN DE IUPC	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	CONSISTENCIA DE INFORMACIÓN DE IUPC	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	CONSISTENCIA DE INFORMACIÓN DE IUPC	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	CONSISTENCIA DE INFORMACIÓN DE IUPC	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	CONSISTENCIA DE INFORMACIÓN DE IUPC	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	CUADRO FINAL DEL IUPC DEPARTAMENTAL	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	CUADRO FINAL DEL IUPC DEPARTAMENTAL	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	CUADRO FINAL DEL IUPC DEPARTAMENTAL	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	CUADRO FINAL DEL IUPC DEPARTAMENTAL	Puede ocurrir en un mes	3:1	Bajo

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de Información	CUADRO FINAL DEL IUPC DEPARTAMENTAL	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	CUADRO FINAL DEL IUPC DEPARTAMENTAL	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	CUADRO FINAL DEL IUPC DEPARTAMENTAL	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	FORMATO IPM	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	FORMATO IPM	Puede ocurrir en un mes	3:4	Alto
Fugas de Información	FORMATO IPM	Puede ocurrir una vez por año o mas	1:4	Medio
Modificación deliberada de información	FORMATO IPM	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	FORMATO IPM	Puede ocurrir en un mes	3:5	Alto
Robo de información	FORMATO IPM	Puede ocurrir una vez por semestre	2:3	Medio
Cortes de suministro eléctrico	INGRESO DE DATOS IPM A SIIP	Puede ocurrir una vez por año o mas	1:3	Bajo
Alteración accidental de la Información	INGRESO DE DATOS IPM A SIIP	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	INGRESO DE DATOS IPM A SIIP	Puede ocurrir una vez por año o mas	1:5	Medio
Fugas de Información	INGRESO DE DATOS IPM A SIIP	Puede ocurrir en un mes	3:1	Bajo
Modificación deliberada de información	INGRESO DE DATOS IPM A SIIP	Puede ocurrir en un mes	3:5	Alto
Destrucción de Información	INGRESO DE DATOS IPM A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Divulgación de información	INGRESO DE DATOS IPM A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	INGRESO DE DATOS IPM A SIIP	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	ANÁLISIS DE INFORMACIÓN DE IPM	Puede ocurrir una vez por año o mas	1:3	Bajo

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de la Información	ANÁLISIS DE INFORMACIÓN DE IPM	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	ANÁLISIS DE INFORMACIÓN DE IPM	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	ANÁLISIS DE INFORMACIÓN DE IPM	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	ANÁLISIS DE INFORMACIÓN DE IPM	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	ANÁLISIS DE INFORMACIÓN DE IPM	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	ANÁLISIS DE INFORMACIÓN DE IPM	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	CONSISTENCIA DE INFORMACIÓN DE IPM	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	CONSISTENCIA DE INFORMACIÓN DE IPM	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	CONSISTENCIA DE INFORMACIÓN DE IPM	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	CONSISTENCIA DE INFORMACIÓN DE IPM	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	CONSISTENCIA DE INFORMACIÓN DE IPM	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	CONSISTENCIA DE INFORMACIÓN DE IPM	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	CONSISTENCIA DE INFORMACIÓN DE IPM	Puede ocurrir una vez por año o mas	1:4	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir una vez a la semana	4:3	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN EVOLUCIÓN MENSUAL	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	AVANCE ECONÓMICO Y SOCIAL REGIONAL MENSUAL	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	AVANCE ECONÓMICO Y SOCIAL REGIONAL MENSUAL	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	AVANCE ECONÓMICO Y SOCIAL REGIONAL MENSUAL	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	AVANCE ECONÓMICO Y SOCIAL REGIONAL MENSUAL	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	AVANCE ECONÓMICO Y SOCIAL REGIONAL MENSUAL	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	AVANCE ECONÓMICO Y	Puede ocurrir una vez por año o mas	1:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
	SOCIAL REGIONAL MENSUAL			
Robo de información	AVANCE ECONÓMICO Y SOCIAL REGIONAL MENSUAL	Puede ocurrir una vez por año o mas	1:4	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por semestre	2:4	Medio
Cortes de suministro eléctrico	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:3	Bajo
Alteración accidental de la Información	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:5	Medio
Fugas de Información	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir en un mes	3:1	Bajo

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Modificación deliberada de información	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir en un mes	3:5	Alto
Destrucción de Información	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:4	Medio
Divulgación de información	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	ACTUALIZACIÓN DE INFORMACIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	EDICIÓN	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	EDICIÓN	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	EDICIÓN	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	EDICIÓN	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	EDICIÓN	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	EDICIÓN	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	EDICIÓN	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	REVISIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	REVISIÓN COMPENDIO	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	REVISIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	REVISIÓN COMPENDIO	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	REVISIÓN COMPENDIO	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	REVISIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	REVISIÓN COMPENDIO	Puede ocurrir una vez por año o mas	1:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por semestre	2:4	Medio
Cortes de suministro eléctrico	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por año o mas	1:3	Bajo
Alteración accidental de la Información	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por año o mas	1:5	Medio
Fugas de Información	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Puede ocurrir en un mes	3:1	Bajo
Modificación deliberada de información	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Puede ocurrir en un mes	3:5	Alto
Destrucción de Información	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por año o mas	1:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Divulgación de información	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	ACTUALIZACIÓN DE INFORMACIÓN SERIES	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	REVISIÓN SERIES	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	REVISIÓN SERIES	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	REVISIÓN SERIES	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	REVISIÓN SERIES	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	REVISIÓN SERIES	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	REVISIÓN SERIES	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	REVISIÓN SERIES	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	FORMATO 2 - MATRIMONIOS Y DIVORCIOS	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	FORMATO 2 - MATRIMONIOS Y DIVORCIOS	Puede ocurrir en un mes	3:4	Alto
Fugas de Información	FORMATO 2 - MATRIMONIOS Y DIVORCIOS	Puede ocurrir una vez por año o mas	1:4	Medio
Modificación deliberada de información	FORMATO 2 - MATRIMONIOS Y DIVORCIOS	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	FORMATO 2 - MATRIMONIOS Y DIVORCIOS	Puede ocurrir en un mes	3:5	Alto
Robo de información	FORMATO 2 - MATRIMONIOS Y DIVORCIOS	Puede ocurrir una vez por semestre	2:3	Medio
Alteración accidental de la Información	FORMATO 2 - NACIMIENTOS Y DEFUNCIONES	Puede ocurrir en un mes	3:5	Alto
Destrucción de la Información	FORMATO 2 - NACIMIENTOS Y DEFUNCIONES	Puede ocurrir en un mes	3:4	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Fugas de Información	FORMATO 2 - NACIMIENTOS Y DEFUNCIONES	Puede ocurrir una vez por año o mas	1:4	Medio
Modificación deliberada de información	FORMATO 2 - NACIMIENTOS Y DEFUNCIONES	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	FORMATO 2 - NACIMIENTOS Y DEFUNCIONES	Puede ocurrir en un mes	3:5	Alto
Robo de información	FORMATO 2 - NACIMIENTOS Y DEFUNCIONES	Puede ocurrir una vez por semestre	2:3	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN RENAMU 1	Puede ocurrir una vez por semestre	2:4	Medio
Avería de origen físico o lógico	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir una vez a la semana	4:4	Alto
Degradación de los soportes de almacenamiento de la información	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir una vez por año o mas	1:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Alteración accidental de la Información	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir una vez a la semana	4:3	Alto
Destrucción de la Información	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir una vez por año o mas	1:4	Medio
Fugas de Información	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir en un mes	3:1	Bajo
Pérdida de equipos	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir una vez por semestre	2:4	Medio
Modificación deliberada de información	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir una vez por semestre	2:4	Medio
Destrucción de Información	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir una vez por año o mas	1:5	Medio
Divulgación de información	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir en un mes	3:3	Medio
Manipulación de equipos	RECOPILACIÓN DE INFORMACIÓN RENAMU 2	Puede ocurrir una vez por semestre	2:4	Medio
Alteración accidental de la Información	TABULACIÓN DE INFORMACIÓN	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	TABULACIÓN DE INFORMACIÓN	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	TABULACIÓN DE INFORMACIÓN	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	TABULACIÓN DE INFORMACIÓN	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	TABULACIÓN DE INFORMACIÓN	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	TABULACIÓN DE INFORMACIÓN	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	TABULACIÓN DE INFORMACIÓN	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	CONSISTENCIA DE INFORMACIÓN DE RENAMU	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	CONSISTENCIA DE INFORMACIÓN DE RENAMU	Puede ocurrir en un mes	3:5	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Fugas de Información	CONSISTENCIA DE INFORMACIÓN DE RENAMU	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	CONSISTENCIA DE INFORMACIÓN DE RENAMU	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	CONSISTENCIA DE INFORMACIÓN DE RENAMU	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	CONSISTENCIA DE INFORMACIÓN DE RENAMU	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	CONSISTENCIA DE INFORMACIÓN DE RENAMU	Puede ocurrir una vez por año o mas	1:4	Medio
Alteración accidental de la Información	CONSISTENCIA DE INFORMACIÓN CARTOGRÁFICA	Puede ocurrir una vez por año o mas	1:3	Bajo
Destrucción de la Información	CONSISTENCIA DE INFORMACIÓN CARTOGRÁFICA	Puede ocurrir en un mes	3:5	Alto
Fugas de Información	CONSISTENCIA DE INFORMACIÓN CARTOGRÁFICA	Puede ocurrir una vez por año o mas	1:5	Medio
Modificación deliberada de información	CONSISTENCIA DE INFORMACIÓN CARTOGRÁFICA	Puede ocurrir en un mes	3:1	Bajo
Destrucción de Información	CONSISTENCIA DE INFORMACIÓN CARTOGRÁFICA	Puede ocurrir en un mes	3:5	Alto
Divulgación de información	CONSISTENCIA DE INFORMACIÓN CARTOGRÁFICA	Puede ocurrir una vez por año o mas	1:4	Medio
Robo de información	CONSISTENCIA DE INFORMACIÓN CARTOGRÁFICA	Puede ocurrir una vez por año o mas	1:4	Medio
Fluctuaciones o sobrecargas eléctricas	PETICIÓN	Puede ocurrir una vez por año o mas	1:3	Bajo
Fallo de servicios de comunicaciones	PETICIÓN	Puede ocurrir en un mes	3:3	Medio
Interrupción de otros servicios y suministros esenciales	PETICIÓN	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	PETICIÓN	Puede ocurrir una vez por semestre	2:3	Medio
Modificación deliberada de información	PETICIÓN	Puede ocurrir una vez por semestre	2:3	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de Información	PETICIÓN	Puede ocurrir una vez por semestre	2:3	Medio
Divulgación de información	PETICIÓN	Puede ocurrir una vez por semestre	2:4	Medio
Fluctuaciones o sobrecargas eléctricas	SEGUIMIENTO PETICIONES	Puede ocurrir una vez por semestre	2:2	Bajo
Fallo de servicios de comunicaciones	SEGUIMIENTO PETICIONES	Puede ocurrir una vez por semestre	2:2	Bajo
Interrupción de otros servicios y suministros esenciales	SEGUIMIENTO PETICIONES	Puede ocurrir una vez por semestre	2:3	Medio
Uso no previsto	SEGUIMIENTO PETICIONES	Puede ocurrir una vez por semestre	2:2	Bajo
Modificación deliberada de información	SEGUIMIENTO PETICIONES	Puede ocurrir una vez por semestre	2:2	Bajo
Destrucción de Información	SEGUIMIENTO PETICIONES	Puede ocurrir una vez por semestre	2:2	Bajo
Divulgación de información	SEGUIMIENTO PETICIONES	Puede ocurrir una vez por año o mas	1:3	Bajo
Errores de usuario	UNETE	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	UNETE	Puede ocurrir en un mes	3:4	Alto
Alteraciones accidentales de información	UNETE	Puede ocurrir en un mes	3:3	Medio
Destrucción de la Información	UNETE	Puede ocurrir una vez por semestre	2:4	Medio
Errores de mantenimiento y actualizaciones de programas	UNETE	Puede ocurrir una vez por semestre	2:3	Medio
Suplantación de la identidad de los usuarios	UNETE	Puede ocurrir en un mes	3:2	Medio
Abuso de los privilegios de acceso	UNETE	Puede ocurrir en un mes	3:2	Medio
Uso no previsto	UNETE	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	UNETE	Puede ocurrir en un mes	3:4	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Destrucción de Información	UNETE	Puede ocurrir en un mes	3:2	Medio
Divulgación de información	UNETE	Puede ocurrir en un mes	3:3	Medio
Manipulación de programas	UNETE	Puede ocurrir en un mes	3:4	Alto
Errores de usuario	RENAMU	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	RENAMU	Puede ocurrir en un mes	3:4	Alto
Alteraciones accidentales de información	RENAMU	Puede ocurrir en un mes	3:3	Medio
Destrucción de la Información	RENAMU	Puede ocurrir una vez por semestre	2:4	Medio
Errores de mantenimiento y actualizaciones de programas	RENAMU	Puede ocurrir una vez por semestre	2:3	Medio
Suplantación de la identidad de los usuarios	RENAMU	Puede ocurrir en un mes	3:2	Medio
Abuso de los privilegios de acceso	RENAMU	Puede ocurrir en un mes	3:2	Medio
Uso no previsto	RENAMU	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	RENAMU	Puede ocurrir en un mes	3:4	Alto
Destrucción de Información	RENAMU	Puede ocurrir en un mes	3:2	Medio
Divulgación de información	RENAMU	Puede ocurrir en un mes	3:3	Medio
Manipulación de programas	RENAMU	Puede ocurrir en un mes	3:4	Alto
Errores de usuario	SGD	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	SGD	Puede ocurrir en un mes	3:4	Alto
Alteraciones accidentales de información	SGD	Puede ocurrir en un mes	3:3	Medio
Destrucción de la Información	SGD	Puede ocurrir una vez por semestre	2:4	Medio
Errores de mantenimiento y actualizaciones de programas	SGD	Puede ocurrir una vez por semestre	2:3	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Suplantación de la identidad de los usuarios	SGD	Puede ocurrir en un mes	3:2	Medio
Abuso de los privilegios de acceso	SGD	Puede ocurrir en un mes	3:2	Medio
Uso no previsto	SGD	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	SGD	Puede ocurrir en un mes	3:4	Alto
Re-encadenamiento de mensajes	SGD	Puede ocurrir en un mes	3:3	Medio
Destrucción de Información	SGD	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	SGD	Puede ocurrir en un mes	3:3	Medio
Manipulación de programas	SGD	Puede ocurrir en un mes	3:4	Alto
Errores de usuario	SIIP	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	SIIP	Puede ocurrir en un mes	3:4	Alto
Alteraciones accidentales de información	SIIP	Puede ocurrir en un mes	3:3	Medio
Destrucción de la Información	SIIP	Puede ocurrir una vez por semestre	2:4	Medio
Errores de mantenimiento y actualizaciones de programas	SIIP	Puede ocurrir una vez por semestre	2:3	Medio
Suplantación de la identidad de los usuarios	SIIP	Puede ocurrir en un mes	3:2	Medio
Abuso de los privilegios de acceso	SIIP	Puede ocurrir en un mes	3:2	Medio
Uso no previsto	SIIP	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	SIIP	Puede ocurrir en un mes	3:4	Alto
Destrucción de Información	SIIP	Puede ocurrir en un mes	3:2	Medio
Divulgación de información	SIIP	Puede ocurrir en un mes	3:3	Medio
Manipulación de programas	SIIP	Puede ocurrir en un mes	3:4	Alto
Errores de usuario	OWA	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	OWA	Puede ocurrir en un mes	3:4	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Alteraciones accidentales de información	OWA	Puede ocurrir en un mes	3:3	Medio
Destrucción de la Información	OWA	Puede ocurrir una vez por semestre	2:4	Medio
Errores de mantenimiento y actualizaciones de programas	OWA	Puede ocurrir una vez por semestre	2:3	Medio
Suplantación de la identidad de los usuarios	OWA	Puede ocurrir en un mes	3:2	Medio
Abuso de los privilegios de acceso	OWA	Puede ocurrir en un mes	3:2	Medio
Uso no previsto	OWA	Puede ocurrir en un mes	3:2	Medio
Difusión de software dañino	OWA	Puede ocurrir en un mes	3:4	Alto
Re-encadenamiento de mensajes	OWA	Puede ocurrir en un mes	3:3	Medio
Destrucción de Información	OWA	Puede ocurrir en un mes	3:3	Medio
Divulgación de información	OWA	Puede ocurrir en un mes	3:3	Medio
Manipulación de programas	OWA	Puede ocurrir en un mes	3:4	Alto
Avería de origen físico o lógico	ACTIVOS INFORMÁTICOS	Puede ocurrir una vez por semestre	2:4	Medio
Cortes de suministro eléctrico	ACTIVOS INFORMÁTICOS	Puede ocurrir una vez por semestre	2:4	Medio
Errores de mantenimiento y actualización de hardware	ACTIVOS INFORMÁTICOS	Puede ocurrir una vez por año o mas	1:5	Medio
Uso no previsto	ACTIVOS INFORMÁTICOS	Puede ocurrir en un mes	3:4	Alto
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN ENAHO	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN ENAHO	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN ENAHO	Puede ocurrir una vez por semestre	2:3	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN ENAHO	Puede ocurrir una vez por semestre	2:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Uso no previsto	ENVIO DE INFORMACIÓN ENAHO	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN ENAHO	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN ENAPRES	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por semestre	2:3	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN ENAPRES	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN ENDES 1	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por semestre	2:4	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN ENDES 1	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN ENDES 2	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por semestre	2:3	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN ENDES 2	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN EPEN 1	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por semestre	2:4	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN EPEN 1	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN EPEN 2	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por semestre	2:3	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN EPEN 2	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN CENSO 1	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN CENSO 1	Puede ocurrir una vez por semestre	2:4	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN CENSO 1	Puede ocurrir una vez por semestre	2:4	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN CENSO 1	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN CENSO 1	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN CENSO 1	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN CENSO 2	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN CENSO 2	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN CENSO 2	Puede ocurrir una vez por semestre	2:4	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN CENSO 2	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN CENSO 2	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN CENSO 2	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN CENSO	Puede ocurrir en un mes	3:4	Alto
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN CENSO	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN CENSO	Puede ocurrir una vez por semestre	2:3	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN CENSO	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN CENSO	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN CENSO	Puede ocurrir una vez por semestre	2:4	Medio
Fallo de servicios de comunicaciones	ENVIO DE INFORMACIÓN	Puede ocurrir en un mes	3:4	Alto

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
	ENCUESTAS TEMPORALES			
Caída del sistema por agotamiento de recursos	ENVIO DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:4	Medio
Suplantación de la identidad de los usuarios	ENVIO DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:3	Medio
Abuso de los privilegios de acceso	ENVIO DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:4	Medio
Uso no previsto	ENVIO DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:4	Medio
Acceso no autorizado	ENVIO DE INFORMACIÓN ENCUESTAS TEMPORALES	Puede ocurrir una vez por semestre	2:4	Medio
Fuego	RESPALDO DE INFORMACIÓN	Puede ocurrir una vez por año o mas	1:5	Medio
Avería de origen físico o lógico	RESPALDO DE INFORMACIÓN	Puede ocurrir una vez por semestre	2:5	Alto
Degradación de los soportes de almacenamiento de la información	RESPALDO DE INFORMACIÓN	Puede ocurrir una vez por año o mas	1:5	Medio
Errores de mantenimiento y actualización de hardware	RESPALDO DE INFORMACIÓN	Puede ocurrir una vez por semestre	2:5	Alto
Ataque destructivo	RESPALDO DE INFORMACIÓN	Puede ocurrir una vez por semestre	2:5	Alto
Daños por agua	DESPACHO DE JEFATURA	Puede ocurrir una vez por año o mas	1:4	Medio
Fluctuaciones o sobrecargas eléctricas	DESPACHO DE JEFATURA	Puede ocurrir una vez por año o mas	1:3	Bajo
Fluctuaciones o sobrecargas eléctricas	DIRECTOR	Puede ocurrir una vez por año o mas	1:4	Medio
Deficiencias en la organización	DIRECTOR	Puede ocurrir una vez por año o mas	1:5	Medio

Nombre del Riesgo	Activo al que está relacionado	¿cada cuánto podría suceder?	Calificación de riesgo	Nivel de riesgo
Fuga de información	DIRECTOR	Puede ocurrir una vez por semestre	2:4	Medio
Indisponibilidad del personal	DIRECTOR	Puede ocurrir una vez por semestre	2:3	Medio
Fluctuaciones o sobrecargas eléctricas	COLABORADORES CAS	Puede ocurrir una vez por año o mas	1:3	Bajo
Deficiencias en la organización	COLABORADORES CAS	Puede ocurrir una vez por semestre	2:4	Medio
Fuga de información	COLABORADORES CAS	Puede ocurrir una vez por semestre	2:4	Medio
Indisponibilidad del personal	COLABORADORES CAS	Puede ocurrir una vez por semestre	2:4	Medio
Fluctuaciones o sobrecargas eléctricas	COLABORADORES CON LOCACIÓN DE SERVICIOS	Puede ocurrir una vez por año o mas	1:3	Bajo
Deficiencias en la organización	COLABORADORES CON LOCACIÓN DE SERVICIOS	Puede ocurrir una vez por semestre	2:4	Medio
Fuga de información	COLABORADORES CON LOCACIÓN DE SERVICIOS	Puede ocurrir una vez por semestre	2:4	Medio
Indisponibilidad del personal	COLABORADORES CON LOCACIÓN DE SERVICIOS	Puede ocurrir una vez por semestre	2:4	Medio

Se determina la siguiente matriz donde se valoriza los riesgos encontrados por cada activo:

Tabla 8

Matriz de Valoración de Riesgos

Frecuencia muy alta	0	0	0	0	0
Frecuencia alta	8	0	15	15	1
Frecuencia media	34	31	37	42	54
Frecuencia baja	1	14	27	113	24

Frecuencia muy baja	4	3	27	85	51
	Muy bajo	Bajo	Medio	Alto	Muy alto

- **Evaluación de Riesgos.**
  - ***Alto***. si el resultado de la valoración es Alto se establecen controles para detectarlos y prevenirlos.
  - ***Medio.*** si el resultado de la valoración es Medio se transfiere el riesgo a un tercero.
  - ***Bajo.*** si el resultado de la valoración es Bajo finaliza el proceso.
- **Análisis de Resultados.**
  - ***Nivel Alto.*** En primer lugar (54) se evidencia en el ingreso de la información al SIIP, así como en la consistencia de la información ingresada, así mismo en el proceso de análisis de la información y los resultados finales del IPC, IUPC, IPM; la amenaza en estos procesos se manifiestan como error involuntario del encargado del ingreso de la información al SIIP quien puede alterar accidental la información, divulgar sin autorización la información recabada, destruir esta información o alterar la información maliciosamente. Se deben establecer controles para el acceso y manejo de la información recabada a nivel de ODEI desde el proceso de recabar la información hasta su publicación final adheridos a los manuales y directivas ya existentes. En segundo lugar (42) se evidencia en los procesos de seguimiento y supervisión de las encuestas permanentes y temporales, así como en los diferentes sistemas manejados y los canales de envío de la información, amenazas como la alteración accidental de la información, destrucción de la información, difusión de software dañino,

manipulación de los sistemas utilizados sin autorización, uso no previsto de activos de información y los fallos que puedan ocurrir en el envío de la información por los diferentes canales. Para ello se deben establecer controles para el acceso de usuarios autorizados y su debida capacitación en el uso correcto de los activos informáticos, además de controles planificados de revisión y reporte del uso de la red y del internet y plan de datos. En tercer lugar (25) se evidencia en los procesos seguimiento y supervisión de las encuestas permanentes y temporales, así como en los informes de incidencias y los respaldos de información además de la importancia que tiene el director para una gestión exitosa en la ODEI Pasco, las amenazas que se pueden presentar son de destrucción de información, modificación deliberada de información, destrucción de la información, averías de origen físico o lógico, errores de mantenimiento y actualización de los activos informáticos, así como deficiencia en las organización. Para ello se deben establecer controles con respecto al tratamiento de la información en el seguimiento y supervisión de las diferentes encuestas, plantear controles para un adecuado uso de copias de respaldo.

- ***Nivel Medio.*** (113) se evidencia en los procesos de recopilación de información de las encuestas permanentes y temporales, en el uso de los activos informáticos, el envío de información, con respecto a los colaboradores CAS y contratados bajo la modalidad de ***Locación*** de Servicios; las amenazas detectadas se refieren a la ocurrencia de perdida de equipos móviles, la posibilidad de modificación deliberada de la información durante la recopilación de esta, la manipulación de equipos, la posibilidad de suplantación de la identidad, durante los envíos de información se detectaron posibilidades de caída del sistema

de transferencia por agotamiento de recursos, abuso de privilegios, accesos no autorizados, se ven deficiencias en la organización por desconocimiento de sus funciones de algunos colaboradores, también se evidencia el uso inadecuado de los equipos informáticos de algunos colaboradores. Para ello se debe solicitar a la Sede Central establecer directivas para el uso adecuado de los equipos con los cuales se recaba la información, sanciones para los colaboradores si incurren a la modificación deliberada, la manipulación no autorizada de equipos, así mismo solicitar el mejoramiento en cuanto su seguridad de los sistemas UNETE, RENAMU, SGID, SIIP, OWA, además de solicitar a la oficina correspondiente para el tratamiento de averías de origen físico y lógico en los activos informáticos, para el envío de la información solicitar controles para su envío y recepción, solicitar la capacitación la capacitación de los colaboradores antes de su incorporación. En segundo lugar (85) se evidencia en la recopilación de información, monitoreo de conexiones, ingreso de datos, realización de la consistencia, en el despacho de jefatura las amenazas detectadas se relacionan a la degradación de los soportes de almacenamiento de la información, posibles cortes de suministro, fugas de información en la utilización de los formatos utilizados en IPC, RENAMU, también se considera que pueden ocurrir daños por agua en las instalaciones de la ODEI Pasco. Para ello se debe solicitar se establezcan controles para el uso, almacenamiento y degradación de equipos utilizados en las diferentes encuestas, solicitar controles para cuando ocurra cortes de suministro eléctrico intempestivos que puedan afectar los activos informáticos, solicitar el mantenimiento constante de la infraestructura de la ODEI Pasco. En tercer lugar (51) se evidencia en las normas internas, la recopilación de la información, seguimiento y supervisión,

ingreso de datos, consistencia de esa información, en los activos informáticos, el respaldo de la información; se evidencian amenazas tales como alteración accidental de la información, la posibilidad de destrucción de la información, fallos en los servicios de comunicación y ataque destructivo, fugas de información, en cuanto a los activos informáticos se puede presentar errores de mantenimiento y actualización en el hardware por no tener un plan de mantenimiento, en cuanto a los respaldos de información puede existir degradación. Para ello se debe solicitar se establezcan controles por parte de Sede Central sobre la recopilación de información, seguimiento y supervisión, ingreso de datos, consistencia de la información, además de realizar un calendario de mantenimiento y actualización de hardware y definir procedimientos para la realización de respaldos de seguridad para la información recopilada en los diferentes equipos (tabletas).

4.1.7. Elaboración de la Declaración de aplicabilidad (SOA) en la ODEI Pasco

- **Estado actual de la Implementación.** La implementación se inició en el Proceso: Administración del Centro de Datos de la Sede Central del INEI un 2023, esta se encuentra a nivel institucional en una etapa inicial a nivel de la ODEI Pasco, esta implementación se limita solo a algunos procesos, y en relación a los requerimientos establecidos por la Norma NTP-ISO/IEC 27001:2014 se encuentran tal como lo demuestra la siguiente tabla:

Tabla 9

Requerimientos NTP-ISO/IEC 27001:2014

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios
4	**Contexto de la organización**				
4.1	**Comprensión de la organización y de su contexto**				
4.1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	**Inicial**			
4.2	**Comprensión de las necesidades y expectativas de las partes interesadas**				
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	**Inicial**			
4.2 (b)	Determinar los requerimientos y aplicaciones relevantes de seguridad de la información	**Inicial**			
4.3	**Determinación del alcance del SGSI**				
4.3	Determinar y documentar el alcance del SGSI	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
4.4	**SGSI**				
4.4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar	**Inicial**			
5	**Liderazgo**				

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios
5.1	**Liderazgo y compromiso**				
5.1	La administración debe demostrar liderazgo y compromiso por el SGSI	**Inicial**			
5.2	**Política**				
5.2	Documentar la Política de Seguridad de la Información	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
5.3	**Roles, responsabilidades y autoridades en la organización**				
5.3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	**Inicial**			
6	**Planificación**				
6.1	**Acciones para tratar los riesgos y oportunidades**				
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades	**Inexistente**			
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria - Controles Anexo A ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios
6.2	**Objetivos de seguridad de la información y planificación para su consecución**				
6.2	Establecer y documentar los planes y objetivos de la seguridad de la información	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
7	**Soporte**				
7.1	**Recursos**				
7.1	Determinar y asignar los recursos necesarios para el SGSI	**Inexistente**			
7.2	**Competencia**				
7.2	Determinar, documentar hacer disponibles las competencias necesarias	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
7.3	**Concienciación**				
7.3	Implementar un programa de concienciación de seguridad	**Inexistente**			
7.4	**Comunicación**				
7.4	Determinar las necesidades de comunicación internas y externas relacionadas al SGSI	**Inexistente**			
7.5	**Información documentada**				
7.5.1	Proveer documentación requerida por el estándar más la requerida por la organización	**Inexistente**			
7.5.2	Proveer un título, autor, formato consistente,	**Inexistente**			

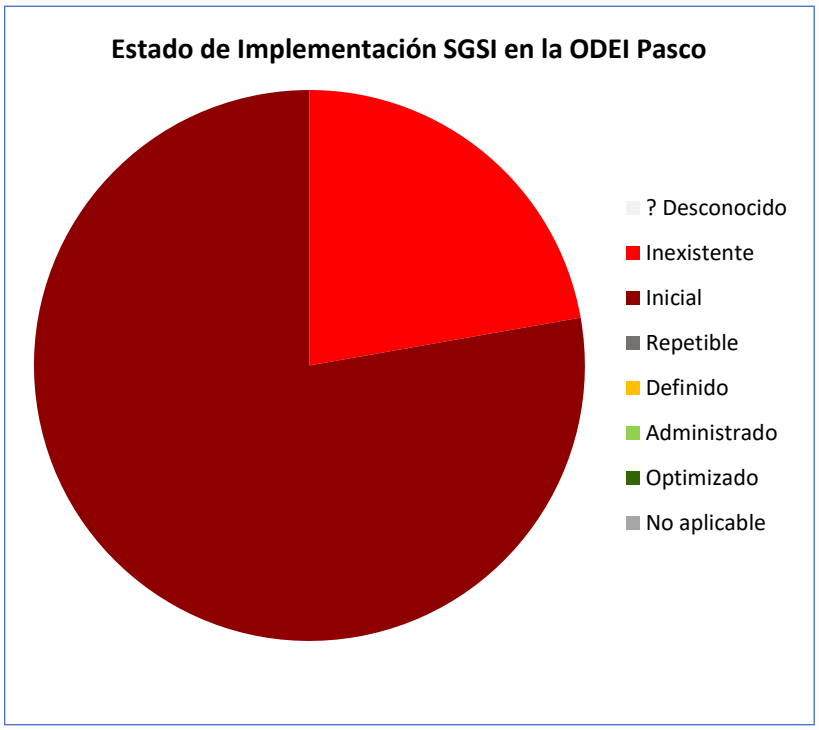
Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios
	revisión y aprobación a los documentos				
7.5.3	Mantener un control adecuado de la documentación	**Inicial**			
8	**Operación**				
8.1	**Planificación y control operacional**				
8.1	Planificar, implementar, controlar y documentar el proceso de gestión de riesgos del SGSI (Tratamiento de riesgos)	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
8.2	**Apreciación de los riesgos de seguridad de la información**				
8.2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
8.3	**Tratamiento de los riesgos de seguridad de la información**				
8.3	Implementar un plan de tratamiento de riesgos y documentar los resultados	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
9	**Evaluación del desempeño**				
9.1	**Seguimiento, medición, análisis y evaluación**				
9.1	Realizar un seguimiento, medición, análisis y evaluación del	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURID

Sección	Requerimientos ISO 27001	Estado	Recurso	Preguntas	Comentarios
	SGSI y los controles				AD DE LA INFORMACIÓN DEL INEI
9.2	**Auditoría interna**				
9.2	Planificar y realizar una auditoría interna del SGSI	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
9.3	**Revisión por la dirección**				
9.3	La administración realiza una revisión periódica del SGSI	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
10	**Mejora**				
10.1	**No conformidad y acciones correctivas**				
10.1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	**Inicial**	POL-001SGSI-INEI	Documentación obligatoria ¿Existe el documento?	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
10.2	**Mejora continua**				
10.2	Mejora continua del SGSI	**Inicial**			

Como se observa en la ODEI Pasco algunos requerimientos se encuentran en una etapa inicial alineados a la Política General de Seguridad de la Información del INEI y otros se encuentran por implementar (inexistentes) por lo que para definir una activa seguridad de los activos de información y adquirir el ISO 27001 es necesario cumplir con dichos requerimientos.

Figura 7

Estado de Implementación del SGSI en la ODEI Pasco



Nota: La figura muestra el estado de Implementación del SGSI en la Oficina Departamental de Estadística e Informática Pasco

- **Controles de Seguridad.** Para la implementación de la Norma NTP-ISO/IEC 27001:2014 se deben **implementar** controles de seguridad de la información, los cuales serán necesarios para prevenir y corregir errores que se puedan presentar y/o afectar a los activos de información.

Estos controles de seguridad permiten mitigar el impacto las vulnerabilidades según el análisis de riesgos ya realizado.

Según la Norma NTP-ISO/IEC 27001:2014 los controles contemplados son los siguientes:

Tabla 10

Controles según la norma NTP-ISO/IEC 27001:2014

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
A5	**Políticas de seguridad de la información**			
A5.1	**Directrices de gestión de la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	Inicial	POL-001SGSI-INEI	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL INEI
A5.1.2	Revisión de las políticas para la seguridad de la información	Inicial		
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Roles y responsabilidades en seguridad de la información	Inicial		
A6.1.2	Segregación de tareas	Inexistente		
A6.1.3	Contacto con las autoridades	Inexistente		
A6.1.4	Contacto con grupos de interés especial	Inexistente		
A6.1.5	Seguridad de la información en la gestión de proyectos	Inexistente		
A6.2	**Los dispositivos móviles y el teletrabajo**			
A6.2.1	Política de dispositivos móviles	Inexistente		
A6.2.2	Teletrabajo	Inexistente		
A7	**Seguridad relativa a los recursos humanos**			
A7.1	**Antes del empleo**			
A7.1.1	Investigación de antecedentes	Definido		

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
A7.1.2	Términos y condiciones del empleo	Definido		
A7.2	**Durante el empleo**			
A7.2.1	Responsabilidades de gestión	Inexistente		
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inicial		
A7.2.3	Proceso disciplinario	Inexistente		
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**			
A7.3.1	Responsabilidades ante la finalización o cambio	Inexistente		
A8	**Gestión de activos**			
A8.1	**Responsabilidad sobre los activos**			
A8.1.1	Inventario de activos	Inicial		
A8.1.2	Propiedad de los activos	Inicial		
A8.1.3	Uso aceptable de los activos	Inicial		
A8.1.4	Devolución de activos	Inexistente		
A8.2	**Clasificación de la información**			
A8.2.1	Clasificación de la información	Inexistente		
A8.2.2	Etiquetado de la información	Inexistente		
A8.2.3	Manipulado de la información	Inicial		
A8.3	**Manipulación de los soportes**			
A8.3.1	Gestión de soportes extraíbles	Inexistente		
A8.3.2	Eliminación de soportes	Inexistente		
A8.3.3	Soportes físicos en tránsito	Inexistente		
A9	**Control de acceso**			
A9.1	**Requisitos de negocio para el control de acceso**			
A9.1.1	Política de control de acceso	Inicial		
A9.1.2	Acceso a las redes y a los servicios de red	Inicial		

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
A9.2	**Gestión de acceso de usuario**			
A9.2.1	Registro y baja de usuario	Definido		
A9.2.2	Provisión de acceso de usuario	Repetible		
A9.2.3	Gestión de privilegios de acceso	Repetible		
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inicial		
A9.2.5	Revisión de los derechos de acceso de usuario	Inicial		
A9.2.6	Retirada o reasignación de los derechos de acceso	Inicial		
A9.3	**Responsabilidades del usuario**			
A9.3.1	Uso de la información secreta de autenticación	Inicial		
A9.4	**Control de acceso a sistemas y aplicaciones**			
A9.4.1	Restricción del acceso a la información	Definido		
A9.4.2	Procedimientos seguros de inicio de sesión	Repetible		
A9.4.3	Sistema de gestión de contraseñas	Repetible		
A9.4.4	Uso de utilidades con privilegios del sistema	Inicial		
A9.4.5	Control de acceso al código fuente de los programas	Inexistente		
A10	**Criptografía**			
A10.1	**Controles criptográficos**			
A10.1.1	Política de uso de los controles criptográficos	Inexistente		
A10.1.2	Gestión de claves	Inexistente		
A11	**Seguridad física y del entorno**			
A11.1	**Áreas seguras**			
A11.1.1	Perímetro de seguridad física	Definido		

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
A11.1.2	Controles físicos de entrada	Inexistente		
A11.1.3	Seguridad de oficinas, despachos y recursos	Inexistente		
A11.1.4	Protección contra las amenazas externas y ambientales	Inexistente		
A11.1.5	El trabajo en áreas seguras	Inexistente		
A11.1.6	Áreas de carga y descarga	Inexistente		
A11.2	**Seguridad de los equipos**			
A11.2.1	Emplazamiento y protección de equipos	Inexistente		
A11.2.2	Instalaciones de suministro	Administrado		
A11.2.3	Seguridad del cableado	Inicial		
A11.2.4	Mantenimiento de los equipos	Inicial		
A11.2.5	Retirada de materiales propiedad de la empresa	Inicial		
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Inexistente		
A11.2.7	Reutilización o eliminación segura de equipos	Inexistente		
A11.2.8	Equipo de usuario desatendido	Inexistente		
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Inexistente		
A12	**Seguridad de las operaciones**			
A12.1	**Procedimientos y responsabilidades operacionales**			
A12.1.1	Documentación de procedimientos operacionales	Inicial		
A12.1.2	Gestión de cambios	Inicial		
A12.1.3	Gestión de capacidades	Inicial		
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Inexistente		

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
A12.2	**Protección contra el software malicioso (malware)**			
A12.2.1	Controles contra el código malicioso	Inicial		
A12.3	**Copias de seguridad**			
A12.3.1	Copias de seguridad de la información	Inicial		
A12.4	**Registros y supervisión**			
A12.4.1	Registro de eventos	Inexistente		
A12.4.2	Protección de la información del registro	Inicial		
A12.4.3	Registros de administración y operación	Inexistente		
A12.4.4	Sincronización del reloj	Inexistente		
A12.5	**Control del software en explotación**			
A12.5.1	Instalación del software en explotación	Administrado		
A12.6	**Gestión de la vulnerabilidad técnica**			
A12.6.1	Gestión de las vulnerabilidades técnicas	Inexistente		
A12.6.2	Restricción en la instalación de software	Administrado		
A12.7	**Consideraciones sobre la auditoria de sistemas de información**			
A12.7.1	Controles de auditoría de sistemas de información	Inicial		
A13	**Seguridad de las comunicaciones**			
A13.1	**Gestión de la seguridad de las redes**			
A13.1.1	Controles de red	Inexistente		
A13.1.2	Seguridad de los servicios de red	Inexistente		
A13.1.3	Segregación en redes	Inexistente		
A13.2	**Intercambio de información**			

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
A13.2.1	Políticas y procedimientos de intercambio de información	Inicial		
A13.2.2	Acuerdos de intercambio de información	Inicial		
A13.2.3	Mensajería electrónica	Definido		
A13.2.4	Acuerdos de confidencialidad o no revelación	Inicial		
A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
A14.1	**Requisitos de seguridad en los sistemas de información**			
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Inicial		
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Inicial		
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Inicial		
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**			
A14.2.1	Política de desarrollo seguro	Inexistente		
A14.2.2	Procedimiento de control de cambios en sistemas	Inexistente		
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Inicial		
A14.2.4	Restricciones a los cambios en los paquetes de software	Definido		
A14.2.5	Principios de ingeniería de sistemas seguros	Inicial		
A14.2.6	Entorno de desarrollo seguro	Inexistente		

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
A14.2.7	Externalización del desarrollo de software	Inexistente		
A14.2.8	Pruebas funcionales de seguridad de sistemas	Inexistente		
A14.2.9	Pruebas de aceptación de sistemas	Inexistente		
A14.3	**Datos de prueba**			
A14.3.1	Protección de los datos de prueba	Inexistente		
A15	**Relación con proveedores**			
A15.1	**Seguridad en las relaciones con proveedores**			
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Repetible		
A15.1.2	Requisitos de seguridad en contratos con terceros	Inicial		
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Inexistente		
A15.2	**Gestión de la provisión de servicios del proveedor**			
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Inexistente		
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Inexistente		
A16	**Gestión de incidentes de seguridad de la información**			
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**			
A16.1.1	Responsabilidades y procedimientos	Inexistente		
A16.1.2	Notificación de los eventos de seguridad de la información	Inexistente		

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
A16.1.3	Notificación de puntos débiles de la seguridad	Inexistente		
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Inexistente		
A16.1.5	Respuesta a incidentes de seguridad de la información	Inexistente		
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inexistente		
A16.1.7	Recopilación de evidencias	Inexistente		
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**			
A17.1	**Continuidad de la seguridad de la información**			
A17.1.1	Planificación de la continuidad de la seguridad de la información	Inicial		
A17.1.2	Implementar la continuidad de la seguridad de la información	Inicial		
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Inicial		
A17.2	**Redundancias**			
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Inicial		
A18	**Cumplimiento**			
A18.1	**Cumplimiento de los requisitos legales y contractuales**			
A18.1.1	Identificación de la legislación aplicable y	Inicial		

Sección	Controles de Seguridad de la Información	Estado	Recurso	Comentarios
	de los requisitos contractuales			
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Administrado		
A18.1.3	Protección de los registros de la organización	Inicial		
A18.1.4	Protección y privacidad de la información de carácter personal	Repetible		
A18.1.5	Regulación de los controles criptográficos	Inexistente		
A18.2	**Revisiones de la seguridad de la información**			
A18.2.1	Revisión independiente de la seguridad de la información	Inicial		
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Inicial		
A18.2.3	Comprobación del cumplimiento técnico	Inexistente		

Según la tabla de controles el nivel de implementación en la ODEI Pasco es el siguiente:

- ***A5: Políticas de Seguridad.*** Se evidencia que en la ODEI Pasco se está iniciando con la definición de las políticas de seguridad, por ser parte descentralizada del INEI, pero solo en algunos aspectos alineados a la Administración del Centro de Datos de la Sede Central del INEI, quedando expuesta el manejo de los activos de información siendo fundamental implementar políticas de seguridad de información para los colaboradores en la ODEI.
- ***A6: Organización de la Seguridad de la Información.*** según la información proporcionada en la ODEI Pasco, las responsabilidades de la seguridad de la información están asignadas a una persona, no existe

segregación de tareas, ni contacto con autoridades y grupos de interés, así como no se contempla la seguridad de la información en la gestión de proyectos. No se mencionan políticas de dispositivos móviles y no existe el teletrabajo.

- ***A7: Seguridad relativa a los Recursos Humanos.*** según la información recabada existen procedimientos definidos para la contratación de personal los cuales cumplen con las normas vigentes, se evidencia además que no incluyen los términos de confidencialidad de divulgación de información en la contratación de colaboradores, en cuanto a las capacitaciones de concientización están en una etapa inicial.
- ***A8: Gestión de Activos; existe un inventario de activos.*** así como la designación del propietario del activo, mas no hay un control oportuno cuando el activo es devuelto a la ODEI Pasco. En cuanto al manejo de la información es necesario implementar estrategias que puedan evitar fugas de información. En cuanto a los medios extraíbles no existen controles definidos para su manejo.
- ***A9: Control de Acceso.*** la implementación de políticas de control de acceso a redes y servicios está definida desde la Sede Central del INEI y la gestión de accesos no se realiza bajo una política de seguridad implementada, la definición de privilegios no está implementada.
- ***A10: Criptografía.*** Con respecto a los controles criptográficos no se aplican.
- ***A11: Seguridad física y del entorno.*** se evidencia que no existe un adecuado manejo de la infraestructura tecnológica, está expuesto a polvo y cortos circuitos. Por otro lado, las instalaciones no son adecuadas ya que existe un hacinamiento, se procura que todos los equipos estén protegidos con UPS, el cableado de red y eléctrico en algunos casos se encuentran

expuestos, no existen políticas de control de puesto de trabajo despejado y pantalla limpia.

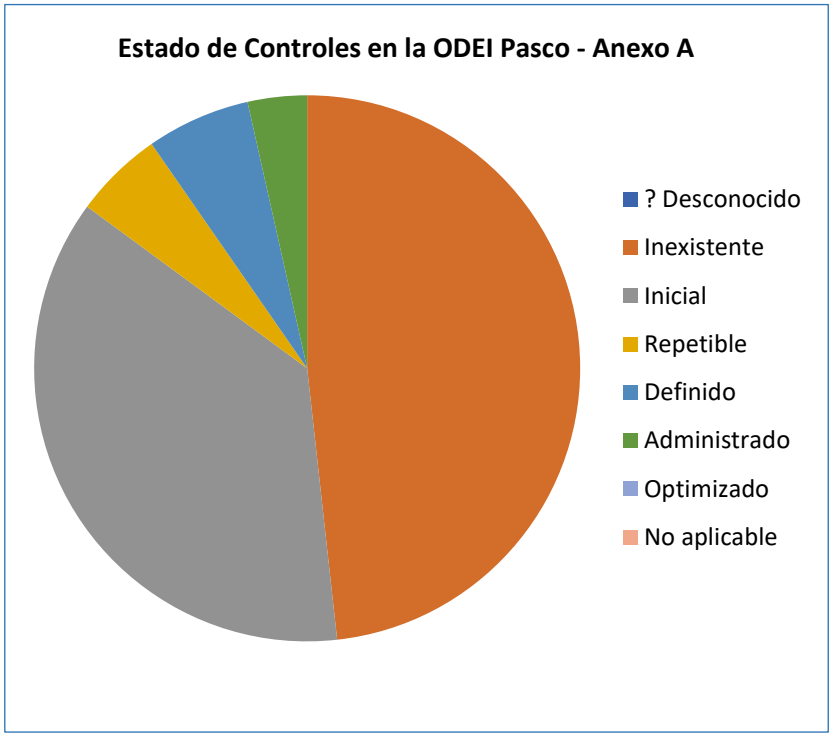
- ***A12: Seguridad de las Operaciones.*** se evidencia documentos de procedimientos operacionales para los diferentes proyectos, no se realiza desarrollo, la prueba de aplicativos se realiza en campo, por cada proyecto realizan sus copias de respaldo, no existe una política de resguardo de información, los softwares de explotación se encuentran administrados desde Sede Central, se debe de realizar capacitaciones al personal de campo y de planta sobre el software malicioso.
- ***A13: Seguridad de las Comunicaciones.*** no se realiza el monitoreo de control de red, no se realiza filtrado de correos maliciosos y acceso de contenido no autorizado. Existe un limitado control de procedimientos de intercambio de información definidos por la Sede Central.
- ***A14: Adquisición.*** desarrollo y mantenimiento de los sistemas de información; la ODEI Pasco al no tener la prerrogativa de desarrollo de sistemas de información en cuanto a la actualización de los softwares, aplicaciones utilizadas estas se actualizan de acuerdo a los cronogramas de la OTIN de Sede Central o de acuerdo a las necesidades de los proyectos existentes.
- ***A15: Relación con Proveedores.*** se limita a informar y monitorear, no se realiza gestión de provisión de servicios del proveedor.
- ***A16: Gestión de la Seguridad de la Información.*** no existen procedimientos para gestionar, evaluar incidentes con respecto a la seguridad de la información, es necesario implementar políticas con la finalidad de que los colaboradores conozcan y enfrenten eventos que con llevan a la seguridad de la información.
- ***A17: Aspectos de Seguridad de Información en la gestión de la continuidad de negocio.*** es necesario conocer sobre las consecuencias

de las amenazas donde los activos de información se ven expuestas para implementar estrategias para la continuidad de los procesos y evitar fallas en el servicio brindado por la entidad.

- ***A18: Cumplimiento.*** se tiene conocimiento sobre la normatividad que se debe cumplir para la operatividad de la entidad, en cuanto a políticas de confidencialidad se carece de un control para ello.

Figura 8

Estado de Controles en la ODEI Pasco



Nota: La figura muestra el estado de Controles en la Oficina Departamental de Estadística e Informática Pasco

- **Estado y Aplicabilidad de los Controles de Seguridad de la Información.** El estado y la **aplicabilidad** de controles de seguridad de la información en la ODEI Pasco se encuentran según el siguiente resumen:

Tabla 11

Estado de los Controles según la norma NTP-ISO/IEC 27001:2014

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de SI
? Desconocido	No ha sido verificado	**0%**	**0%**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	**22%**	**48%**
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	**78%**	**37%**
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	**0%**	**5%**
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.	**0%**	**6%**
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	**0%**	**4%**
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	**0%**	**0%**
No aplicable	A fin de certificar un SGSI, todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	**0%**	**0%**

4.1.8. Hallazgos encontrados

- Se evidencia que no existe una política definida de seguridad de la información para el ***caso*** de estudio ODEI Pasco.
- Se evidencia que falta una política para la gestión de activos. Se cuenta con un inventario de equipos informáticos, pero no se cuenta con una adecuada regulación de responsabilidades del usuario hacia el equipo a cargo.
- En el proceso de contratación de colaboradores no se evidencia una cláusula de confidencialidad de información a su vez no reciben a una adecuada capacitación sobre la seguridad e la información.
- Se evidencia una alta probabilidad que la información se vea comprometida por la alteración, divulgación por falta de control en el manejo de esta.
- No existe una política de generación de copias de respaldo para generarlo, etiquetarlo y almacenarlo.
- El uso del correo electrónico personal para realizar funciones propias del trabajo, por fallas con el correo institucional.
- Tener equipos desatendidos o con contraseñas débiles da lugar a una posible amenaza.
- No se observa un control para la gestión de incidentes, no llevar una bitácora de seguimiento da lugar a que el incidente quede sin ser atendido.

4.1.9. Recomendaciones

- Solicitar definir políticas de seguridad con el fin de ejecutar las tareas y procedimientos propios de las funciones de la ODEI Pasco.
- Solicitar definir una política de gestión de activos con el fin de realizar un mantenimiento preventivo a los equipos informáticos y crear responsabilidades a los usuarios.

- Proponer integrar la confidencialidad de los datos recopilados en las cláusulas en el contrato de los colaboradores.
- Proponer un control accesos de usuarios a los equipos informáticos definiendo responsabilidades.
- Proponer una política de tratamiento de la información en sus diferentes niveles.
- Proponer se implemente una política de creación de copias de respaldo.
- Proponer que se capacite a los colaboradores permanentes y eventuales sobre las diferentes amenazas de los softwares maliciosos, ingeniería social, phishing entre otros.
- Proponer una política para la gestión de incidentes.

4.2. Programación específica

Tabla 12

Cronograma de Actividades

MES	MES 1				MES 2				MES 3				MES 4			
ACTIVIDAD / SEMANA	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Reconocimiento general de la Oficina Departamental de Estadística Pasco																
Levantamiento de información																
Determinar los controles de seguridad de información existentes en la organización																
Recopilación de información de activos de información existentes																
Realizar la metodología MAGERIT para el análisis y evaluación de riesgos																
Realizar la Declaración de Aplicabilidad (SOA)																

	MES	MES 1				MES 2				MES 3				MES 4			
ACTIVIDAD	SEMANA	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar el informe de hallazgos encontrados																	
Definir las políticas de seguridad																	
Definir los procedimientos de seguridad																	
Definir las conclusiones y recomendaciones																	
Presentación del Informe Final																	

CONCLUSIONES

En mérito al trabajo de suficiencia profesional se llegaron a las siguientes conclusiones, donde la ODEI Pasco al igual que las Oficinas Departamentales a nivel nacional se constituyen como oficinas donde se obtienen los indicadores primarios con los cuales se obtienen estadísticas oficiales para la toma de decisiones a nivel nacional por lo que la seguridad de esta información es primordial lo cual constituye el activo de información del INEI por lo que un SGSI garantizaría la integridad, confidencialidad y disponibilidad de esta.

La mitigación de riesgos se debe realizar con políticas definidas y los controles se seguridad para cada proceso interno se deben realizar desde la toma de la información por parte del encuestador y/o entrevistador.

Para mitigar las amenazas detectadas es importante establecer un SGSI a nivel de cada ODEI, ya que con ello se garantiza la seguridad de la información que viene hacer el principal activo de la institución.

RECOMENDACIONES

Concluido el trabajo de suficiencia profesional se definen las siguientes recomendaciones; es importante el compromiso de los directivos de la institución ya que depende de ello que los funcionarios y personal se comprometa activamente en la implementación del SGSI.

En el caso de la ODEI Pasco su infraestructura física pone en riesgo los activos informáticos por ende los activos de información, por lo que se recomienda la mejora de las instalaciones para una adecuada administración de recursos. Por otro lado, es indispensable realizar jornadas de sensibilización para los colaboradores permanentes y temporales sobre las políticas de seguridad a implementarse.

Sería importante que, para la implementación del SGSI, se contratara un Auxiliar de SGSI, que coordine con la Oficial del SGSI de la sede central del INEI y se enfoque a las actividades funcionales propias del SGSI.

REFERENCIAS BIBLIOGRÁFICAS

Coelho, F. Araújo, L, Bezerra, E (2014): *Gestión de la seguridad de la información* (Escuela superior de redes – Colombia).

Diaz, M. 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. (*Tesis de grado. Universidad USMP San Martin de Porres. Facultad de Ingeniería y Arquitectura) Lima-Perú.

Espinel, R. (2017). *Proyecto de investigación estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de ti para la empresa market mix. (Tesis* de grado, Universidad Católica de Colombia). https://repository.ucatolica.edu.co/bitstream/10983/15240/1/Esp%20Auditoria%20de%20sistemas.pdf.

Gui, S. G. (2018): *Introducción a la seguridad de la información*. Uoc.edu https://openaccess.uoc.edu/bitstream/10609/142807/1/M%C3%B3dulo%201_Introducci%C3%B3n%20a%20la%20seguridad%20de%20la%20informaci%C3%B3n.pdf

Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de Investigación*. (6ta) edición. Mc Graw-Hill. México: Interamericana editores.

Izcara Palacios, S. P. (2014). *La hipótesis de la investigación*. http://scielo.sld.cu/pdf/men/v16n1/1815-7696-men-16-01-122.pdf

Jácome, C. (2019). *Diseño de una política de gestión de seguridad de la información para el área de imagenología del hospital general docente de calderón utilizando los estandares ISO 27001 e ISO 27799.* (Tesis de fin de grado, Universidad de Faculta de Arquitectura e Ingeniería). Ecuador – Quito. https://repositorio.uisek.edu.ec/bitstream/123456789/3343/1/TESIS%20MTI%20EDUARDO%20PUGA.pdf

https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/3369/cruz_fukusaki.pdf?sequence=1&isAllowed=y

MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (2024). gob.es. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Mendoza, O (2018). *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018.* (Tesis de posgrado, Universidad César Vallejo). Lima- Perú.

Normaiso27001.(2024).es. https://www.normaiso27001.es/referencias-normativas-iso-27000/#def311

Organización Internacional de Normalización/Comisión Electrotécnica Internacional. (2004): *Information technology — Security techniques — Management of information and communications technology security* (ISO/IEC 13335-1). https://www.iso.org/standard/39066.html

Organización Internacional de Normalización/Comisión Electrotécnica Internacional. (2022): *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC 27002). https://www.iso.org/es/contents/data/standard/07/56/75652.html

Organización Internacional de Normalización/Comisión Electrotécnica Internacional. (2014): *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO/IEC 27000). https://www.iso.org/standard/63411.html

Porto, J. P., & Gardey, A. (2008, junio 20). *Información*. Definición.de; Definicion.de. https://definicion.de/informacion/

Sistema de gestión de seguridad de la información. (2024). gob.pe. https://www.gob.pe/14086-sistema-de-gestion-de-seguridad-de-la-informacion

Vega Briceño, E. (2021): *Seguridad de la información*. Editorial Científica 3Ciencias. https://3ciencias.com/libros/libro/seguridad-de-la-informacion/

ANEXO

Cerro de Pasco, agosto 1 de 2024.

SEÑORES:
UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN
FACULTAD DE INGENIERIA
ESCUELA DE SISTEMAS Y COMPUTACIÓN

De mi mayor consideración:

Por la presente mencionar que el Sr. JOSE ANTONIO MENDOZA MAURICIO identificado con DNI 04068358, colaborador en la Oficina Departamental de Estadistica e Informática de Pasco (ODEI Pasco) en el presente año en el proyecto denominado Actualización Cartográfica y del Directorio de Viviendas y Establecimientos 2024 desempeñándose en el cargo de COORDINADOR DEPARTAMENTAL, ha desarrollado el **ESTUDIO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION EN LA OFICINA DEPARTAMENTAL PASCO** bajo los lineamientos de la Norma **NTP-ISO/IEC 27001:2014.**

En tal sentido remito la presente para fines correspondientes

Atentamente;

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA
Víctor Raul Huanca Remigio
DIRECTOR