UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

ESCUELA DE POSTGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS

MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI, PARA FORTALECER LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y MONITOREAR LOS ACTIVOS DE INFORMACIÓN PARA EL INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA - INEI FILIAL LAMBAYEQUE.

TESIS

PRESENTADA PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE.

AUTOR:

ING. NILTON ROGGER NIÑO MORANTE

ASESOR:

DR. GIULIANA FIORELLA LECCA ORREGO

LAMBAYEQUE – PERÚ

– 2018 –

Modelo de un Sistema de Gestión de Seguridad de Información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el instituto nacional de estadística e informática - INEI Filial Lambayeque.

Ing. Nilton Rogger Niño Morante
AUTOR

Dr. Giuliana Fiorella Lecca Orrego
ASESOR

Presentada a la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo para optar el grado de: Maestro en Ingeniería de Sistemas con Mención en Gerencia de Tecnologías de la Información y Gestión del Software.

APROBADO POR:

Dr. ARMANDO MORENO HEREDIA
PRESIDENTE

Mg. ERNESTO CELI ARÉVALO
SECRETARIO

Mg. JESSIE BRAVO JAICO
VOCAL

LAMBAYEQUE – PERÚ

– 2018 –

DEDICATORIA

A mi querido Dios por guiarme e iluminarme, dándome fuerzas para seguir adelante y no derrumbarme ante los problemas que se me presentaron, enseñándome a afrontar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A don Agustín Niño Zapata y doña Bertha Morante Valderrama, mis amados padres, quienes con esfuerzo y sacrificio supieron guiarme y apoyarme por el camino del éxito profesional, con mucho amor mi logro es para ellos.

A mis queridos hermanos Yessenia Paola y Luis Alberto, por su amistad incondicional y por estar en los momentos difíciles.

AGRADECIMIENTO

Al finalizar un trabajo tan arduo y lleno de dificultades como el desarrollo de una tesis de maestría, es inevitable que te asalte un muy humano egocentrismo que te lleva a concentrar la mayor parte del mérito en el aporte que has hecho. Sin embargo, el análisis objetivo te muestra inmediatamente que la magnitud de ese aporte hubiese sido imposible sin la participación de personas y la institución que han facilitado las cosas para que este trabajo llegue a un feliz término. Por ello, es para mí un verdadero placer utilizar este espacio para ser justo y consecuente con ellos, expresándoles mis agradecimientos.

Agradecer de manera especial y sincero al Mg. José Sámame Martínez por su apoyo y confianza en mi trabajo y su capacidad para guiar mis ideas ha sido un aporte invaluable, no solamente en el desarrollo de esta tesis, sino también en mi formación como profesional. Las ideas propias, siempre enmarcadas en su orientación y rigurosidad, han sido la clave del buen trabajo que hemos realizado juntos, el cual no se puede concebir sin su siempre oportuno apoyo. Le agradezco también el haberme facilitado siempre los medios suficientes para llevar a cabo todas las actividades propuestas durante el desarrollo de esta tesis. Muchas gracias amigo José.

Para mis mejores amigos que han compartido conmigo los “ires y venires” en el plano personal y profesional: Denis Balarezo, Ivan Quilcate Cerna, de quienes siempre he recibido apoyo y palabras de aliento y a Percy Gonzales Ñique mi estimado hermano, ya que su apoyo me permitió seguir siempre en nuevos pasos profesionales que a la vez se convirtieron en una base sólida de hábitos de trabajo con los cuales afrontar el futuro.

Y, por supuesto, el agradecimiento más profundo y sentido va para mi familia. Sin su apoyo, colaboración e inspiración habría sido imposible llevar a cabo esta dura etapa de mi vida. A mis padres, Agustín y Bertha, por su ejemplo de lucha y honestidad; a mi hermano Luis Alberto por su tenacidad y superación; ¡a mi hermana Yesenia por su paciencia, por su cariño y generosidad y a mis sobrinas hermosas: Anggely, Nahomi, Cristhel y nueva sobrina Khaleesi. ¡Por ellos y para ellos!...

Es la hora de partir, la dura y fría hora que la noche sujeta a todo horario.
(Pablo Neruda)

ÍNDICE

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

RESUMEN

Cada día la importancia de la información en las empresas va tomando más importancia. Las empresas en la actualidad pueden recolectar y clasificar la información de modo que se pueda utilizar rápida y eficientemente de forma más inteligente y a medida que se obtiene más información, se comienza a tener una visión general de las cosas y se utiliza a su favor para la toma de decisiones. Pero dicha información en el ámbito laboral está expuesto a riesgos induciendo a pérdidas en el negocio sino son controlados a tiempo y de forma adecuada.

Los conceptos relacionados a la gestión del riesgo frente a la seguridad de la información y su importancia fueron descritos en el presente trabajo; así como también la de conocer los estándares y metodologías que permiten el desarrollo del análisis de riesgo para una institución ODEI Lambayeque cuya finalidad es la protección de la información, conociendo las fortalezas y debilidades que pudiesen afectar durante todo el ciclo de vida del servicio.

Con finalidad de cambiar este panorama, presentamos la tesis de maestría denominada "Modelo de un Sistema de Gestión de Seguridad de Información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el instituto nacional de estadística e informática-INEI Filial Lambayeque", cuyo principal objetivo es proteger los activos de información. El presente trabajo hace uso del modelo PDCA y la metodología Magerit VS 3 para lograr conformar un sistema de gestión de la información, abarcando aspectos administrativos, como Dirección Ejecutiva de Difusión Estadística y Dirección Ejecutiva de Producción Estadística, basados en el estándar NTP ISO/IEC 27001:2014.

Finalmente, el aporte de este caso estudio es identificar el nivel de riesgo en que se encuentran los activos de información mediante el nivel de madurez de la seguridad implementada y sobre todo incentivar a los colaboradores a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

PALABRAS CLAVE: SGSI, NTP ISO/IEC 27001:2014, Magerit V3, PDCA

ABSTRACT

Every day the importance of information in companies is becoming more important. Companies can now collect and classify information so that it can be used quickly and more efficiently than the extent that more information can be obtained, a general overview of things is used and used in their favor for the taking of decisions. But this information in the workplace is explicitly induced by a similar situation.

The concepts related to risk management versus information security and its importance were described in the present work; as well as to know the standards and methodologies that allow the development of risk analysis for an ODEI Lambayeque institution whose purpose is the protection of information, knowing the strengths and weaknesses that could affect throughout the life cycle of the service.

In order to change this panorama, we present the master's thesis called "Model of an Information Security Management System - ISMS, to strengthen the confidentiality, integrity, availability and monitoring of information assets for the national statistical and informatics institute- INEI Filial Lambayeque ", whose main objective is to protect information assets. The present work makes use of the PDCA model and the Magerit VS 3 methodology to achieve an information management system, covering administrative aspects, such as the Executive Directorate of Statistical Diffusion and the Executive Direction of Statistical Production, based on the NTP ISO / IEC standard. 27001: 2014.

Finally, the contribution of this case study is to identify the level of risk in which information assets are found through the level of maturity of the security implemented and, above all, to encourage employees to follow the respective rules and procedures regarding the security of the information and resources.

KEYWORDS: SGSI, NTP ISO/IEC 27001:2014, Magerit V3, PDCA

INTRODUCCIÓN

En un mundo tan interconectado como el actual, el principal activo de una empresa es la información que en ella se genera y se maneja, de ahí la necesidad de protegerla y hacer extensible esa protección a los sistemas tanto físicos como tecnológicos que la administran, es por ello que para lograrlo las empresas deben reconocer la necesidad de aplicar normas, planes y acciones de carácter preventivo y reactivo en cuanto a la protección de este activo.

El caso de estudio fue aplicado en ODEI Lambayeque, es por ello que es necesario establecer normas y procedimientos con el fin de proteger los activos de información fundamentales para el éxito de la institución, dando como respuesta proponer el desarrollo de un Sistema de Gestión de Seguridad de Información o SGSI como proceso sistémico, organizado y documentado para implementar y gestionar la seguridad de la información que tanto carece la institución, dicho sistema propone mantener la confidencialidad, integridad y disponibilidad de los activos de información, es por ello que para el desarrollo del sistema se eligió el estándar NTP ISO/IEC 27001:2014 sirviendo como guía para el desarrollo del caso de estudio.

El presente proyecto se ha centrado en seis capítulos:

El primer capítulo hace una remisión al marco de referencia, en la cual se reunió los conceptos relacionados a la gestión de riesgos frente a la seguridad de la información sirviendo de base para el desarrollo de este caso de estudio.

El segundo capítulo hace referencia a la situación actual de la empresa donde se realizó la investigación, en ella se aplicaron las herramientas de análisis para determinar el estado de la institución ODEI Lambayeque.

El tercer capítulo hace referencia a los aspectos de la problemática determinando la formulación del problema, justificación y objetivos de la investigación.

El cuarto capítulo se hace referencia a los materiales y métodos, en donde se utilizaron instrumentos de recolección de datos definiendo así la hipótesis y el diseño metodológico a usar.

El quinto capítulo hace referencia a la fase de desarrollo, la metodología utilizada es propuesta por la norma seleccionada, la cual para el desarrollo del sistema se realizó bajo el uso del ciclo de Deming o PDCA y para la gestión de riesgos se utilizó la metodología propuesta MAGERIT V3.

El sexto capítulo hace referencia a las conclusiones y recomendaciones del presente caso de estudio.

CAPÍTULO I

MARCO DE REFERENCIA

1 CAPÍTULO I: MARCO DE REFERENCIA

1.1 MARCO CONCEPTUAL

1.1.1 Definiciones

1.1.1.1 Actores de la Seguridad

Los Actores responsables de la seguridad, son todas las personas que están involucradas en el manejo de los activos de información ya se almacenada de forma digital o física dentro de una institución u organización.

1.1.1.2 Vulnerabilidades

Constituye un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza. En la actualidad se contempla que hay ataques intencionados y no intencionados, mismos a los que la empresa siempre es vulnerable, en mayor o menor medida. Cuando existe una vulnerabilidad en la seguridad informática, en general ésta se considera como un defecto de diseño, en la implementación del sistema o en su funcionamiento. La primera vulnerabilidad que puede suceder es que los diseñadores del sistema no sean capaces de prever todas las amenazas que existen o que pueden existir en el futuro, y como es imposible predecir el futuro, los sistemas siempre serán vulnerables.

Otra vulnerabilidad, consecuencia de la anterior, es un mal diseño del protocolo, que en su momento parece ser lo suficientemente seguro; sin embargo, al ponerlo en práctica, se descubren ciertas debilidades que no eran tan evidentes al momento de su diseño, aun cuando se supone que los organismos de normalización tienen la capacidad y la responsabilidad para tratar de manera adecuada todo lo relacionado con la seguridad de los protocolos, su implementación, configuración y funcionamiento **(Baca, 2016, págs. 31-32)**.

1.1.1.3 Amenazas

Se entiende por amenaza una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad, afectando parte de la información y de la TI de la organización. Cuando la información, la TI o cualquier otro tipo de activo es víctima de una amenaza, éstos no se ven afectados en todas sus dimensiones ni en la misma cuantía. Por tanto, una vez determinado que una amenaza podría perjudicar a un activo, hay que estimar cuán vulnerable es dicho activo en dos sentidos: 1) degradación, que significa cuán perjudicado resultaría el activo, y todo activo dañado tiene un costo en su reparación o reposición y 2) frecuencia, que significa cada cuándo se materializa la amenaza. Luego, habrá que determinar en qué consisten las amenazas que pueden afectar a cada activo de la empresa y causar un daño considerable.

De acuerdo con la recomendación UIT-T X. 800, una amenaza de seguridad constituye una violación potencial de la seguridad. Es potencial porque existe la probabilidad de que se genere un cambio intencional, pero no autorizado, del estado del sistema. Aunque también se considera una amenaza a la seguridad cuando es posible que haya una fuga de información, por supuesto no autorizada, pero no se modifica el estado del sistema, y simplemente se extraen datos importantes, como contraseñas, con el fin de realizar movimientos bancarios, como transferencias electrónicas de dinero **(Baca, 2016, págs. 29-30)**.

1.1.1.4 Riesgos

Nombra que el nivel más simple, es el proceso de gestión de riesgos identifica y prioriza los peligros inherentes al desarrollo de un producto, sistema u organización. La gestión del riego es una parte importante de la gestión de la seguridad y define como el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no

deseado. La valoración de riesgos es el proceso que consiste en identificar los problemas antes de que aparezcan.

En la gestión de riesgos, existe un factor de incertidumbre asociado con la probabilidad de que aparezcan las amenazas, que es diferente, dependiendo de cada situación. Esto significa que la amenaza solo puede predecir dentro de ciertos límites. Además, el impacto valorado para un riesgo concreto también tiene asociado incertidumbre, debido a que el incidente no deseado puede no resultar tal y como se esperaba. Debido a la existencia de estos factores de incertidumbre, que afecta la precisión de las predicciones asociadas con ellos, la planificación y la justificación de la seguridad pueden ser muy complejas, incluso aunque se pueda determinar de forma aproximada el retorno de la inversión en seguridad (ROSI).

Un incidente no deseado presenta tres componentes: amenazas, vulnerabilidad e impacto. Las vulnerabilidades indican la debilidad del activo que puede ser explotada por una amenaza. Si ninguno de estos dos componentes está presente, puede que no se produzca un incidente de seguridad ni que aparezcan riesgos.

Los riesgos se atenúan con la implantación de **salvaguardas**, también conocida como medidas, controles o contramedidas. Las Salvaguarda pueden actuar contra la amenaza, la vulnerabilidad, el impacto o contra el propio riesgo. Sin embargo, no es factible atenuar todos los riesgos de forma completa, debido, en gran parte, al elevado coste económico y a las incertidumbres asociadas. Por tanto, siempre debe aceptarse algún riesgo residual. La presencia de una elevada incertidumbre, la aceptación del riesgo se puede hacer muy problemática debido a su naturaleza inexacta. La entidad que presenta el riesgo tiene que tener en cuenta esa incertidumbre asociada con el sistema. Las áreas de proceso de todo modelo de madurez incluyen actividades que aseguran que la organización del proveedor analice las amenazas, las vulnerabilidades, los impactos y los riesgos asociados **(Bertolín, 2008, págs. 7-8)**.

1.1.1.5 Administración de Riesgos

Habla que la administración de riesgos es preciso primero intentar una definición de riesgo. Riesgo se define como la posibilidad de que las expectativas positivas para un sistema orientado al logro de objetivos no se realicen. En esta definición se encuentran los tres elementos esenciales del riesgo, como son:

- ✓ La incertidumbre.
- ✓ Las consecuencias indeseadas para un sistema.
- ✓ El cambio en las circunstancias existentes. Si bien en algunas circunstancias el riesgo es totalmente inmanejable, por estar por completo fuera de nuestro control; es el hecho de que algo debe cambiar antes de que ocurra un desastre lo que hace posible la administración de riesgos, ya que de alguna manera es posible influenciar en aquellos factores que deben cambiar. Por ejemplo, nada podemos hacer para evitar que ocurra un terremoto, pero si podemos levantar construcciones más sólidas y seguras frente a la materialización de dicho fenómeno.

Según Peter Drucker, tratar de eliminar el riesgo en las empresas es algo inútil. El riesgo es algo inherente al hecho de comprometer recursos actuales en busca de resultados futuros. De hecho, el progreso económico se define como la habilidad de tomar riesgos. La administración de riesgos se puede definir entonces como el proceso de identificación, medida y administración de los riesgos que amenazan la existencia, los activos, las ganancias o al personal de una organización, o los servicios que ésta provee. El principal objetivo de la ciencia de la administración de riesgos debe ser el de permitirle a la organización tomar los riesgos adecuados, proveyendo el conocimiento y la comprensión de dichos riesgos, identificando los recursos y esfuerzos necesarios para alcanzar los resultados deseados, movilizando las energías necesarias para ello y midiendo los resultados contra las expectativas presupuestas; además de proveer los medios para la temprana detección y corrección de decisiones erradas o inadecuadas **(Nahum, 2016)**.

1.1.1.6 Información

Plantea que uno de los fundadores de la teoría de la información, Claude E. SHANON, un ingeniero nacido en Michigan en 1916, publicó en 1948 algunos trabajos relacionados con el tratamiento de la información, a partir del ensayo de teoremas y modelos que intentaban analizar la esencia de los procesos naturales; con las preocupaciones básicas existentes con respecto al error, su control y corrección, y con la idea de que el caos es el destino de todo y la información el elemento para descifrarlo. Aunque sus trabajos estaban dirigidos fundamentalmente a las especialidades de la telefonía y la radio, lo curioso de los resultados de sus estudios fue comprobar que la expresión matemática para la cantidad de información - llamada bit, y que se representaba por combinaciones en secuencias de ceros (0) y unos (1) - presentaba la misma forma de la ecuación del principio de entropía - estado físico y medida de desorden de un sistema, definido por la Física. Un poco después, James Watson y Francis Crick descubrieron los principios de los códigos de ADN, que forman un sistema de información a partir de la doble espiral de ADN y la forma en que trabajan los genes **(Goñi Camejo, 2000, págs. 201-202)**.

Información que, por referirse a hechos o circunstancias que otros desconocen, puede generar ventajas a quien dispone de ella. En el ámbito de los mercados de valores, información a la que se ha tenido acceso reservadamente, con ocasión del desempeño de un cargo o del ejercicio de una actividad empresarial o profesional, y que, por su relevancia para la cotización de los valores, es susceptible de ser utilizada en provecho propio o ajeno **(Real Academia Española, La 23ª edición (2014), pág. Parr 19)**.

1.1.1.7 Gestión de la Información

La finalidad de la Gestión de la información es ofrecer mecanismos que permitieran a la organización adquirir, producir y transmitir, al menor coste posible, datos e informaciones con una calidad, exactitud y actualidad suficientes para servir a los objetivos de la organización13. En términos perfectamente entendibles sería conseguir la información adecuada, para la persona que lo necesita, en el momento que lo necesita, al mejor precio posible para toma la mejor de las decisiones.

En el momento actual parece indiscutible que el éxito de la empresa no dependerá únicamente de cómo maneje sus activos materiales, sino también de la gestión de los recursos de información. La importancia de este recurso es tal que algunos autores estiman que las organizaciones deben ser consideradas como sistemas de información. Es frecuente confundir un sistema de información con la tecnología que lo soporta. Las Tecnologías de la información han supuesto una auténtica revolución en la capacidad de manejo de los recursos de información, permitiendo un rápido y eficiente proceso de adquisición, enriquecimiento y acceso a la misma, aunque nunca hay que olvidar que un Sistema de Gestión de Información va más allá de las propias herramientas utilizadas **(Morales, 2004)**.

El Sistema de Gestión de Información es el encargado de seleccionar, procesar y distribuir la información procedente de los ámbitos interno, externo y corporativo:

- ✓ Información interna. La producida en la actividad cotidiana de la institución.
- ✓ Información externa. La adquirida por la institución para disponer de información sobre los temas de su interés.
- ✓ Información corporativa o pública. La que la institución emite al exterior.

Las funciones de la Gestión Información abarcarían desde:

- ✓ Determinar las necesidades de información en correspondencia a sus funciones y actividades.
- ✓ Mejora de los canales de comunicación y acceso a la información.
- ✓ Mejora de los procesos informativos.
- ✓ Empleo eficiente de los recursos.

En este contexto, la información es considerada un recurso, un producto y un activo

- ✓ La información como activo tiene un coste y debe tener un rendimiento.
- ✓ La información como producto deberá tener unas exigencias de calidad.
- ✓ La información como activo implica que la organización se preocupe por poseerla, gestionarla y utilizarla.

1.1.1.8 Impacto

Una organización se ve afectada cuando se produce una situación que atenta contra su funcionamiento normal; estas consecuencias para la empresa reciben el nombre de impacto. Dicho de otra forma, el impacto sería el alcance producido o daño causado en caso de que una amenaza se materialice.

Dos organizaciones pueden verse afectadas en diferente medida ante la materialización de la misma amenaza si han adoptado estrategias diferentes para solucionarla. Así, el impacto del borrado del disco duro ocasionado por un virus informático será muy escaso en una empresa que realiza periódicamente copias de seguridad de la información importante, pero será bastante grave en una empresa que no lleva a cabo copias de seguridad regularmente.

Un impacto leve no afecta prácticamente al funcionamiento de la empresa y se produce en organizaciones que han identificado las amenazas y han establecido las pautas a seguir en el caso de que se materialicen. Por otro lado, un impacto grave afecta seriamente a la empresa pudiendo ocasionar su quiebra y se produce en organizaciones que no han considerado las consecuencias que supone para ellas la materialización de esa amenaza. Las empresas deben, por tanto, identificar los impactos para la organización en el caso de que las posibles amenazas se produzcan. Esta tarea es uno de los objetivos del análisis de riesgos que debe realizar toda organización (**Escrivá Gascó, Romero Serrano, & Ramada, 2017**).

1.1.1.9 Desastres

Según ISO 27001, un desastre es cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización. Por ejemplo, la caída de un servidor como consecuencia de una subida de tensión o un ataque.

Un evento de este tipo puede destruir los activos de la empresa. Tradicionalmente se planteaba únicamente la destrucción de recursos físicos, como sillas, edificios, etc. pero hoy día las organizaciones se enfrentan a una nueva forma de desastre que afecta a los recursos lógicos, que constituye uno de sus principales activos: la información.

Un desastre de este tipo podría ocasionar grandes pérdidas e incluso el cese de la actividad económica. Las organizaciones deben estar preparadas ante cualquier tipo de desastre de manera que se reduzca el impacto que pueda ocasionar. Para ello, desarrollan e implantan planes de contingencia que permiten la prevención y recuperación de desastres informáticos (**Escrivá Gascó, Romero Serrano, & Ramada, 2017**).

1.1.1.10 Activos

El activo son los bienes, derechos y otros recursos de los que dispone una empresa, pudiendo ser, por ejemplo, muebles, construcciones, equipos informáticos o derechos de cobro por servicios prestados o venta de bienes a clientes. También, se incluirían aquellos de los que se espera obtener un beneficio económico en el futuro.

El activo se divide en dos partes:

- ✓ **Activo no corriente o fijo:** en este grupo se incluyen aquellos bienes y derechos que se mantendrán en la empresa durante más de un año. No se adquieren para su venta o comercialización. Ejemplos de activos no corrientes serían la maquinaria o bienes inmuebles.
- ✓ **Activo corriente o circulante:** aquí se incluyen los bienes y derechos que permanecerán en la empresa menos de un año, es decir, se adquieren con el fin de venderlos o consumirlos a corto plazo. Un ejemplo serían las existencias.

¿Qué es un Activo de Información?

Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.

En los últimos años la información es el activo más importante que posee una organización empresarial y por eso se ha llegado al origen del término de activo de información **(ISOTools Excellence, 2015)**.

Ejemplos:

ACTIVOS DE INFORMACIÓN PURA

- ✓ **Datos digitales**
  Personales, Financieros, Legales, Investigación y desarrollo, Estratégicos, Comerciales, Correo electrónico, Contestadores automáticos, Bases de datos, Unidades lógicas, Copias de seguridad.
- ✓ **Activos tangibles**
  Personales, Financieros, Legales, Investigación y desarrollo, Estratégicos y comerciales, Correo electrónico, Otros materiales de copia de seguridad, Llaves de oficinas y Otros medios de almacenamiento.
- ✓ **Activos intangibles**
  Conocimiento, Relaciones, Secretos comerciales, Licencias, Patentes, Experiencia, Conocimientos técnicos, Imagen corporativa, Marca, Reputación comercial, Confianza de los clientes, Ventaja competitiva, Ética, Productividad.
- ✓ **Software de aplicación**
  Propietario desarrollo por la organización, Cliente, Planificación de recursos empresariales, Gestión de la información, Utilidades, Herramientas de bases de datos, Aplicaciones de comercio electrónico y Middleware.
- ✓ **Sistemas operativos**
  Servidores, Ordenadores de sobremesa, Ordenadores contrales, Dispositivos de red y Dispositivos de mano e incrustados.

ACTIVOS FÍSICOS

- ✓ **Infraestructura de TI**
  Edificios, Centros de datos, Habitaciones de equipos y servidores, Armarios de red, Oficinas, Escritorios, Cajones, Archivadores, Salas de almacenamiento de medios físicos, Cajas de seguridad, Dispositivos de identificación, Autentificación, Control de acceso al personal y Otros dispositivos de seguridad.
- ✓ **Controles de entorno de TI**
  Equipos de alarma, Supresión contra incendio, Sistemas de alimentación ininterrumpida, Alimentación de potencia, Acondicionadores, Filtros, Supresores de potencia, Deshumificadores, Refrigeradores, Alarmas de aire y Alarmas de agua.
- ✓ **Hardware de TI**
  Dispositivos de almacenamiento, Ordenadores de mesa, Estaciones de trabajo, Ordenadores portátiles, Equipos de mano, Servidores, Módems, Líneas de terminación de red, Dispositivos de comunicaciones y Equipos multifunción.
- ✓ **Activos de servicios de TI**
  Servicios de autenticación de usuario, Administración de procesos, Enlaces, Cortafuegos, Servidores proxy, Servicios de red, Servicios inalámbricos, Anti-spam, Virus, Spyware, Detección y prevención de intrusiones, Teletrabajo, Seguridad, Correo electrónico, Mensajería instantánea, Servicios web, Contratos de soporte y Mantenimiento de software.

ACTIVOS HUMANOS

- ✓ **Empleados**
  Personal y directivos, Participar los que tienen roles de gestión como altos cargos, Arquitectos de software y desarrolladores, Administradores de sistemas, Administradores de seguridad, Operadores, Abogados, Auditores, Usuarios con poder y Expertos en general.
- ✓ **Externos**
  Trabajadores temporales, Consultores externos, Asesores especialistas, Contratistas especializados, Proveedores y Socios.

1.1.2 Seguridad de la Información

Se refiere a la protección de los **activos de información** fundamentalmente para el éxito de la organización. En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo.

La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como **Crítica** (Es indispensable para la operación de la empresa), **Valiosa** (Es un activo de la empresa y muy valioso) y **Sensible** (Debe de ser conocida por las personas autorizadas) **(INTECO - Instituto de Normas Técnicas de Costa Rica, 2002)**.

1.1.2.1 Objetivos Generales de la Seguridad de la Información

Menciona que la meta final de la seguridad de la información es permitir que la organización cumpla con todos sus objetivos de negocio o misión. Los objetivos principales son los siguientes **(Bertolín, 2008, págs. 1-2)**:

- ✓ **Disponibilidad:** solo para uso autorizado. La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.
- ✓ **Integridad:** es la propiedad que se encarga de garantizar que la información no haya sido alterada por usuarios no autorizados, evitando la perdida de consistencia mientras se almacena, procesa o trasmite. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.
- ✓ **Confidencialidad:** es la propiedad que intenta que la que la información privada o secreta no se revele a individuos no autorizados. La protección de la confidencialidad de aplica a los datos almacenados durante el procesamiento, mientras se trasmiten y se encuentran en tránsito. Para muchas organizaciones, la confidencialidad se encuentra, frecuentemente, detrás de la disponibilidad y de la integridad, en términos de importancia. Para algunos sistemas y para tipos específicos de datos, como los autentica dores, la confidencialidad es de extrema importancia.

- ✓ **Confiabilidad:** es la garantía que los cuatro objetivos anteriores se han cumplido adecuadamente. Es la base de la confianza en la que las medidas de seguridad, tanto técnicas, como operacionales, funcionan tal y como se idearon para proteger el sistema y la información que procesa.

1.1.2.2 Función Y Propósito de la Seguridad de la Información

Señala que la función de seguridad de la información tradicional se concentra en la información y cómo esta deber ser protegida. Es decir, estudia sus detalles y sus medios de difusión o almacenamiento para establecer las medidas tecnológicas requeridas que permitan un acceso confiable y controlado. En esta dirección, la seguridad hace énfasis en la forma como deben hacerse las cosas para obtener el comportamiento deseado y evitar sorpresas en el futuro que impacten el nivel de confianza del usuario en el acceso a los medios donde se encuentre registrada o almacenada la información. En consecuencia, una función de seguridad de la información trata de encontrar e impartir una manera de entender la protección de los **activos de información** orientada claramente por los controles conocidos y aplicados. En este sentido, las personas reconocerán la seguridad de la información como la atención a las medidas de restricción que le permiten conocer el nivel de confiabilidad del acceso y uso de los datos y su procesamiento, haciendo de estas una rutina básica y propia que cada persona debe memorizar y aplicar. Si el objetivo de la educación es el aprendizaje, el de la seguridad son los riesgos y no los controles. Parece una herejía lo que se plantea en esta reflexión, pero no lo es; es realmente el resultado de comprender que la seguridad es una propiedad emergente de un sistema, que no viene de impartir clases sobre cómo fluye y se asegura la información, sino más bien de buscar constantemente respuestas en los inesperados comportamientos que el mismo sistema presenta, fruto de la interacción entre sus componentes. La constante es que estamos expuestos a los riesgos, se hace necesario aprender de la incertidumbre y de las “fallas de control” para comprender que en la sabiduría del error está la fuente del aseguramiento permanente de la información de las empresas. Si el secreto de la educación es el aprendizaje, entonces la inteligencia de la función de la seguridad estará en su capacidad de aprender de la dinámica de los flujos de la información en los negocios, comprender los elementos computarizados requeridos que permitan un acceso confiable y controlado. En esta dirección, la seguridad hace énfasis en la forma como deben hacerse las cosas para obtener el comportamiento deseado y evitar sorpresas en el futuro que impacten el nivel de confianza del usuario en el acceso a los medios donde se encuentre registrada o almacenada la información. En consecuencia, con lo anterior, una función de seguridad de la información planteada de esta forma trata de encontrar e impartir una manera de entender la protección de los activos de información orientada claramente por los controles conocidos y aplicados. En este sentido, las personas reconocerán la seguridad de la información como la atención a las medidas de restricción que le permiten conocer el nivel de confiabilidad del acceso y uso de los datos y su procesamiento, haciendo de estas una rutina básica y propia que cada persona debe memorizar y aplicar. Entender la función de seguridad de esta manera es cerrarle la posibilidad a la organización para descubrir en su función de negocio nuevas formas de construir confianza en el acceso y uso de la información; es negarle la posibilidad de reconocer nuevos valores y comportamientos que se pueden desarrollar para confirmar una estrategia de protección basada en las personas; es perder el potencial de acción y conocimiento de cada individuo en los procesos de negocio, para revelar las intenciones de los atacantes **(Cano Martínez, 2016, págs. 15-16).**

1.2 MARCO TEÓRICO

1.2.1 Norma NTP ISO/IEC 27001:2014

1.2.1.1 Reseña Histórica

La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de abril a junio del 2014, utilizando como antecedente a la norma ISO/IEC 27001:2013 Information Technology – Security techniques – Information security management systems – Requirements y la ISO/IEC 27001:2013/COR 1 2013 Information Technology – Security techniques – Information security management systems – Requirements.

El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos presentó a la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias -CNB-, con fecha 2014-08-19, el PNTP-ISO/IEC 27001:2014, para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2014-10-18. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN.

Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, 2ª Edición, el 01 de diciembre de 2014. Esta Norma Técnica Peruana reemplaza a la NTP-ISO/IEC 27001:2008 (revisada el 2013) y es una adopción de la norma ISO/IEC 27001:2013 y de la ISO/IEC 27001:2013/COR 1.

La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada en concordancia a las Guías Peruanas GP 001:1995 y GP 002:1995 **(Oficina Nacional de Gobierno Electrónico e Informática, 2017)**.

1.2.1.2 Norma Técnica de GSI 27001 y su uso obligatorio

En el Perú, por R.M. Nº 004-2016-PCM, publicada el 14 de enero del 2016 se aprobó el uso obligatorio de la NTP ISO/IEC 27001:2014. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2º edición en todas las entidades integrantes del Sistema Nacional de Informática **(El Peruano, 2016, pág. 2)**.

Esta Norma Técnica Peruana reemplaza a la NTP-ISO/EIC 27001:2008 (revisada el 2013) y es una adopción de la norma ISO/EIC 27001:2013 y de la ISO/EIC 27001:2013/COR 1. La Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada en concordancia con las Guías Peruanas GP 001:1995 y GP 002:1995 **(NÚÑEZ PONCE, 2016)**.

a) Objeto y Campo de Aplicación

La Norma Técnica Peruana 27001:2014 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, dentro del contexto de la organización. Incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información.

b) Implementación

Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos años para la implementación y/o adecuación la norma. Sin embargo, dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la seguridad de la información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico (ONGEI) de la Presidencia del Consejo de Ministros **(Núñez Ponce, 2016)**.

c) Certificación

Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana NTP ISO/IEC 27001:2014, lo podrán realizar de forma opcional y con recursos propios de cada entidad.

d) Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, el cual estará conformado por:

- ✓ El Titular de la entidad.
- ✓ El responsable de administración o quien haga sus veces.
- ✓ El responsable de planificación o quien haga sus veces.
- ✓ El responsable del área de informática o quien haga sus veces.
- ✓ El responsable del área legal o quien haga sus veces y
- ✓ El oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad.

e) Responsabilidad de la implementación

La responsabilidad de la implementación de la norma será del titular de cada entidad.

f) Contenido:

La Norma Técnica tiene el siguiente contenido.

Parte I: Norma NTP ISO/IEC 27001:2014.

f.1. Objeto de aplicación.

La Norma Técnica Peruana 27001:2014 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, dentro del contexto de la organización. Incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información.

f.2. Referencias Normativas.

Las referencias normativas están señaladas en la norma y son indispensables para su aplicación.

f.3. Términos y Definiciones.

Se aplican los términos y definiciones proporcionados en ISO/IEC 27000.

f.4. Contexto de la Organización.

- ✓ La organización debe determinar los aspectos externos e internos que son relevantes y que afectan su capacidad de lograr los resultados deseados.
- ✓ La organización debe comprender las necesidades de las partes interesadas.
- ✓ Finalmente debe determinar el alcance del sistema de gestión de seguridad de la información.

f.5. Liderazgo.

- ✓ La alta dirección debe demostrar liderazgo y compromiso respecto al sistema de gestión de seguridad de la información.
- ✓ La alta dirección debe establecer una política de seguridad de la información que fije objetivos y que esté disponible comunicada e informada.
- ✓ Es la organización de los roles, responsabilidades y autoridades

f.6. Planificación.

La organización debe planificar acciones para abordar riesgos y oportunidades.

f.7. Soporte.

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

f.8. Operación.

- ✓ La organización debe controlar los procesos necesarios para cumplir con los requisitos de seguridad.
- ✓ Se debe realizar una evaluación de riesgos de seguridad de la información.
- ✓ Realizar el plan de manejo de riesgos de seguridad de la información.

f.9. Evaluación de Desempeño.

Realizar el monitoreo, la medición, análisis y evaluación del desempeño de la seguridad de la información y la efectividad del sistema de gestión de seguridad de la información.

f.10. Mejoras.

La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información.

Parte II: Informe Técnico:

f.1. Antecedentes.

Es una breve reseña histórica de la norma técnica peruana.

f.2. Base Legal.

- ✓ RM N° 129-2012-PCM Implementación Obligatoria de la NTP ISO IEC/27001:2008.
- ✓ LEY N° 29664 Ley que Crea el Sistema Nacional de Gestión de Desastres (SINAGERD).
- ✓ Ley 29733, Ley de Protección de Datos Personales y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS.
- ✓ Decreto Supremo Nº 013-2003-PCM, Dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.
- ✓ Resolución Ministerial Nº 179-2004-PCM, que aprueba el uso obligatorio de la "Norma Técnica Peruana NTP-ISO/IEC 12207:2004, Tecnología de la Información, Procesos del ciclo de vida del software 1ª Edición" y moificatoria.
- ✓ R.M. Nº 004-2016-PCM, publicada el 14 de enero del 2016 se aprueba el uso obligatorio de la NTP ISO/IEC 27001:2014. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2º edición en todas las entidades integrantes del Sistema Nacional de Informática.

1.2.2 Sistema de Gestión de Seguridad de Información (SGSI)

1.2.2.1 Definición de un SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore.

La norma específica que, como cualquier otro sistema de gestión, el SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Es decir, tanto la documentación de soporte como las tareas que se realizan. Los sistemas de gestión que definen las normas ISO siempre están documentados, ya que, por un lado, es la mejor manera de formalizar normas e instrucciones y, por otro, son más fáciles de transmitir y comunicar, cosa que no sucedería si se confía en un traspaso de información verbal informal.

La norma es compatible con el resto de las normas ISO para sistemas de gestión (UNE-EN ISO 9001 y UNE-EN ISO 14001) y poseen idéntica estructura y requisitos comunes, por lo que se recomienda integrar el SGSI con el resto de los sistemas de gestión que existan en la empresa para no duplicar esfuerzos. Incluso cuando no exista un sistema de gestión formal, el amplio conocimiento actual de estos sistemas hace que las principales características de la norma sean comprensibles para la mayoría de la gente, y que para explicarla en detalle sea suficiente con incidir en las diferencias fundamentales, a saber, que con un SGSI lo que tratamos es de gestionar la seguridad de la información de nuestra organización **(Gómez & Andrés, 2012)**.

1.2.2.2 Ventajas de los SGSI

La implantación de un SGSI es importante porque permite contar con un Plan de Continuidad del Negocio cuyo objetivo de control es neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna.

1.2.2.3 Beneficios

Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

- ✓ Reducción del riesgo de pérdida, robo o corrupción de información.
- ✓ Los clientes tienen acceso a la información a través medidas de seguridad.
- ✓ Los riesgos y sus controles son continuamente revisados.
- ✓ Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- ✓ Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- ✓ Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- ✓ Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- ✓ Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- ✓ Confianza y reglas claras para las personas de la organización.
- ✓ Reducción de costes y mejora de los procesos y servicio.
- ✓ Aumento de la motivación y satisfacción del personal.
- ✓ Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

1.2.2.4 Esquema del SGSI

Imagen 1: Esquema del Sistema de Gestión de Seguridad de Información ISO 27001

1.3 ESTÁNDARES Y NORMAS PARA ASEGURAR LA INFORMACIÓN

1.3.1 ISO SERIE 27000

A semejanza de otras normas ISO, la 27000 es una serie de estándares, que incluye (o incluirá, pues algunas partes aún están en desarrollo), definiciones de vocabulario (ISO 27000), requisitos para sistemas de gestión de seguridad de la información (ISO 27001), guía de buenas prácticas en objetivos de control y controles recomendables de seguridad de la información (ISO 27002), una guía de implementación de SGSI (Sistema de Gestión en Seguridad de la Información) junto a información de uso del esquema PDCA (Plan, Do, Check, Act) [6] (ISO 27003), especificación de métricas para determinar la eficacia de SGSI (ISO 27004), una guía de técnicas de gestión de riesgo (ISO 27005), especificación de requisitos para acreditación de entidades de auditoria y certificación de SGSI (ISO 27006), una guía de auditoria de SGSI (ISO 27007), una guía de gestión de seguridad de la información para telecomunicaciones (ISO 27011), una guía de continuidad de negocio en cuanto a TIC (ISO 27031), una guía de Ciberseguridad (ISO 27032), una guía de seguridad en redes (ISO 27033), una guía de seguridad en aplicaciones (ISO 27034), y una guía de seguridad de la información en el sector sanitario (ISO 27799).ISO/IEC 27001 (**Burgos Salazar & G. Campos, 2010**).

1.3.1.1 Familias ISO 27000

A semejanza de otras familias de normas ISO, la 27000 está formada por:

- ✓ **ISO 27000:** Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido.
  - ✓ **ISO 27001**. Es la norma principal de la serie y contiene los requisitos del "***Sistema de Gestión de Seguridad de la Información***". En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2013 para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

La ISO/IEC 27001:2013, ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. La norma ISO/IEC 27.001 es un estándar que especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Especifica además los requerimientos para la implementación de controles de seguridad para las necesidades de una organización, un sector de la misma, o un proceso, según el alcance del SGSI. Establece entre otras cosas, la documentación exigida para su certificación en el caso del cumplimiento de todos los requisitos.

Sin embargo, si bien sugiere un enfoque para su cumplimiento, no establece una metodología concreta para lograr los productos y esa documentación requerida, ni especifica un flujo de trabajo (Workflow) con procesos bien definidos.

Este estándar internacional adopta también el modelo Plan-Do-Check-Act (PDCA), es decir, se basa en un ciclo de mejora continua que consiste en planificar, desarrollar, comprobar y actuar en consecuencia con lo que se haya detectado al efectuar las comprobaciones. De esta manera se conseguirá ir refinando la gestión, haciéndola más eficaz y efectiva **(Gómez & Andrés, 2012, pág. 16).**

El Objeto y campo de aplicación de la norma, como el resto de las normas aplicables a los sistemas de gestión, está pensada para que se emplee en todo tipo de organizaciones (empresas privadas y públicas, entidades sin ánimo de lucro, etc.), sin importar el tamaño o la actividad. Esta norma específica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica. Por ejemplo, uno de los principales requisitos es la realización de un análisis de riesgos con unas determinadas características de objetividad y precisión, pero no aporta indicaciones de cuál es la mejor manera de llevar a cabo dicho análisis. Puede ejecutarse con una herramienta comercial, con una aplicación diseñada expresamente para la empresa, mediante reuniones, entrevistas, tablas o cualquier otro método que se estime oportuno. Todos estos recursos servirán para cumplir la norma, siempre y cuando se observen los requisitos de objetividad del método, los resultados sean repetibles y la metodología se documente **(Gómez & Andrés, 2012, pág. 17)**.

- ✓ **ISO 27002:** Desde el 1 de Julio de 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a Seguridad de la Información. No es certificable.
- ✓ **ISO 27003:** Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.
- ✓ **ISO 27004:** Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.
- ✓ **ISO 27005:** Consistirá en una guía de técnicas para la gestión del riesgo de la Seguridad de la Información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI.
- ✓ **ISO 27006:** Especifica los requisitos para la acreditación de entidades de auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.
- ✓ **ISO 27007:** Consistirá en una guía de auditoría de un SGSI.
- ✓ **ISO 27011:** Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones.
- ✓ **ISO 27031:** Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
- ✓ **ISO 27032:** Consistirá en una guía relativa a la ciberseguridad.
- ✓ **ISO 27033:** Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.
- ✓ **ISO 27034:** Consistirá en una guía de seguridad en aplicaciones.
- ✓ **ISO 27799:** Es un estándar de gestión de seguridad de la información en el sector (**Gómez Gómez, 2010)**.

1.3.2 Modelo PDCA

El ciclo de Deming o más conocido como PDCA (Plan-Do-Check-Act, de sus siglas en inglés) es un proceso metodológico desarrollado por Shewart y Deming para abordar los proyectos de mejora sobre procesos propios, externos e internos. Hoy en día, muchas normas ISO y estándares basan sus requisitos en este ciclo de mejora.

Una novedad con respecto a la norma ISO 27001:2013, es la desaparición del ciclo PDCA como marco obligatorio para la gestión de mejora continua, indicando únicamente en su apartado 10.2 que "la organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información". No obstante, el ciclo PDCA está implícito en la propia estructura de la norma, por lo que a continuación se desarrolla este modelo de mejora continua que creemos que es necesario conocer. El modelo PDCA o "Planificar-Hacer-Verificar-Actuar", consta de un conjunto de fases que permiten establecer un modelo comparable a lo largo del tiempo, de manera que se pueda medir el grado de mejora alcanzado:

- ✓ **Plan:** En esta fase se planifica la implantación del SGSI. Se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos
- ✓ **Do:** En esta fase se implementa y pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas. Para ello debe de disponerse de procedimientos en los que se identifique claramente quién debe hacer qué tareas, asegurando la capacitación necesaria para ello.
- ✓ **Check:** En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente.
- ✓ **Act:** En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase **(Gómez Fernández & Fernández River, 2015)**.

1.3.3 MAGERIT VS 3.0

Magerit es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Publicas", creado por el Consejo Superior de Administración Electrónica (CSAE). El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España. Se elaboró Magerit porque está dirigido a los medios electrónicos, informáticos y telemáticos, ya que su uso en la actualidad es frecuente, lo cual ha dado lugar al origen de ciertos riesgos que se deben de evitar con medidas preventivas para lograr tener confianza en utilizarlos.

No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a estos riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas). La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, Magerit, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos (**Gaona Vásquez, 2013, pág. 28**).

1.3.3.1 Objetivos de Magerit

En el libro I de la publicación de Magerit versión 3 persigue los siguientes objetivos:

- ✓ **Directos**:
  - Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
  - Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
  - Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

- ✓ **Indirectos**:
  - Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.3.3.2 Metodología Magerit versión 3

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados de uso de tecnologías de la información **(Amutio Gómez, Candau, & Mañas, 2012)**.

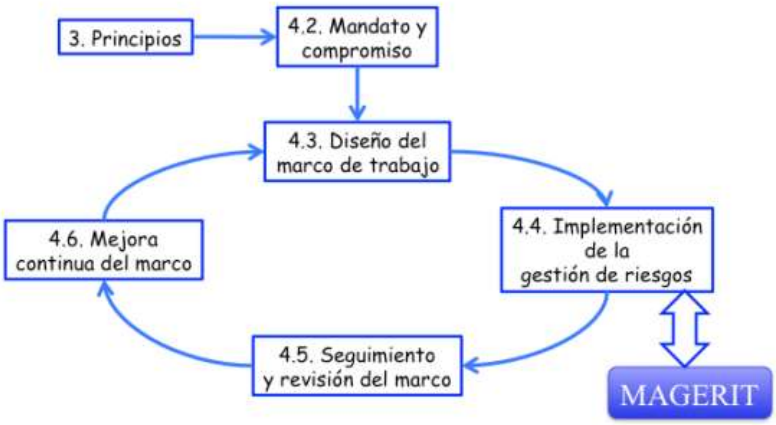


Imagen 2: ISO 31000 - Marco de trabajo para la gestión de riesgos

En las "Directrices de la OCDE para la seguridad de sistemas y redes de información-Hacia una cultura de la seguridad", que en su principio 6 dice:

6) Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo

Existen varias aproximaciones que sirven para analizar los riesgos que pueden sufrir sistemas y las tecnologías de la información y comunicación: guías formales, aproximaciones metódicas y herramientas de soporte. Todas ellas tienen como finalidad el saber cuan seguros o inseguros son los sistemas. Existen muchos elementos que hay que considerar para lograr tener buenos resultados. Es por ello que Magerit está basado sobre una aproximación metódica que no deja lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Existen varias aproximaciones que sirven para analizar los riesgos que pueden sufrir sistemas y las tecnologías de la información y comunicación: guías formales, aproximaciones metódicas y herramientas de soporte. Todas ellas tienen como finalidad el saber cuan seguros o inseguros son los sistemas. Existen muchos elementos que hay que considerar para lograr tener buenos resultados. Es por ello que Magerit está basado sobre una aproximación metódica que no deja lugar a la improvisación, ni dependa de la arbitrariedad del analista.

CAPÍTULO II

SITUACIÓN ACTUAL DE LA EMPRESA

2 CAPITULO II: SITUACIÓN ACTUAL DE LA EMPRESA

2.1 BREVE RESEÑA HISTÓRICA

2.1.1 Historia del ODEI - Lambayeque

La Oficina Departamental de Estadística E Informática (ODEI) – Lambayeque, es un órgano ejecutivo del Instituto Nacional de Estadística e Informática en el nivel departamental, que depende estructuralmente de la jefatura de INEI y funcionalmente de la oficina técnica de estadística departamental (OTED). Siendo un órgano desconcentrado del INEI, responsable de promover, orientar, desarrollar y coordinar las acciones de capacitación e investigación en los campos de la estadística e informática y áreas afines en su Sede Departamental.

Dentro de su ámbito de competencia es responsable de la gestión y resultados de las actividades estadísticas e informáticas, propias de sus funciones generales correspondiente a su jurisdicción. Para el cumplimiento de sus objetivos y funciones cuenta con autonomía técnica y de gestión, establecido en su ley de creación. Actualmente el jefe de ODEI – Lambayeque es el Ing. Daniel Cancino Castañeda, director departamental de Lambayeque.

Jefaturas

La ODEI de Lambayeque, para el cumplimiento de sus objetivos, cuenta con la siguiente estructura orgánica:

- ✓ Oficina Departamental de Estadística e Informática de Lambayeque
- ✓ Dirección Ejecutiva de Difusión Estadística
- ✓ Dirección Ejecutiva de Producción Estadística

Funciones y Objetivos

Las funciones de la ODEI – Filial Lambayeque son las contempladas, en el Decreto Supremo Nº 043-2001-PCM Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática:

- ✓ Coordinar, orientar, supervisar y evaluar, la ejecución del Plan Estadístico Departamental y Local y, Administrar el banco de Datos Departamental.
- ✓ Normar, dirigir, coordinar y supervisar las actividades estadísticas en el ámbito departamental.
- ✓ Administrar los recursos presupuestales, materiales y el personal asignado.
- ✓ Apoyar a las autoridades departamentales con información estadística oportuna, confiable y útil.
- ✓ Centralizar, publicar y difundir las estadísticas Departamentales oportunamente, de acuerdo a las normas técnicas emitidas por los órganos de Línea del INEI.

2.1.2 Base Legal

- ✓ Decreto Legislativo Nº 276, “Ley de Bases de la Carrera Administrativa y de Remuneraciones del Sector Público” y su Reglamento aprobado mediante Decreto Supremo Nº 005-90-PCM.
- ✓ Decreto Legislativo Nº 604, “Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática”.
- ✓ Decreto Supremo Nº 043-2001-PCM, que aprueba el “Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática”.
- ✓ Resolución Suprema Nº263-2001-PCM, que aprueba el “Cuadro para Asignación de Personal del INEI”.

- ✓ Resolución Jefatural Nº095-95-INAP/DNR, que aprueba la Directiva Nº 001-95- INAP/DNP sobre "Normas para la Formulación de Manuales de Organización y Funciones".
- ✓ Resolución de Contraloría Nº072-98-CG, que aprueba las "Normas Técnicas de Control Interno para el Sector Público".

  Visión y Misión.

2.1.3 Ubicación

La sede de ODEI - Lambayeque, se encuentra ubicada en el centro de la ciudad de Chiclayo, en la Av. Balta Nº 658 - 2° piso Chiclayo, a 50 m.t.s. de la Plaza de Armas.

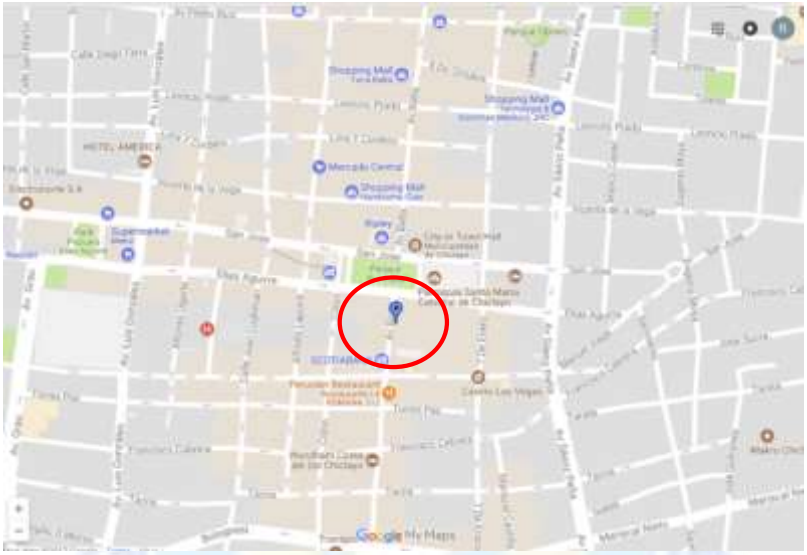


Imagen 3: Ubicación de la Institución

2.2 MARCO ESTRATÉGICO INSTITUCIONAL

2.2.1 Visión

Ser una institución líder de las estadísticas en la Región Lambayeque, utilizando tecnología de punta para el mayor beneficio de los usuarios.

2.2.2 Misión

Como oficina departamental dependiente del Instituto Nacional de Estadística e Informática, producimos y difundimos información estadística social, demográfica y económica de carácter confiable, oportuno y de calidad.

2.2.3 Valores Institucionales

Los valores tienen como principal propiedad la de construir un denominador común de comportamiento, en los cuales se sustenta el trabajo de todos y cada uno del personal de la institución. La manera de lograr estos valores dentro de la cultura institucional, es a través de la capacitación, seguimiento y evaluación e coherencia con los planes institucionales, los cuales son: Respeto, Responsabilidad, Honestidad, Trabajo en equipo, Orden, Transparencia, Ética, Imparcialidad, Compromiso, Integridad, Liderazgo.

2.2.4 Principios

- ✓ Respeto a las normas.
- ✓ Discrecionalidad.
- ✓ Rendición de cuentas.
- ✓ Actitud proactiva

2.2.5 Organigrama

El siguiente diagrama organizacional de la institución ODEI Lambayeque, se basa en el documento MOF (Manual de Organización y funciones), documento que se encuentra desactualizado ya que no contemplan las áreas de O.T. Administración y O.T de Informática.

Se sugiere la reestructuración del diagrama institucional ya que el documento no ha sido actualizado desde el 2001, año en el que fue estructurado.

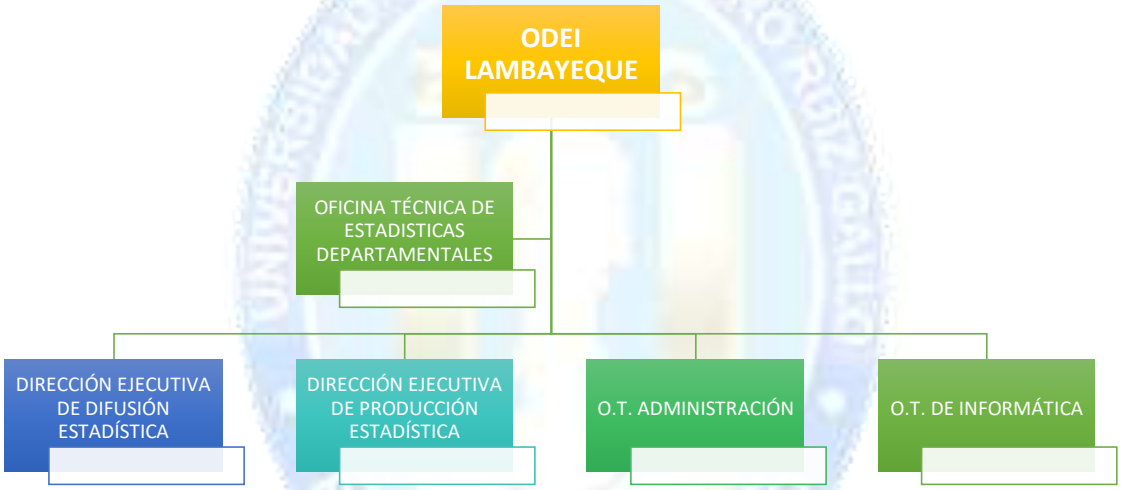


Imagen 4: Organigrama de ODEI Lambayeque

2.3 PROCESOS

Se identifica los procesos de toda institución, identificando primero los procesos más importantes con los que cuenta la institución para luego poder identificar los procesos más relevantes y así poder delimitar más adelante el alcance del Sistema de Gestión de Seguridad de la Información en base a ellos.

(Lefcovich, 2009) define que un proceso es un conjunto de actividades o tareas lógicas relacionadas y secuenciales que convierte unos factores iniciales (inputs) en bienes o servicios deseados (outputs), añadiendo un valor a los mismos dentro del negocio; por lo tanto, toman una entrada y le agregan valor para producir una salida.

Los procesos de la institución tienen que responden ante la dirección departamental, los cuales reciben como salida un servicio. Se realizó el proceso de levantamiento de la información para proceder a identificar los procesos "CORE de Negocio", procesos de Soporte y Procesos Operativos.

A continuación, se describirán los principales procesos que soportan las distintas áreas de la institución ODEI – Filial Lambayeque.

Imagen 5: Mapa de Procesos Nivel I

2.3.1 Procesos CORE

(Cordova Tobon, 2008) Destinados a establecer y controlar las metas de la empresa. Son los que proporcionan directrices a los demás procesos, es decir, indican cómo se deben realizar para que se pueda lograr la visión de la empresa. Son conocidos también como procesos visionarios y son liderados por la alta dirección. También llamado "Core Business" es la razón de ser de la compañía, aquello por lo cual se crea y en lo que se va a generar el máximo valor añadido. El concepto de procesos CORE pasa por analizar de forma sistemática las actividades de la empresa y ver cuál es la aportación de valor que estas tienen. En un entorno cada vez más competitivo las empresas tratan de buscar elementos diferenciadores de su competencia y desarrollar aquellas áreas que son el núcleo o la razón de ser de la empresa.

- ✓ **Gestión del IPC (Índice de Precios al Consumidor)**

El Índice de Precios al Consumidor (IPC) es un indicador que registra los precios de los productos de una canasta familiar, el ODEI Lambayeque genera el indicador macroeconómico y es realizado mensualmente.

El proceso comienza cuando se selecciona una muestra de productos (ejemplo 1500 productos utilizados) y el personal encargado sale a diario a investigar los precios de los productos que pertenecen a una canasta familiar en las diferentes empresas del departamento de Lambayeque (bodegas, farmacias, supermercados, mercados) y recopilar los precios de los productos, una vez recopilada toda esta información y tomando como precio el "Año Base 2009" se realiza la comparación para determinar la inflación. Una vez obtenido se procesa la información y se ingresa al sistema gubernamental denominado "SIIE (Sistema de Información de Inflación Estadística". Para finalizar se publica un boletín mensual y se informa a la central del INEI en lima donde concentra toda la información de todas las oficinas departamentales restantes.

- ✓ **Gestión del Centro Documentario**

El centro de documentación del ODEI Lambayeque se encarga de resguardar, controlar, gestiona y difundir la documentación que genera la institución. Su objetivo principal es la explosión documental por parte de los usuarios que solicitan la información por ejemplo personas profesionales, universitarios, estudiantes, investigadores y público en general, es decir tiene como finalidad servir de referencia y ayuda a los investigadores.

El Proceso comienza cuando los lectores (personas jurídicas o naturales) se acercan al área y el encargado realiza la difusión de los documentos a cargo que son prestados al lector. Al finalizar el mes se realiza un reporte donde se informa cuántos usuarios han ingresado a la biblioteca (Profesionales, Universitarios, Alumnos, Investigadores) y realizan el marketing para la venta de los documentos si son solicitados (El pago para la adquisición del informe se realiza en el área de Administración).

- ✓ **Gestión del Compendio Estadístico del Departamento**

Este proceso se origina en el área de "Dirección Ejecutiva de Producción Estadística" el cual maneja información básica sectorial y el cual tiene una duración entre 5 a 6 meses para generarlo.

El proceso tiene una periodicidad anual y se origina cuando el área mencionada genera los formatos para ser completados con información administrativa por los diferentes sectores del departamento del Lambayeque tales como sector del Medio Ambiente, Población y Demografía, Educación y Cultura, Salud, Vivienda, Trabajo, Interior, Justicia, Desarrollo Social, Cuentas Departamentales, Agrícola, Turismo, Financiero y Finanzas Públicas, a continuación el área recopila toda la información completada en los formatos (física o email) e inicia el proceso de validación el cual consiste en que los formatos sean completados adecuadamente según sus normas establecidas, una vez completado este paso, los datos obtenidos de los diferentes sectores pasan a ser digitalizados y ser tabulados para ser presentados como información estadística actualizada y detallada, dicha información contiene cuadros y gráficos estadísticos y su cobertura está referida al ámbito geográfico del departamento de Lambayeque. También, incluye series históricas de las variables más importantes que contribuirán al estudio y mejor comprensión de la realidad departamental en el mediano y largo plazo.

Toda la información es consolidad en un informe llamado "Compendio Estadístico del Departamento de Lambayeque" que será editado como un libro e impreso para la posterior venta al público en el centro documentario.

Para finalizar, los resultados del informe del departamento de Lambayeque se son enviados a la central del INEI, a través de los siguientes productos: base de datos, sistemas de información y publicaciones.

- ✓ **Gestión de la Evolución de las Actividades de Producción**

Este proceso se inicia en el área de "Dirección Ejecutiva de Producción Estadística" el cual maneja análisis de los sectores económicos es decir de aquellos sectores que requieren producción y para su generación tiene una duración de 2 semanas y se nos informa sobre la producción del departamento del Lambayeque mostrando la evolución de la actividad productiva y sectorial a corto plazo.

El proceso tiene una periodicidad mensual y normalmente viene ligado al proceso del "Compendio Estadístico del Departamento", una vez obtenido la información de los sectores productivos tales como Sector Agropecuario, Sector Pesca, Sector Minería e Hidrocarburos, Sector Manufactura, Sector Electricidad, Gas y Agua, Sector Construcción, Sector Comercio, Sector Transporte, Almacenamiento y Mensajería, Alojamiento y Restaurantes, Telecomunicaciones y Otros Servicios de Información, Sector Financiero y Seguros, Servicios Prestados a Empresas, Administración Pública se digitan los datos y se determina en función al comportamiento de un subconjunto de variables seleccionadas en cada rama de actividad económica, cuantificándolas a través de cuadros y gráficos estadísticos informándonos sobre evolución de la producción sectorial, dicho informe está dirigido a los principales agentes productivos del sector del departamento de Lambayeque. Toda la información es consolidad en un informe llamado "Evolución de las Actividades de Producción del Departamento de Lambayeque" que será editado como un libro e impreso para la posterior venta al público en el centro documentario.

Para finalizar, los resultados del informe del departamento de Lambayeque se son enviados a la central del INEI, a través de los siguientes productos: base de datos, sistemas de información y publicaciones.

- ✓ **Gestión del Registro Nacional de Municipalidades**

Se crea mediante Ley Nº 27563 a cargo del Instituto Nacional de Estadística e Informática (INEI), con el objetivo de integrar y disponer de información estadística de las Municipalidades Provinciales y Distritales, así como de las Municipalidades de Centros Poblados identificadas en el departamento de Lambayeque, a fin de generar indicadores municipales que sirvan de apoyo a la gestión regional y local para la planificación y la adecuada toma de decisiones.

El método recolección de la información es por auto- diligenciamiento, es decir, el alcalde o el funcionario municipal designado es responsable del diligenciamiento del formulario y la veracidad de los datos. Para el relevamiento de la información se utiliza dos tipos de formularios; el Formulario 01 en formato impreso y electrónico dirigido a las Municipalidades Provinciales y Distritales, y el Formulario 02 en formato impreso para las Municipalidades de Centros Poblados del departamento de Lambayeque.

Las principales variables investigadas en el RENAMU están referidas a la infraestructura municipal, recursos humanos, planificación municipal, licencias de funcionamiento y edificación, saneamiento ambiental y salubridad, educación y cultura, salud, programas sociales, seguridad ciudadana, defensa civil, promoción del desarrollo económico local, conservación del ambiente, participación vecinal, infraestructura de comunicación, alumbrado público, agua potable y alcantarillado.

Los resultados del RENAMU del departamento de Lambayeque se difunden en la página Web del INEI, a través de los siguientes productos: base de datos, sistemas de información y publicaciones.

2.3.2 Procesos Operativos

Son aquellos que impactan directamente sobre la satisfacción del cliente o usuarios y cualquier otro aspecto de la misión de la organización. Son procesos operativos típicos como los de venta, producción y servicio post- venta. También se les conoce como procesos misionales porque son los sustentan la razón de ser del negocio **(Cordova Tobon, 2008).**

✓ **Gestión de Censos y Encuestas**

La diferencia entre el censo y encuesta es que el censo es realizado a nivel nacional mientras que la encuesta es realiza a nivel departamental. Ambos documentos son elaborados en el área de Dirección y Gerencia Censal de la central de INEI Lima, el cual se desarrollan a través del planeamiento, programación, formulación de la base legales y establecimiento de las organizaciones funcionales censales, una vez finalizada todas las tareas mencionadas, son aprobadas mediante los documentos técnicos básicos del censo que son: el plan directriz, el programa censal, el cuestionario y la cédula censal. Como lo mencionamos, todas estas actividades son realizadas en el departamento de INEI – Lima, las ODEI[1]s de los departamentos son solamente ejecutoras de los censos y encuestas que son programadas en cada departamento a través del documento Plan Operativo Institucional – POI.

Para ambos documentos, las solicitudes para participar en los proyectos se inician inscribiéndose en la página web del INEI y el área de recursos de lima procesa toda la información de los postulantes y genera la relación de los contratados para las encuestas o censos, dichos contratos son gestionados por el área de administración. Los encuestadores realizan su labor y centran la información en ODEI del departamento de Lambayeque donde será procesada para generar su reporte y el informe final será enviado a LIMA al área de "Dirección de Censos y Encuestas"

2.3.3 Procesos de Soporte

Son procesos que no están ligados directamente a la misión de la organización, pero resultan necesarios para que los procesos CORE y Operativos puedan cumplir sus objetivos. Son procesos transversales a toda la organización. De alguna manera los procesos estratégicos son procesos de soporte, pues deben estar igualmente apoyando que los procesos CORE se diseñen y realicen para satisfacer el mercado objetivo y responder a las estrategias de diferenciación o de valor agregado **(Cordova Tobon, 2008).**

✓ **Gestión Administrativa**

Gestionada por el área de Oficina Técnica de Administración, la mencionada área no se encuentra contemplada dentro del documento MOF, este proceso inicia con la recopilación y generación de informes sobre los recursos humanos, planilla y recaudación y finaliza cuando toda información recopilada es reportada a la Oficina general de administración que se encuentra en el INEI Lima.

✓ **Gestión de Centro de Computo**

Existen 4 procesos que en esta área se cumplen en la mayoría de las empresas, las cuales son la planificación, el desarrollo, soporte a usuarios y compras y contratación. El área de cómputo de ODEI Lambayeque solo cuanta con el proceso de soporte de TI y los procesos restantes se realizan en la Central del INEI.

Dentro de lo que corresponde a soporte de TI, cuando un usuario tiene un problema con alguna aplicación, equipo, entre otros, o simplemente desea algo adicional, que puede ser un acceso, un cambio de equipo, entre otros, debe realizar un requerimiento informal y es el jefe de O.T. de informática quien se encarga de atender el pedido, recoger la información, solicitar la autorización respectiva y remitir la atención a la unidad que corresponde. Una vez realizada la atención, se encarga de informarle al usuario y se le pide su conformidad. Si no hay problemas, se procede a cerrar el requerimiento. En caso el usuario detecte algún problema en la atención, le informa a encargado, quienes reanuda la solicitud y la vuelven a remitir a la unidad respectiva para su atención.

[1] ODEI = Oficina Departamental de Estadística e Informática

2.4 ACTIVOS

Un activo es cualquier valor para la organización o institución que requiera ser protegido, es decir, estos activos deberán ser aquéllos que estén relacionados con el ciclo de vida de los datos relevantes previamente identificado y sus distintos tratamientos. Para realizar la identificación y ponderar con suficiente nivel de detalle los activos de información en el área de "***Dirección Ejecutiva de Producción Estadística" y "Dirección Ejecutiva de Difusión Estadística"*** de ODEI Lambayeque, dicha recopilación permitirá hacer la valoración del riesgo. Se pueden identificar dos tipos de activos:

- ✓ Los activos primarios: corresponden a la esencia de la institución
  - Información de los procesos y actividades principales.
- ✓ Los activos de apoyo: en los cuales residen los activos de información, como son:
  - Hardware
  - Software
  - Redes y telecomunicaciones
  - Personal
  - Otros

2.4.1 Identificación de los Activos Principales

Para describir el alcance de la investigación de modo más exacto, se identificarán los activos primarios que serán objetos de estudio, dichos activos se refieren a los procesos, actividades del negocio e información. Los activos primarios identificados son los procesos e información centrales que pertenecen a las áreas de "***Dirección Ejecutiva de Producción Estadística" y*** "***Dirección Ejecutiva de Difusión Estadística",*** del instituto, dichos activos en las áreas mencionadas serán los más apropiado para diseñar las políticas de seguridad de la información.

Los activos primarios son de dos tipos:

- ✓ **Procesos y actividades del negocio.**
  Gestión del Compendio Estadístico del Departamento
  Gestión de la Evolución de las Actividades de Producción
  Gestión de IPC
  Gestión del Registro Nacional de Municipalidades
- ✓ **Información**
  - Información contenida en los contenedores de datos tantos físicos como virtuales pertenecientes a las áreas en mención.
  - Información contenida en sistemas gubernamentales externos.
  - Información Confidencial.
    - Información protegida por el secreto tecnológico que están regulados, unos por el inciso 5 del artículo 2 de la Constitución, y los demás por la legislación pertinente
    - Información referida a los datos de los diferentes sectores de la provincia del departamento de Lambayeque cuya publicidad constituya una invasión a la confidencialidad.

2.4.2 Identificación de los Activos de Apoyo

A continuación, se listarán los activos de apoyo que fueron identificados en la institución ODEI Lambayeque. Es una de las tareas indispensables debido a que en estos activos es donde residen los activos principales de la información, y es en estos activos donde identificaremos sus vulnerabilidades que son explotables por amenazas que tienen como objetivo desactivar los activos primarios.

✓ **HARDWARE**

- Servidores

MODELO	DATA CENTER
HP	1
GENERAL	**1**

- PC escritorio

MODELO	ADMINISTRATIVO	ALMACEN	ALUMNOS	GENERAL
DELL Optiplex 7010	18	4		22
DELL Optiplex 745	8	5		13
DELL OPTIPLEX 746		1		1
DELL OPTIPLEX 747		1		1
DELL OPTIPLEX 9020		1	30	31
GENERAL	**26**	**11**	**30**	**68**

- PC portátil

MODELO	CANTIDAD
DELL E6440	10

- Equipos multifuncionales

EQUIPO	CANTIDAD
Impresoras	6
Proyectores	10
Cámaras de Seguridad	3

- Soporte de Información

EQUIPO	CANTIDAD
Discos Duros Externos	2
DVDs	Variables

- Fuentes de energía ininterrumpida

  No cuenta con UPC

- Equipo de Aire Acondicionado

EQUIPO	CANTIDAD
Aire Acondicionado	2

- Otros Medios

  Material impreso

✓ **SOFTWARE**

TIPO	MODELO	GENERAL
Software de Sistema	Microsoft Windows 7	21
	Microsoft Windows 8.1	31
	Microsoft Windows 8.2	1
	Microsoft Windows XP	14
Software de Aplicación	Microsoft Office Hogar y Empresas 2013	67
	IBM SPSS 22	5
	Sistema IPC(Índice de Precio Consumidor)	1
	Sistema de Control de Encomienda	1
	Página Web de la Institución (Lima)	1
Software de Utilidad	Kaspersky Antivirus	30
	ESET NOD32 antivirus	37

- Redes y telecomunicaciones

EQUIPO	CANTIDAD
Router	1
HUB	1
Switch	4

- Personal

RESPONSABLES DE LA TOMA DE DECISIONES
Jefatura de la Oficina Departamental de Estadística e Informática de Lambayeque. Jefatura de la Dirección Ejecutiva de Producción Estadística. Jefatura de la Dirección Ejecutiva de Difusión Estadística.
PERSONAL DE OPERACIONES Y MANTENIMIENTO
02 trabajadores que realizan las operaciones de tecnología de la información y comunicación, asignándoles todos los derechos de operaciones y mantenimiento.
USUARIO
Personal que se le asignas derechos especiales de acceso al sistema de información para realizar sus tareas cotidianas.

- Otros

SERVICIOS ESENCIALES
Todos los servicios requeridos para que opere el personal de la institución: - Los servicios de Internet y telecomunicaciones son proveídos por Movistar. - Electro Norte ENSA S.A suministra la energía eléctrica. - EPSEL S.A suministra de agua.

2.5 APLICACIÓN DE LA ENCUESTA EN LA INSTITUCIÓN

Esta fase de la investigación consistió en el desarrollo y administración de una encuesta como instrumento para recopilar información de las personas identificadas como fuentes de consulta para lograr los objetivos del estudio. Para ello se diseñó una lista formal de preguntas a modo de cuestionario, ya que es técnica más comúnmente utilizado en la investigación de gestión y es ideal para proporcionar información cuantificada. El uso de cuestionario ofreció transparencia de cómo se recogido y analizado los datos, además, ofrece la posibilidad de que otros utilicen los mismos datos, se amplié la investigación y puede proporcionar interpretaciones alternativas.

Dichas preguntas fueron divididas en 4 dimensiones:

- ✓ Cultura Organizacional
- ✓ Gestión de Recursos Humanos
- ✓ Seguridad Física y Ambiental de la Organización
- ✓ Control de Accesos
- ✓ Gestión de Continuidad del Negocio

Población

En primer lugar, se determinará cual será el marco muestra y la unidad de análisis, para luego proceder a delimitar la población que será estudiada y sobre la cual se pretende generalizar los resultados; para ello, se tomará como referencia (marco muestral) el Cuadro de Personal de planta del Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque.

En base a dicha información se ha determinado:

Universo: el personal que trabaja con la ODEI Lambayeque; Dicho personal labora en las diferentes áreas administrativas del Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque.

Informante: Los usuarios en las diferentes dependencias/ áreas del Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque que emplean para su trabajo los sistemas locales.

2.6 ENCUESTA DIRIGIDA A LOS COLABORADORES

CULTURA ORGANIZACIONAL

- 1. ¿Existe procedimientos de seguridad de la información que se manipula en su área?
- 2. ¿Cree que al existir relaciones amistosas con el personal técnico de sistemas afectaría la seguridad de los activos de información que se maneja en su área?
- 3. ¿Cree usted, que el entorno laboral es el adecuado en cuanto a seguridad de los activos de información se refiere?
- 4. ¿Considera que su personal tiene un compromiso ético con las actividades ligadas a la protección y seguridad de los datos manipulados en su área?
- 5. ¿Cree usted que se debe realiza frecuentemente copias de seguridad de la información relevante para el área, porque?

RECURSOS HUMANOS

- 6. ¿El personal de su área tiene conocimiento de la importancia de la seguridad los datos que se manipula ahí?
- 7. ¿Su personal cuenta con un plan de capacitación sobre seguridad de la información?
- 8. ¿Su personal ha recibido una capacitación por parte del área informática sobre cómo proteger sus la información (Física y Virtual)?

SEGURIDAD FÍSICA Y AMBIENTAL

- 9. ¿Al ocurrir un robo que ocasione pérdida de la información lo reportaría inmediatamente al área correspondiente?
- 10. ¿Qué medida utiliza más frecuente para respaldar sus datos?
- 11. ¿Cree que los datos de su área son importantes y se debe tomar en cuenta las medidas adecuadas para su protección?
- 12. ¿Si un virus informático afecta los datos de su área que tanto retrasaría el trabajo de su personal?

CONTROL DE ACCESOS

- 13. ¿Considera que la configuración de la red de la institución es la adecuada para brindar seguridad a los datos que se manipulan en el área Dirección Ejecutiva de Producción Estadística?
- 14. ¿Considera que su personal está capacitado para entrar a los sistemas en red de una forma segura y eficaz?
- 15. Como medida de prevención ¿con que frecuencia cambia las contraseñas de acceso a los sistema que manipula?
- 16. ¿Comparte su computador o sus contraseñas al sistema con otras personas de la institución?
- 17. ¿Al navegar por internet, que precauciones toma para protegerse de virus y otros ataques?

SEGURIDAD EN OPERACIONES

- 18. ¿Tengo suficientes habilidades para restringirle a su personal guardar la información en los diferentes dispositivos externos (archivos, correos electrónicos, en la nube, etc.) de forma adecuada?
- 19. ¿Al utilizar el correo electrónico tiene conocimiento sobre los peligros de acceder a email como los Pishing, webs falsas, ingeniería social, etc.?
- 20. ¿Qué medidas cree que son las más seguras para guardar la información crítica que en su área se maneja?

DIMENSIONES	INDICADORES	VARIABLES
CULTURA ORGANIZACIONAL	✓ **I1:** Liderazgo y compromiso de la alta dirección sobre seguridad de la información.	✓ **V1:** La cultura organizacional contribuye efectivamente a la aplicación de SGSI
RECURSOS HUMANOS	✓ **I2:** Nivel de concientización de seguridad de información. ✓ **I3:** Numero de capacitaciones sobre seguridad de la información.	✓ **V2:** Los Recursos Humanos deben tener un buen nivel capacitación y de concientización para la implementación de SGSI.
SEGURIDAD FÍSICA Y AMBIENTAL	✓ **I4:** Controles identificados de seguridad de la información	✓ **V3:** Identificar controles de seguridad física y ambiental para resguardar la información(equipos e infraestructura de la institución).
CONTROL DE ACCESOS	✓ **I5:** Controles de acceso para la seguridad de la información.	✓ **V4:** Establecimientos de Controles de acceso para el resguardo de la seguridad de la información.
SEGURIDAD EN OPERACIONES	✓ **I6:** Identificaciones de activos críticos ✓ **I7:** Diseño de proyectos de seguridad de la información.	✓ **V5:** Identificación y salvaguardar los activos críticos para la continuidad de la institución

2.7 PROCESAMIENTO E INTERPRETACIÓN DE LOS DATOS.

2.7.1 Cultura Organizacional

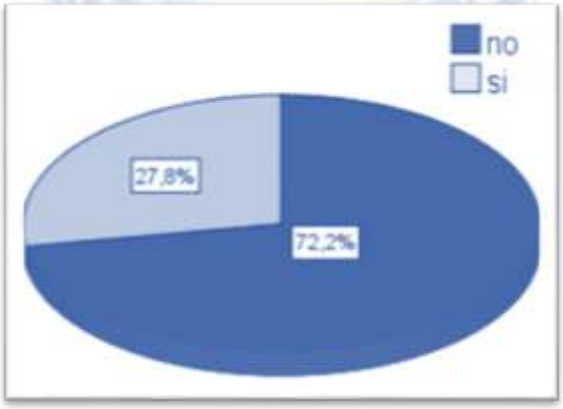
Pregunta 1: ¿Existe procedimientos de seguridad de la información que se manipula en su área?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	16	44,4	44,4	44,4
	si	20	55,6	55,6	100,0
	Total	36	100,0	100,0	

Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 55.6% del personal administrativo que respondieron que existe procedimiento de seguridad de la información que se manipula en su área y el 44.4% respondieron que no existe procedimientos de seguridad de la información que se manipula en su área.

Pregunta 02: ¿Cree que al existir relaciones amistosas con el personal técnico de sistemas afectaría la seguridad de los activos de información que se maneja en su área?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	26	72,2	72,2	72,2
	si	10	27,8	27,8	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 72.2% del personal administrativo que respondieron que no existe relaciones amistosas con el personal técnico de sistemas que afectaría la seguridad de los activos de información que se maneja en su área y el 27.8% respondieron que existe relaciones amistosas con el personal técnico de sistemas que afectaría la seguridad de los activos de información que se maneja en su área.

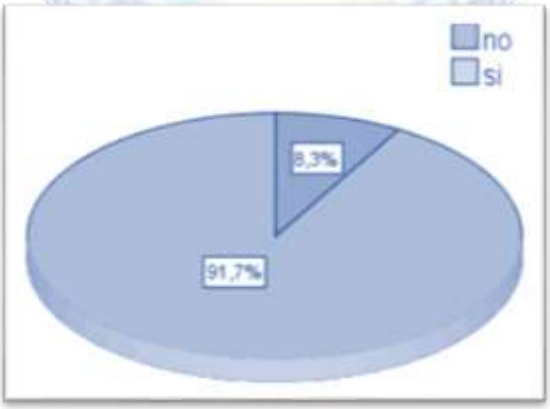
Pregunta 03: ¿Cree usted, que el entorno laboral es el adecuado en cuanto a seguridad de los activos de información se refiere?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	14	38,9	38,9	38,9
	si	22	61,1	61,1	100,0
	Total	36	100,0	100,0	

Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 61.1% del personal administrativo respondieron que el entorno laboral es el adecuado en cuanto a seguridad de los activos de información y el 38.9% respondieron que el entorno laboral no es el adecuado en cuanto a seguridad de los activos de información.

Pregunta 04: ¿Considera que su personal tiene un compromiso ético con las actividades ligadas a la protección y seguridad de los datos manipulados en su área?

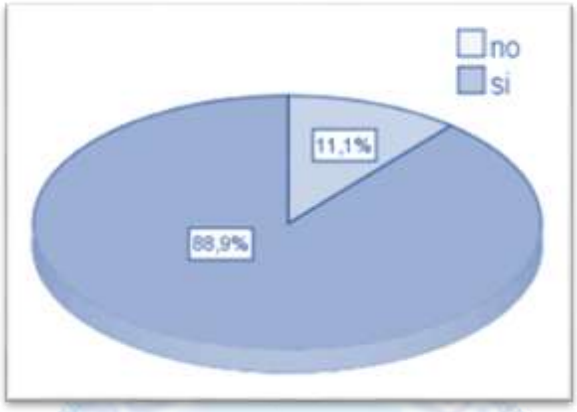
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	3	8,3	8,3	8,3
	si	33	91,7	91,7	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 91.7% del personal administrativo respondieron que su personal tiene un compromiso ético con las actividades ligadas a la protección y seguridad de los datos manipulados en su área y el 8.3% respondieron que su personal no tiene un compromiso ético con las actividades ligadas a la protección y seguridad de los datos manipulados en su área.

Pregunta 05: ¿Cree usted que se debe realiza frecuentemente copias de seguridad de la información relevante para el área?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	4	11,1	11,1	11,1
	si	32	88,9	88,9	100,0
	Total	36	100,0	100,0	

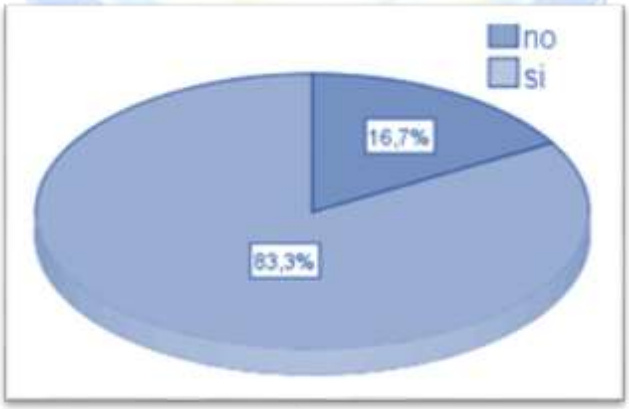


Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 88.9% del personal administrativo respondieron que se debe realizar frecuentemente copias de seguridad de la información relevante para el área y el 11.1% respondieron que no se debe realizar frecuentemente copias de seguridad de la información relevante para el área.

2.7.2 Recursos Humanos

Pregunta 06: ¿El personal de su área tiene conocimiento de la importancia de la seguridad los datos que se manipula ahí?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	6	16,7	16,7	16,7
	si	30	83,3	83,3	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 83.3% del personal administrativo respondieron que el personal de su área tiene conocimiento de la importancia de la seguridad de los datos que se manipula y el 16.7% respondieron que el personal de su área no tiene conocimiento de la importancia de la seguridad los datos que se manipula.

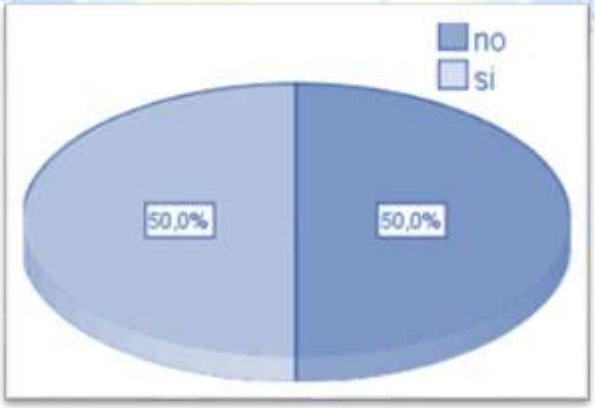
Pregunta 07: ¿Su personal cuenta con un plan de capacitación sobre seguridad de la información?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	18	50,0	50,0	50,0
	si	18	50,0	50,0	100,0
	Total	36	100,0	100,0	

Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 50% del personal administrativo respondieron que el personal cuenta con un plan de capacitación sobre seguridad de la información y el 50% respondieron que el personal no cuenta con un plan de capacitación sobre seguridad de la información.

Pregunta 08: ¿Su personal ha recibido una capacitación por parte del área informática sobre cómo proteger su información (Física y Virtual)?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	18	50,0	50,0	50,0
	si	18	50,0	50,0	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 50% del personal administrativo respondieron que el personal ha recibido una capacitación por parte del área informática sobre cómo proteger sus informaciones y el 50% respondieron que el personal no ha recibido una capacitación por parte del área informática sobre cómo proteger su la información.

2.7.3 Seguridad Física y Ambiental

Pregunta 09: ¿Al ocurrir un robo que ocasione pérdida de la información lo reportaría inmediatamente al área correspondiente?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	si	36	100,0	100,0	100,0

Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se

obtiene que el porcentaje más elevado con un 100% del personal administrativo respondieron que al ocurrir un robo que ocasione pérdida de la información lo reportaría inmediatamente al área correspondiente.

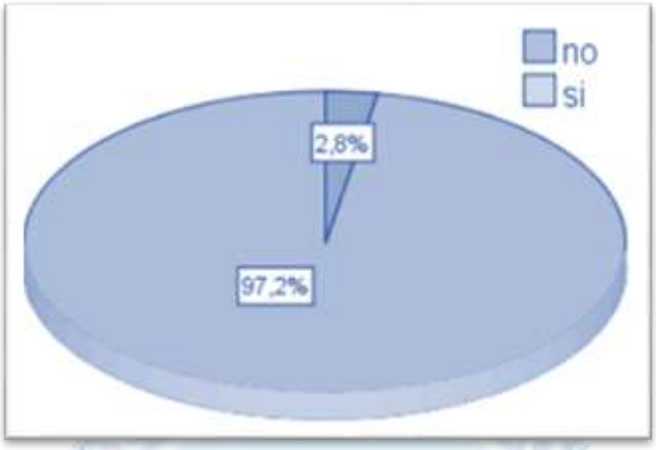
Pregunta 10: ¿Qué medida utiliza más frecuente para respaldar sus datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	a. Hacer una copia de seguridad de archivos manualmente	19	52,8	52,8	52,8
	b. Con un programa para hacer copias de seguridad	4	11,1	11,1	63,9
	c. Respaldar a una nube	8	22,2	22,2	86,1
	d. Ninguna	5	13,9	13,9	100,0
	Total	**36**	**100,0**	**100,0**	

Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 52.8% del personal administrativo respondieron que la medida más frecuente para respaldar sus datos es hacer una copia de seguridad de los archivos manualmente y el 11.1% respondieron que la medida para respaldar sus archivos es con un programa para hacer copias de seguridad.

Pregunta 11: ¿Cree que los datos de su área son importantes y se debe tomar en cuenta las medidas adecuadas para su protección?

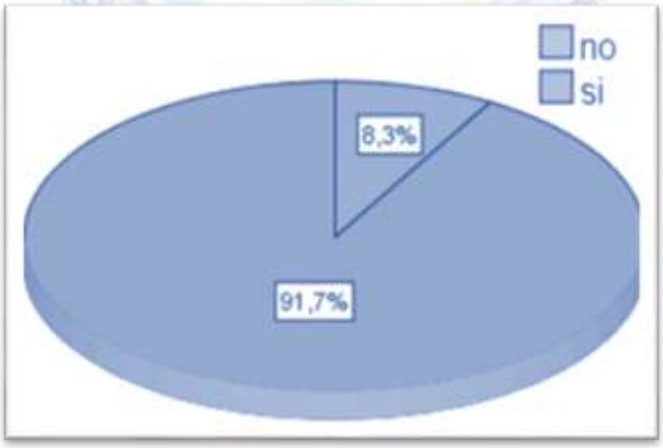
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	1	2,8	2,8	2,8
	si	35	97,2	97,2	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 97.2% del personal administrativo respondieron que los datos de su área son importantes y se debe tomar en cuenta las medidas adecuadas para su protección y el 2.8% respondieron que no creen que los datos de su área sean importantes y se debe tomar en cuenta las medidas adecuadas para su protección.

Pregunta 12: ¿Si un virus informático afecta los datos de su área que tanto retrasaría el trabajo de su personal?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	3	8,3	8,3	8,3
	si	33	91,7	91,7	100,0
	Total	36	100,0	100,0	

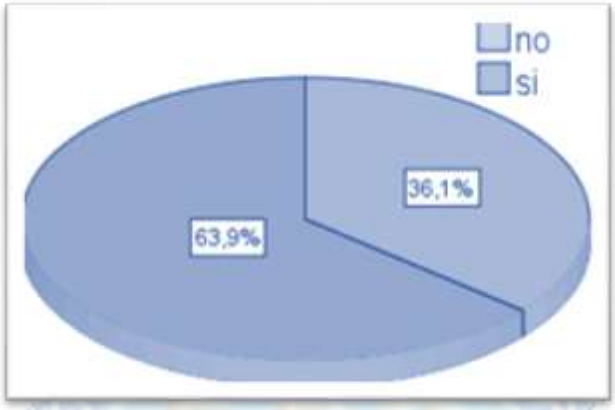


Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 91.7% del personal administrativo respondieron que si un virus informático afecta los datos de su área que tanto retrasaría el trabajo de su personal y el 8.3% respondieron que un virus informático no afecta los datos de su área que tanto retrasaría el trabajo de su personal.

2.7.4 Control de Accesos

Pregunta 13: ¿Considera que la configuración de la red de la institución es la adecuada para brindar seguridad a los datos que se manipulan en el área Dirección Ejecutiva de Producción Estadística?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	13	36,1	36,1	36,1
	si	23	63,9	63,9	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 63.9% del personal administrativo respondieron que la configuración de la red de la institución es la adecuada para brindar seguridad a los datos que se manipulan en el área Dirección Ejecutiva de Producción Estadística y el 36.1% respondieron que la configuración de la red de la institución no es la adecuada para brindar seguridad a los datos que se manipulan en el área Dirección Ejecutiva de Producción Estadística.

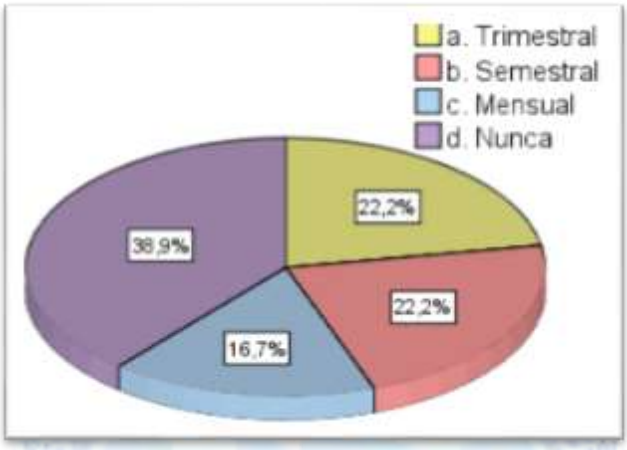
Pregunta 14: ¿Considera que su personal está capacitado para entrar a los sistemas en red de una forma segura y eficaz?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	11	30,6	30,6	30,6
	si	25	69,4	69,4	100,0
	Total	36	100,0	100,0	

Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 69.4% del personal administrativo respondieron que su personal está capacitado para entrar a los sistemas en red de una forma segura y eficaz y el 30.6% respondieron que su personal no está capacitado para entrar a los sistemas en red de una forma segura y eficaz.

Pregunta 15: Como medida de prevención ¿con que frecuencia cambia las contraseñas de acceso al sistema que manipula?

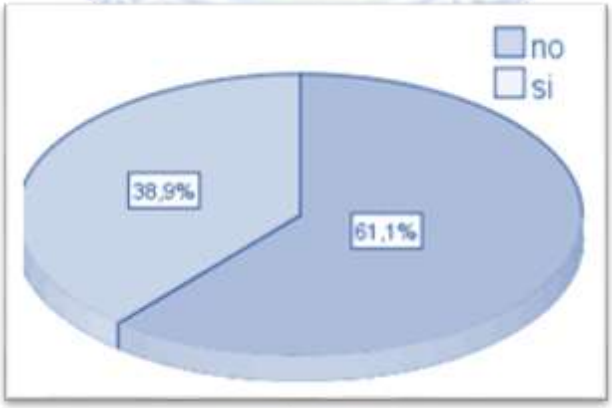
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	a. Trimestral	8	22,2	22,2	22,2
	b. Semestral	8	22,2	22,2	44,4
	c. Mensual	6	16,7	16,7	61,1
	d. Nunca	14	38,9	38,9	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 38.9% del personal administrativo respondieron que la medida más frecuente para cambiar las contraseñas de acceso a los sistemas es nunca y el 16.7% respondieron que la medida menos frecuente para cambiar las contraseñas es mensual.

Pregunta 16: ¿Comparte su computador o sus contraseñas al sistema con otras personas de la institución?

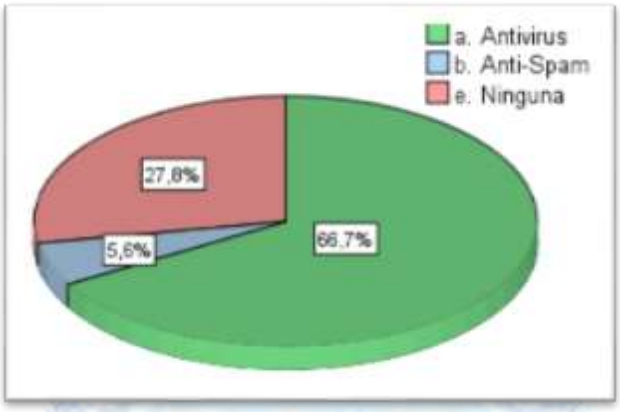
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	22	61,1	61,1	61,1
	si	14	38,9	38,9	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 38.9% del personal administrativo respondieron que la medida más frecuente para cambiar las contraseñas de acceso a los sistemas es nunca y el 16.7% respondieron que la medida menos frecuente para cambiar las contraseñas es mensual.

Pregunta 17: ¿Al navegar por internet, que precauciones toma para protegerse de virus y otros ataques?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	a. Antivirus	24	66,7	66,7	66,7
	b. Anti-Spam	2	5,6	5,6	72,2
	e. Ninguna	10	27,8	27,8	100,0
	Total	36	100,0	100,0	

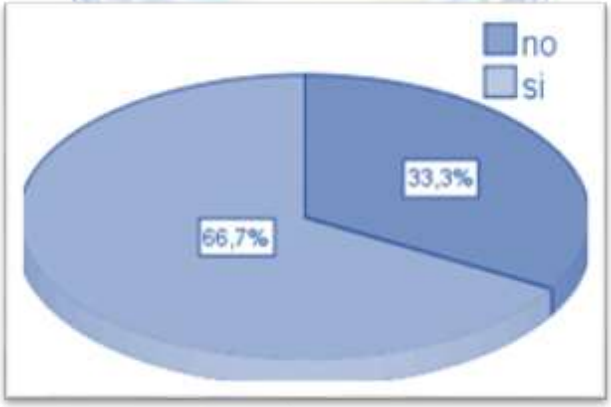


Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 66.7% del personal administrativo respondieron que la precaución que se toma para protegerse de virus y otros ataques al navegar por internet es el antivirus y el 5.6% respondieron que la precaución que se toma para protegerse de virus y otros ataques al navegar por internet es el anti-spam.

2.7.5 Seguridad en Operaciones

Pregunta 18: ¿Tengo suficientes habilidades para restringirle a su personal guardar la información en los diferentes dispositivos externos (archivos, correos electrónicos, en la nube, etc.) de forma adecuada?

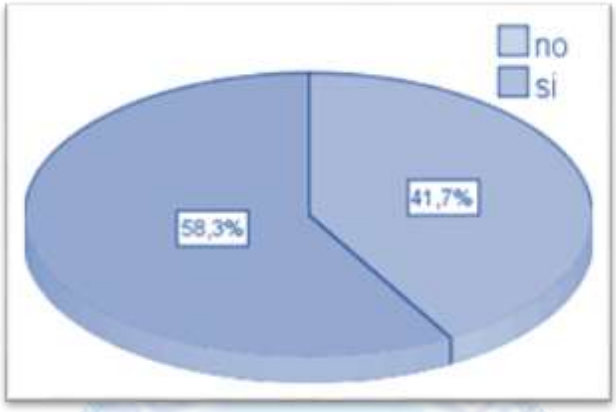
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	12	33,3	33,3	33,3
	si	24	66,7	66,7	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 66.7% del personal administrativo respondieron que hay suficientes habilidades para restringirle a su personal guardar la información en los diferentes dispositivos externos de forma adecuada y el 33.3% respondieron que no hay suficientes habilidades para restringirle a su personal guardar la información en los diferentes dispositivos externos de forma adecuada.

Pregunta 19: ¿Al utilizar el correo electrónico tiene conocimiento sobre los peligros de acceder a email como los Pishing, webs falsas, ingeniería social, etc.?

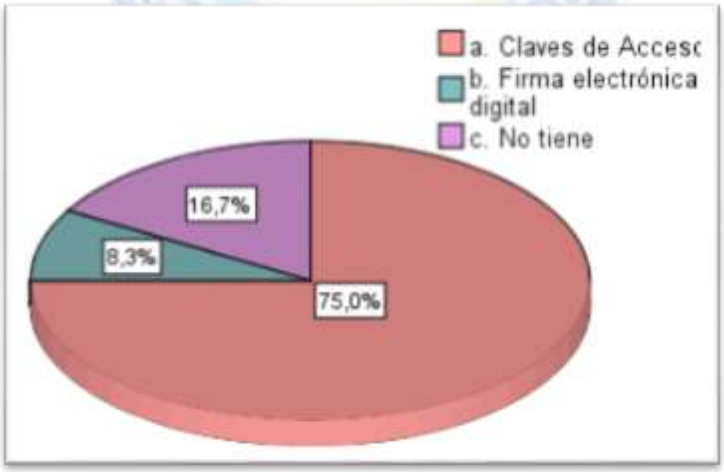
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	no	15	41,7	41,7	41,7
	si	21	58,3	58,3	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 58.3% del personal administrativo respondieron que al utilizar el correo tiene conocimientos sobre los peligros de acceder a email como los Pishing, webs falsas, ingeniería social y el 33.3% respondieron que al utilizar el correo no tiene conocimientos sobre los peligros de acceder a email como los Pishing, webs falsas, ingeniería social.

Pregunta 20: ¿Qué medidas cree que son las más seguras para guardar la información crítica que en su área se maneja?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	a. Claves de Acceso	27	75,0	75,0	75,0
	b. Firma electrónica digital	3	8,3	8,3	83,3
	c. No tiene	6	16,7	16,7	100,0
	Total	36	100,0	100,0	



Análisis e Interpretación: De la información obtenida del instituto ODEI Lambayeque, se obtiene que el porcentaje más elevado con un 75.0% del personal administrativo respondieron que la medida más segura para guardar información crítica es las calves de acceso y el 8.3% respondieron que la medida más segura para guardar información crítica es firma electrónica digital.

2.8 PROCESO DE DESARROLLO

2.8.1 Conclusiones

- ✓ Se realizó un diagnóstico de la situación actual de la seguridad de información en la institución ODEI Lambayeque.
- ✓ Se evaluó la seguridad que se debe tener a los activos de información incluyendo riesgos, amanezcas y vulnerabilidades de la institución.
- ✓ Se identificó que el 64% de los colaboradores de la institución afirman contar con el hardware y software necesario para realizar sus actividades de forma eficaz y eficiente.
- ✓ Se observó que es necesario contar un proceso de control al acceso a la información por personal autorizado e implementar procedimientos acordes con la seguridad de acceso a la información.
- ✓ Así mismo también se observó un alto índice de acuerdo para establecer procedimientos para minimizar el impacto y permitir la continuidad con respecto a la seguridad de los activos críticos.

Con los puntos se deduce que el proyecto de investigación es viable para la institución ODEI Lambayeque, en las principales áreas de Dirección Ejecutiva y Producción Estadística.

2.8.2 Recomendaciones

Se recomienda que a través de la presente investigación que amerita relevancia ampliar y profundizar el desarrollo del SGSI propuesto cuyo aporte es fundamental para el potenciar la seguridad de la información en las áreas de Dirección Ejecutiva y Producción Estadística de la institución.

CAPÍTULO III

ASPECTOS DE LA PROBLEMÁTICA

3 CAPITULO III: ASPECTOS DE LA PROBLEMÁTICA

3.1 REALIDAD PROBLEMÁTICA

Cada día la importancia de la información en las empresas va tomando más fuerza, información que se encuentra en las empresas, tales como los correos electrónicos, páginas web, imágenes, base de datos, faxes, contratos, prestaciones, documentos, fotos, mensajes, conversaciones, etc. No se trata solo de la información registrada, ni de la que la gente genera por sí misma, sino también de la información creada en las PC o Laptops, nos encontramos en un punto de inflexión muy interesante en el que podemos obtener suficientes datos y suficiente poder de computación como para poder hacer algo con dicha información. Las empresas en la actualidad pueden recolectar y clasificar la información de modo que se pueda utilizar rápida y eficientemente de forma más inteligente y a medida que se obtiene más información, se comienza a tener una visión general de las cosas y se utiliza a su favor para la toma de decisiones.

Pero en las empresas dicho activo, la información a diario se encuentra amenazada por riesgos que ponen en peligro su confidencialidad, integridad y disponibilidad y con ello la viabilidad del negocio ya que es esencial para alcanzar los objetivos estratégicos.

Riesgos que no solo provienen desde el exterior de la empresa, sino también desde el interior, en la actualidad el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de hacer negocios, a la vez que han aumentado los riesgos para las empresas que se exponen a nuevas amenazas. Desafortunadamente, es relativamente fácil tener acceso a las herramientas que permiten a personas no autorizadas llegar hasta la información protegida, con poco esfuerzo y conocimientos, causando graves perjuicios para la empresa. La mayor parte de la información de las empresas, reside en equipos informáticos, soportes de almacenamiento y redes de datos, englobados dentro de lo que se conoce como sistemas de información.

El problema radica que estos sistemas de información están sujetos a riesgos y amenazas que pueden generarse desde dentro de la propia organización o desde el exterior, es por ello que la información es un valioso activo del que depende el buen funcionamiento de una organización, pero lamentablemente no todas las empresas ponen los medios necesarios para evitar el robo y manipulación de los de sus datos confidenciales.

Existen dos tipos de riesgos que pueden afectar el activo de información de una empresa, los riesgos físicos como incendios, inundaciones, terremotos o vandalismo que pueden afectar la disponibilidad de nuestra información y recursos, haciendo inviable la continuidad de nuestro negocio si no se está preparado para afrontarlos. Por otra parte se encuentran los riesgos lógicos amenazas relacionados con la propia tecnología que aumentan día a día como Hackers, robos de identidad, spam, virus, robos de información y espionaje industrial, por nombrar algunos, pueden acabar con la confianza de nuestros clientes y la imagen en el mercado **(INTECO - Instituto de Normas Técnicas de Costa Rica, 2002)**.

En la actualidad el aspecto más básico es proteger el activo de la información, lamentablemente el aumento de los riesgos está resultando exponencial al avance de las nuevas tecnologías y tanto empresas internacionales como nacionales se han visto afectadas, pondremos como ejemplos:

Internacional:

(Crespo, 2016), podemos poner como ejemplo reciente a BitGo es una empresa con sede en California – Estados Unidos que ofrece la plataforma líder para la seguridad y las tecnologías de Bitcoin[2], podría decirse que no solo es la plataforma más segura, también la más rápida siendo

[2] Bitcoin es una moneda, como el euro o el dólar estadounidense, que sirve para intercambiar bienes y servicios. Sin embargo, a diferencia de otras monedas, Bitcoin es una divisa electrónica que presenta novedosas características y destaca por su eficiencia, seguridad y facilidad de intercambio. Su mayor diferencia frente al resto de monedas, se trata de una moneda descentralizada, por lo que nadie la controla.

una de las más eficientes, pero en los últimos meses el monedero BitGo sufre un ataque DDoS prolongado que hace que la industria se tambalee ya que se han vivido ataques contra los servicios que ofrece la empresa, hackeo que ha supuesto la fuga de datos de los clientes y en muchos casos supuso dejar vacías las cuentas de los usuarios. El ataque contra los servicios no solo ha afectado a este monedero virtual, también a otros servicios que hacen uso de su API, como por ejemplo Wirex, Bitstamp, Bitfinex, Unocoin y Kraken. El resultado ha sido una gran cantidad de horas fuera de servicio en los últimos meses.

Como ejemplo en el año 2016 los hackers financiados por gobiernos, están utilizando un truco inteligente para atacar infraestructuras críticas (lado corporativo) como centrales nucleares, represas, refinerías de petróleo. Según Eric Knapp, ingeniero jefe de ciberseguridad de Honeywell, un tercio de malware encontrado en infraestructuras críticas vinieron de unidades USB conectadas por los usuarios. El malware especialmente diseñado infecta unidades USB que se utilizan por los empleados, y luego infecta el sistema de control de la infraestructura crítica cuando está conectado en ese lado. Por ejemplo el malware Stuxnet, que fue creado por los Estados Unidos e Israel, específicamente contra las instalaciones nucleares iraníes. El virus parecía un software normal para operadores de plantas de energía nuclear, pero degradaba lentamente la planta, dejando a los iraníes con ninguna otra opción más que la de cerrar la planta **(Turton, 2016)**.

Como ejemplo el año 2011 conocido como el "El Año del Hacker", en referencia al auge de colectivos como ANONYMOUS o LULZSEC y a los numerosos ataques a corporaciones en todo el mundo, como Sony PlayStation Network en que se expuso la información de más de 77 millones de usuarios marcó un pico, pero llegó 2012 y el asunto todavía estaba sin resolver. Entonces el golpe se lo llevó BLIZZARD, luego APPLE, UBISOFT, EVERNOTE, LINKEDIN, YAHOO, NINTENDO, TWITTER, pocas compañías se libran **(Pomeyrol, 2013)**.

Nacional:

(El Comercio, 2015), podemos poner como ejemplo en el año 2012 al Organismo Superior de las Contrataciones del Estado – OCSE, la cual en la madrugada del 4 de noviembre, un desperfecto en el servidor informático hizo colapsar el denominado Sistema Electrónico de Adquisiciones y Contrataciones del Estado (SEACE). Se perdió toda la información almacenada de los procesos de contrataciones de las entidades públicas del país, de los años 2009 al 2012. Desaparecieron casi 800 mil archivos digitales que alojaban las bases de los procesos, la buena pro, los contratos, las cartas-fianza y la absolución de consultas, y que se centralizan en la base de datos del OSCE. El problema alcanzo a 1.746 entidades del Estado, de un total de 3.080.

Otro claro ejemplo ocurrió en noviembre de 2009, donde piratas informáticos chilenos hachearon la web del Ministerio de Trabajo del Perú con mensajes que hacían alucinación al espionaje de ese país al nuestro.

3.2 ANÁLISIS DE LA SITUACIÓN ACTUAL

El Instituto Nacional de Estadística e Informática – Filial Lambayeque o también llamado la oficina departamental de estadística e informática (ODEI) – Lambayeque, es un órgano ejecutivo en el nivel departamental, que depende estructuralmente de la jefatura de INEI- Lima y funcionalmente de la oficina técnica de estadística departamental (OTED). Se encuentra ubicado en la avenida Balta Nº 658 – 2do piso en la ciudad de Chiclayo.

Dentro de su ámbito de competencia es responsable de la gestión y resultados de las actividades estadísticas e informáticas, propias de sus funciones generales correspondiente a su jurisdicción. Para el cumplimiento de sus objetivos y funciones cuenta con autonomía técnica y de gestión, establecido en la ley de creación.

Bitcoin no tiene un emisor central como los dólares o los euros, la criptomoneda es producida por las personas y empresas de alrededor del mundo dedicando gran cantidad de recursos a la minería.

ODEI - Lambayeque está formada por las áreas de Dirección departamental, Oficina técnica de estadísticas departamentales, Dirección ejecutiva de difusión estadística, Dirección ejecutiva de producción estadística, O.T. Administración y O.T. De informática

Luego de un análisis de todas las áreas involucradas, la investigación se centrará sobre las áreas de "**Dirección Ejecutiva de Producción Estadística" y** "**Dirección Ejecutiva de Difusión Estadística"**, puesto que estas áreas manejan información muy importante. El área de Producción Estadística recopila información de los diversos sectores de la actividad pública y de algunas empresas de todo el departamento de Lambayeque, una vez que se recopila la información, se tabula, se generan cuadros estadísticos y se elabora documentos oficiales que demuestren como está la actividad económica y social en el departamento y que dicha información, sirva como herramienta para la toma de decisiones al estado peruano y el área de Difusión Estadística recopila información sobre los precios de la canasta familiar y el proceso de marketing de los libros que procesan.

Las áreas de Difusión Estadística y Producción Estadística fueron analizadas mediante una entrevista al Ing. Daniel Cansino Castañeda, director departamental, quien permitió dar un recorrido a las instalaciones, asimismo, proporcionó el reglamento autorizado con la que se cuenta, se realizó un análisis de las áreas y basándose en la experiencia de trabajo se analizó la situación de las áreas desde su origen hasta la actualidad la cual la detallaremos a continuación:

Dirección Ejecutiva de Producción Estadística

Los sectores de los cuales se necesita dicha información son: gerencia regional de agricultura, gerencia regional de salud y Es Salud, gerencia regional de transporte, gerencia regional de educación, gerencia regional de turismo, gobierno regional de Lambayeque, universidades, policía nacional, etc.

Existen dos informes principales que genera esta área después de la recopilación de información de todos los sectores involucrados, los reportes son el "**Compendio Estadístico de Lambayeque**" el cual maneja información básica sectorial y el cual tiene una duración entre 5 a 6 meses para generarlo y el informe de "**Evolución de las Actividades de Producción**" el cual maneja análisis de los sectores económicos es decir de aquellos sectores que requieren producción y para su generación tiene una duración entre 2 a 4 semanas.

Dirección Ejecutiva de Difusión Estadística

Esta área se encarga de resguardar, controlar, gestiona y difundir la documentación que genera la institución. Su objetivo principal es la explosión documental por parte de los usuarios que solicitan la información por ejemplo personas profesionales, universitarios, estudiantes, investigadores y público en general, es decir tiene como finalidad servir de referencia y ayudar a los investigadores. Así como la de generar mensualmente el informe del indicador macroeconómico

Las áreas en mención, solo ha contado con los 2 mismos problema durante varios años, el cual es la perdida de información debido a las falla técnicas del servidor donde se guarda la información recaudada de los sectores y el extravió de información estadística confidenciales debido a que los usuarios comenten errores y borran sus datos de forma accidental y hasta la actualidad no ha contado con otro tipo problema en lo que respecta a la perdida de este activo de la información, pero esto no significa que dicho activo no esté sujeta a amenaza o vulnerabilidades tales como hackers que puedan borrar o alterar sus datos, divulgación de contraseñas, virus, robos de las computadoras o algún desastre natural como terremoto, incendios y de más. Si ocurriera lo mencionado, generaría al ODEI Lambayeque perdidas de dinero, ya que los trabajadores de estas áreas y de otras áreas tendrían recarga de trabajo, doble costo de tiempo e incluso despedida de personal. Todo esto por la pérdida valiosa de la información.

Esta área en mención no cuenta con medidas, controles y procedimientos de seguridad para preservas sus activos de información frente a vulnerabilidades que pueden afectar la

disponibilidad de los activos de información y recursos haciendo inviable la continuidad del negocio y amenazas que puede acabar con la confianza del pueblo y la imagen en el departamento de ODEI de la región Lambayeque, es por ello que la investigación se basara en las áreas denominas "***Dirección Ejecutiva de Producción Estadística***" *y* "***Dirección Ejecutiva de Difusión Estadística***" por ser consideradas las áreas más importantes de la institución.

3.3 FORMULACIÓN DEL PROBLEMA

¿De qué manera la propuesta del Modelo de Sistema de Gestión de Seguridad de Información - SGSI permitirá fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información en el Instituto Nacional de Estadística e Informática – INEI Filial Lambayeque?

3.4 JUSTIFICACIÓN E IMPORTANCIA DEL ESTUDIO

El presente trabajo de investigación se ha planteado para Instituto Nacional de Estadística e Informática – Filial Lambayeque con la finalidad de fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información del área de Dirección Ejecutiva de Producción Estadística, debido a que el área mencionada es pieza indispensable para saber el estado de la actividad económica y social en el departamento de Lambayeque y dicha información sirve como herramienta para la toma de decisiones al estado peruano

Dicho trabajo de investigación es muy importante para la institución debido a que permitirá establecer políticas, procedimientos y monitoreo con el objetivo de disminuir los riesgos ante la pérdida de información, permitiendo reducir las amenazas hasta alcanzar un nivel asumible para el área y permitiendo que la continuidad del negocio está asegurada y la de reducir costos derivado de una racionalización de los recursos.

3.5 OBJETIVOS

3.5.1 Objetivo General

Modelar un sistema de gestión de seguridad de información (SGSI) que permita fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información en los procesos claves que se encuentran bajo la gerencia del instituto nacional de estadística e informática-ODEI Lambayeque.

3.5.2 Objetivos específicos

A. Realizar un diagnóstico de la situación actual de la seguridad de información en la institución ODEI Lambayeque y centrándonos en las áreas de "Dirección Ejecutiva de Producción Estadística" y "Dirección Ejecutiva de Difusión Estadística".
B. Evaluar el cuidado y distribución de la información del área seleccionada a través de una metodología de trabajo con encuestas, cuestionarios, entrevistas y otros.
C. Identificar a través del análisis de riesgo los proyectos que potenciarán la seguridad de la información en las áreas de "Dirección Ejecutiva de Producción Estadística" y "Dirección Ejecutiva de Difusión Estadística" (Tecnología de información y comunicaciones).
D. Conocer las diferentes condiciones de acceso a la información, tanto externo como interno de las áreas mencionadas.

Proponer un SGSI para identificar los riesgos, las amenazas y las vulnerabilidades para brindar a las áreas de "Dirección Ejecutiva de Producción Estadística" y "Dirección Ejecutiva de Difusión Estadística" información valiosa del estado actual de la seguridad de información.

CAPÍTULO IV

MATERIALES Y MÉTODOS

4 CAPITULO IV: MATERIALES Y MÉTODOS

4.1 HIPÓTESIS Y VARIABLES

4.1.1 Formulación de la Hipótesis

Por ser la investigación una propuesta de un Modelo de Sistema de Gestión de Seguridad De Información - SGSI para el Instituto Nacional de Estadística e Informática - INEI Filial Lambayeque, no se necesita plantear una hipótesis.

4.1.2 Variables y Operacionalización

- ✓ **INDEPENDIENTE:** SGSI

  Definición: SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. SGSI, la seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad, disponibilidad y control, así como de los sistemas implicados en su tratamiento, dentro de una organización.

  Definición Operacional: SGSI que nos permitirá establecer políticas, procedimientos y controles con el objetivo de disminuir los riesgos el instituto nacional de estadística e informática-INEI Filial Lambayeque.

- ✓ **DEPENDIENTE:** Protección y control de la seguridad de la información para el INEI - Filial Lambayeque: confidencialidad, integridad, disponibilidad y monitoreo.

  Definición: Protección a todo aquello que la entidad como el INEI - Filial Lambayeque considera importante en cuanto a sus activos de información, como los reportes de las dos áreas más importantes (Producción y Difusión Estadística) ya que sería criticó que la información que se manejan en la institución pudieran ser accedidos por intrusos, afectando la confidencialidad, disponibilidad e integridad de sus activos de información. La gestión de los controles técnicos a plantear será recomendada por un sistema de información para proteger los fundamentos básicos de la seguridad de la información.

  Definición Operacional: Es la gestión en la que se emplearán los controles necesarios para proteger la información, con la finalidad de fortalecer la confidencialidad, integridad, disponibilidad y control de los documentos en el instituto nacional de estadística e informática INEI - Filial Lambayeque y de esta forma, evaluar las vulnerabilidades y reducir los riesgos.

4.2 DISEÑO METODOLÓGICO

4.2.1 Tipo de Estudio y diseño de contrastación de hipótesis

El proyecto propuesto está referido a una investigación **Descriptiva**. Ya que de acuerdo con el fin que persigue determinar los problemas actuales, mediante una descripción y de comprender de forma íntegra el presente.

Es de tipo **transversal**; pues se trata de conocer la percepción del usuario en una sola vez, y se procede a su descripción y análisis; la recolección de los datos se desarrollará en un periodo determinado que corresponde al segundo o tercer trimestre de 2016.

4.2.2 Población, muestra de estudio y muestreo

- ✓ **POBLACIÓN**

  En primer lugar, se determinará cuál será el marco muestral y la unidad de análisis, para luego proceder a delimitar la población que será estudiada y sobre la cual se pretende generalizar los resultados; para ello, se tomará como referencia (marco muestral) el Cuadro de Personal de planta del Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque. En base a dicha información se ha determinado:

Universo: el personal que trabaja con la ODEI Lambayeque; Dicho personal labora en las diferentes áreas administrativas del Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque.

Informante: Los usuarios en las diferentes dependencias/ áreas del Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque que emplean para su trabajo los sistemas locales.

Personal Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque

CONDICIÓN	PERSONAL
Nombrados	8
Contratación Administrativa de Servicio	8
Proyecto permanente ENAHO	8
Proyecto permanente ENAPRES	5
Proyecto permanente ENDES	8
TOTAL	37

- ✓ **MUESTRA**
  La muestra es el conjunto de elementos de la población accesible que va a formar parte de nuestro estudio, por lo que será el Personal de Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque.
- ✓ **MUESTREO**
  No se considerará realizar la técnica de muestreo porque se trabajará con el total de la población accesible para la aplicación del instrumento a crear.

4.2.3 Métodos y procedimientos para la recolección de datos.

Entre los principales métodos que se empleará en la presente investigación, se considera la encuesta, que permitirá recabar la información sobre la percepción en relación a los factores críticos de éxito por parte de los usuarios del sistema de información del Instituto Nacional de Estadística e Informática – Oficina departamental de Lambayeque. Para la presente investigación, se ha empleado el cuestionario, que ha sido desarrollado a partir de las variables e indicadores de acuerdo a la investigación teórica y propuesta del investigador.

CUESTIONARIO

Se medirá con un análisis de riesgo, el cuse se modela comenzando con la valoración de los activos, y que consiste en la información que tiene los criterios requeridos para ayudar a lograr los objetivos de la institución de estudio (incluyendo todos los recursos necesarios para producir dicha información).

TIPO DE ENCUESTA

Considerando las características de la encuesta, se utilizará la encuesta personal basado en cuestionarios de preguntas cerradas con escala de intervalo (Kendall & Kendall, 1997), para poder cumplir al menos con el tamaño de muestra recomendado.

4.2.4 Análisis Estadísticos De Los Datos

Para el procesamiento estadístico de datos se iniciará con la digitación de los cuestionarios y encuestas aplicadas bajo un formato predefinido de captura de información en base al cuestionario formulado; se usará el software versión 22 de SPSS para Windows con el apoyo de Microsoft Excel. El ingreso de datos se realizará por el investigador. Los datos se presentarán en estadísticas univariantes que se describirán en tablas de distribución de frecuencias con sus figuras respectivas. Para el análisis y prueba de hipótesis, se emplea la técnica de análisis multivariante; en particular, el análisis factorial.

CAPÍTULO V

FASE DE DESARROLLO

5 CAPITULO V: FASE DE DESARROLLO

En el siguiente capítulo, se realizará el desarrollo de SGSI proveyendo un marco de trabajo para el tratamiento de riesgos que permita mantener la continuidad del negocio del instituto ODEI Lambayeque para el cumplimiento de la legislación y fomentar las buenas practicas.

5.1 PLANEAR (PLAN)

En esta fase se establecerá los objetivos y procesos necesarios para llegar a establecer los controles de seguridad de información esperados por la institución ODEI de Lambayeque, en este caso de estudio, la protección de los activos de información para las áreas de "***Dirección Ejecutiva de Producción Estadística***" *y* "***Dirección Ejecutiva de Difusión Estadística***". Para ello, realizaremos las siguientes acciones que detallaremos a continuación:

5.1.1 Línea Base: Evaluación de la Situación de Seguridad Actual

Tomaremos la primera medición de los indicadores contemplados antes del desarrollo del proyecto de investigación a la institución, dicha información nos servirá como Línea Base para reconocer el valor de los indicadores antes de iniciarse las acciones planificadas, es decir establecer un punto de partida del proyecto.

Dentro del proceso del proyecto, esta line base que constituiremos nos permitirá establecer futuras comparaciones y permitiéndonos indagar por los cambios ocurridos conforme el proyecto se vaya desarrollando.

El resultado de la línea base se expresa en un informe que describe la situación actual de la institución ODEI Lambayeque, en cuanto al estado de seguridad de los activos de información, dicho informe se basa en el estándar NTP ISO/IEC 27001:2014. (Ver Anexo 04 - INEISGSI01 - Evaluación de la situación de seguridad actual (línea de base))

5.1.2 Análisis de Brechas

Este análisis nos permite conocer el estado actual de la institución frente al cumplimiento de la NTP ISO/IEC 27001:2014, específicamente en los 114 controles definidos en la 27002 que el estándar ofrece, es decir, permitiéndonos identificar la situación actual referente a la gestión de seguridad de información dentro del modelo de negocio de ODEI Lambayeque dedicado a la producción y difusión de informes estadísticos de la región. Habiendo establecido un alcance moderado y previo coordinación con el responsable máximo de la institución (Director Departamental), el proyecto de investigación se basará en **5 dimensiones**, las cuales son:

- ✓ Cultura organizacional.
- ✓ Recursos humanos.
- ✓ Control de accesos
- ✓ Seguridad física y ambiental.
- ✓ Continuidad de negocio.

Los objetivos principales de este análisis, son estudiar la información arrojada en la auditoría, priorizando las brechas respecto al plan estratégico del negocio para identificar las principales brechas a tratar y proveer un resumen ejecutivo identificando los principales problemas de seguridad que aquejan a la institución.

Plantilla de Análisis de Brechas

INEI SGSI 02 - ANÁLISIS DE BRECHAS							
Dim.	**Cláusula**	**Descripción**	**C**	**NC**	**CP**	**Control**	**Referencia de la NTP ISO/IEC 27001:2014**

Tabla 1: Plantilla de Análisis de Brechas

A continuación, se presenta la plantilla del documento que será utilizado en el proyecto de investigación. Asimismo, resulta muy importante reconocer que valores ingresar en cada uno de los campos de este documento:

- ✓ **Dimensión:** las dimensiones básicas de la seguridad de la información.
- ✓ **Clausula:** identificador del control que se están aplicando para alcanzar el objetivo de control correspondiente.
- ✓ **Control:** nombre del control que se están aplicando para alcanzar el objetivo de control correspondiente.
- ✓ **C:** Cumple la salvaguarda en la institución.
- ✓ **NC:** No Cumple la salvaguarda en la institución.
- ✓ **CP:** Cumple Parcialmente la salvaguarda en la institución.
- ✓ **Control:** definición del control especifico basada en el estándar.
- ✓ **Referencia de la NTP ISO/IEC 27001:2014:** justificación de la aplicación del control.

Como consecuencia obtuvimos una matriz de análisis de brechas, esto nos permite establecer estrategias y mecanismos de acción para el cumplimiento de los procedimientos y objetivos de control que establece la norma anteriormente mencionada y desarrollar el sistema de gestión de seguridad de información. (Ver Anexo 05 - INEISGSI02 - Análisis de Brechas).

5.1.3 Definir el Alcance de SGSI

Se establece el alcance de sistema de gestión de seguridad de información para ODEI Lambayeque, es de suma importancia establecer un alcance moderado ya que un alcance excesivo puede hacer que nuestro proyecto sea inabordable y por ende se llevaría al fracaso y si establecemos un alcance muy reducido puede que no contemplemos aspectos realmente importantes y por ende dar un resultado que no sea de utilidad para los propósitos de la institución.

Al haber realizado un estudio de los procesos de la institución (Procesos CORE, procesos operativos y procesos de soporte) y basándonos en la norma NTP ISO/IEC 27001:2014 que nos ofrece una lista de dominios en las que se debe aplicar la seguridad de la información, se decide que este proyecto de investigación al ser de corto tiempo de duración y adicionando que la institución es muy grande de abarcar, junto con el director departamental el cual es la autoridad máxima, se tomó la siguiente decisión:

El sistema de gestión de seguridad de la información está destinado cubrir toda la información que queda expuesta a sufrir cambios, alteraciones o robo de los activos de las áreas principales de la institución, las cuales son "***Dirección Ejecutiva de Producción Estadística"*** *y "**Dirección Ejecutiva de Difusión Estadística"***. (Ver Anexo 06 - INEISGSI03 - Definición del Alcance)

5.1.4 Elaborar la Políticas de Seguridad de Información

"Las Políticas son documentos de alto nivel" las cuales constituyen la filosofía corporativa y el pensamiento estratégico de la alta gerencia. Al haber establecido el alcance, el responsable directamente en este caso el director departamental o un equipo de la Alta Dirección autorizado por el, deberá emitir e implementar una política de seguridad de información que apoye al logro de los objetivos de la institución.

El responsable debe diseñar un ambiente de control positivo, cuyo único trabajo es la de formular, desarrollar, documentar, anunciar y fiscalizar las políticas que abarcan las metas y las directrices generales. Estas políticas serán aplicadas a las áreas que fueron mencionadas en el alcance, dicha política debe ser formalmente aprobadas y apoyadas por la alta dirección. (Ver Anexo 07 - INEISGSI04 - Política Seguridad Información).

Proceso – Elaborar la Políticas de Seguridad de Información

A continuación, se presenta el proceso que se realizó para elaborar la Política de Seguridad de Información en la institución donde se está desarrollando el proyecto de investigación:

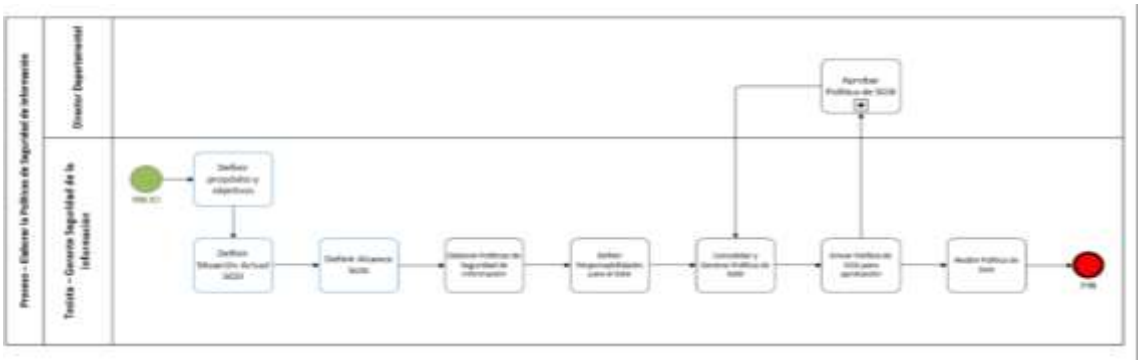


Imagen 6: Proceso – Elaborar la Políticas de Seguridad de Información

5.1.5 Declaración de Aplicabilidad

La presente declaración de aplicabilidad, es un documento que contiene todos los controles de Seguridad de la Información establecidos en la institución, detallando su aplicabilidad, estado y documentación relacionada. Es muy importante ya que es el nexo entre la evaluación y el tratamiento del riesgo, así como el documento que define la implementación de los controles del SGSI.

Para este caso de estudio, en la institución ODEI Lambayeque se confirmó que no existe una declaración de aplicabilidad, por la cual se presenta una propuesta donde se identificaron que controles se deben implementar dentro del documento de aplicabilidad, esto se basó en la identificación de que procesos están considerados dentro de la política y el alcance del proyecto, así como también las justificaciones de aquellos controles que no serán implementados. (Ver Anexo 08 - INEISGSI05 - Declaración de aplicabilidad)

Plantilla de Declaración de Aplicabilidad

INEISGSI05 - DECLARACIÓN DE APLICABILIDAD					
Dimensión	**ID**	**Controles**	**Aplica**	**Justificación**	**Control**

Tabla 2: Plantilla de Declaración de Aplicabilidad

A continuación, se presenta la plantilla del documento que será utilizado en el proyecto de investigación. Asimismo, resulta muy importante reconocer que valores ingresar en cada uno de los campos de este documento, dicha información está basada en el estándar NTP ISO/IEC 27001:2014:

- ✓ **Dimensión:** las dimensiones básicas de la seguridad de la información.
- ✓ **ID:** identificador del control del estándar.
- ✓ **Controles:** donde se indican el nombre del control que se están aplicando para alcanzar el objetivo de control correspondiente.
- ✓ **Aplica:** se debe responder previa coordinación con el responsable máximo de la institución, si el control correspondiente se decide si se va a implementar (Si o No).
- ✓ **Justificación:** en este campo se detalla la razón por la de se necesita implementar o no el control especificado.
- ✓ **Control:** definición del control especifico basada en el estándar.

Proceso – Elaborar la Declaración de Aplicabilidad

A continuación, se presenta el proceso que se realizó para elaborar la Declaración de Aplicabilidad en la institución donde se está desarrollando el proyecto de investigación:

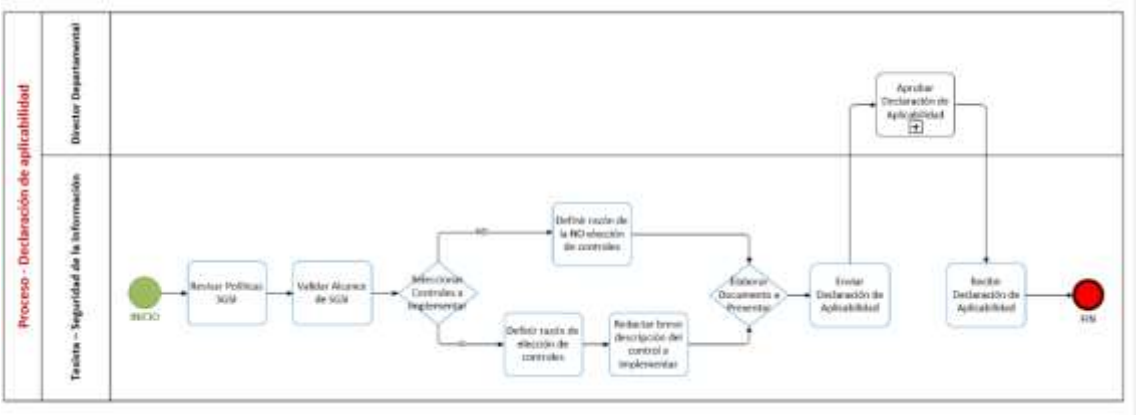


Imagen 7: Proceso - Declaración de Aplicabilidad

5.1.6 Evaluación de Riesgos Basados en Magerit

Como es de conocimiento general, de toda organización se encuentra expuesta a riesgos; debido a que no existe un entorno 100% seguro, ya que la exposición de riesgos es constante. Por tal motivo toda organización deberá estar alerta a cualquier cambio o situación extraña y que considera que podría afectar negativamente a un activo, a un dominio o a toda su organización **(Lucero Gómez & Valverde Padilla, 2012, pág. 38).**

En esta etapa de evaluación de riesgos basados en Magerit, debe alcanzar los siguientes objetivos:

- ✓ Identificar los activos de información más relevantes que posee la institución ODI Lambayeque en las áreas mencionadas.
- ✓ Establecer las amenazas a las que se encuentran expuestas cada activo de información.
- ✓ Elegir salvaguardas apropiadas para los activos de información.
- ✓ Estimar el impacto si se materializara alguna amenaza.

Ver Anexo 10 - INEISGSI07 - Evaluación de riesgos

Plantilla de Matriz de Evaluación de Riesgo

INEISGSI09 - EVALUACIÓN DE RIESGOS														
ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	**Impacto**		**Probabilidad**		RI	SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			

Tabla 3: Plantilla de Matriz de Evaluación de Riesgo

A continuación, se presenta la plantilla del documento que será utilizado en el proyecto de investigación. Asimismo, resulta muy importante reconocer que valores ingresar en cada uno de los campos de este documento, dicha información está basada en el estándar NTP ISO/IEC 27001:2014:

- ✓ **Activo:** se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- ✓ **C:** se refiere a la confidencialidad de los activos de información, dicho valor oscila entre Baja y Alta.
- ✓ **I:** se refiere a la integridad de los activos de información, dicho valor oscila entre Baja y Alta.
- ✓ **D:** se refiere a la disponibilidad de los activos de información, dicho valor oscila entre Baja y Alta.

- ✓ **V:** se refiere a la Valoración que se le asigna al activo de la información, el cual se obtiene mediante la fórmula **(33%D + 33%I + 33%D) x 10**
- ✓ **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- ✓ **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la institución.
- ✓ **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- ✓ **Impacto:** El coste para la institución de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- ✓ **Probabilidad:** El riego es la probabilidad de que se produzca un impacto determinado en un activo de seguridad, en un dominio e incluso en toda la institución.
- ✓ **RI:** Riesgo Inherente, este valor se genera automáticamente en base a la fórmula:
  RI= Nivel de Impacto x Nivel de Probabilidad
- ✓ **Salvaguarda:** Las políticas, los procedimientos, las prácticas y las estructuras institucionales concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- ✓ **Respuesta al Riesgo:** respuesta al riesgo detectado, el valor oscila entre evitar, transferir, mitigar o aceptar.

Proceso – Elaborar Matriz de Evaluación de Riesgos

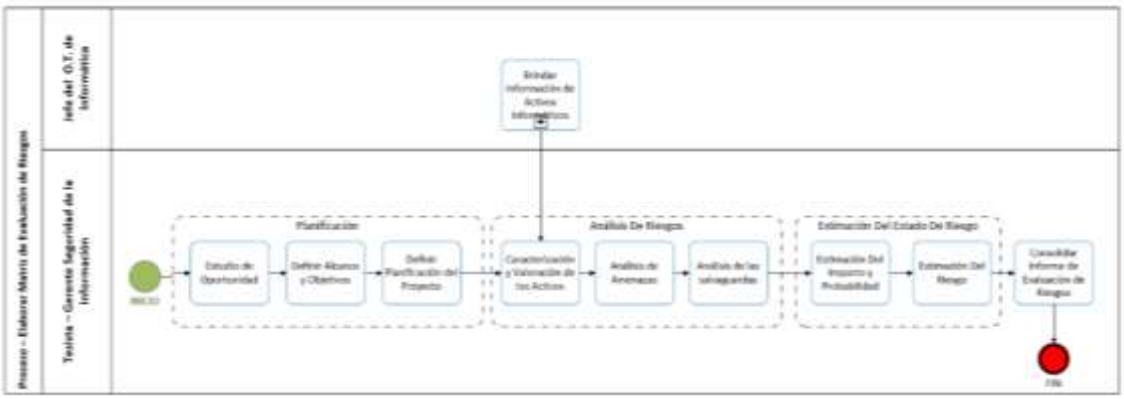


Imagen 8: Proceso – Elaborar Matriz de Evaluación de Riesgos

Apoyándonos en la metodología Magerit VS 3.0 se desarrollarán tres procesos de análisis de riesgos dela seguridad de la información para el logro del proyecto de investigación:

5.1.6.1 Proceso P1: Planificación

Empezaremos con una de las etapas más importantes de la metodología, ya que estableceremos el marco de referencia para el desarrollo del proyecto, esta etapa contara con 4 actividades las cuales son:

- ✓ **Actividad 1: Estudio de Oportunidad.**

El objetivo específico en esta actividad, es realizar un diagnóstico sobre el estado de seguridad de la información de la institución ODEI Lambayeque, así como la de comprometer a la dirección departamental del instituto para poder realizar una propuesta de SGSI.

✓ **Actividad 2: Definición del Alcance y Objetivos del Proyecto**

Una vez recibido el visto aprobatorio por la alta dirección para desarrollar el proyecto, se establece los limites, el dominio y los objetivos para su proceso. Esta actividad ya ha sido desarrollada en la fase del PDCA denominada "Definir el Alcance de SGSI", dichos objetivos han sido planteados con el propósito de realizar un minucioso y real análisis de riesgos que lleven a una futura e exitosa implementación del sistema de gestión de seguridad de información para la institución ODEI Lambayeque.

✓ **Actividad 3: Planificación del Proyecto**

Para el desarrollo exitoso del proyecto de investigación, se debe realizar un cronograma de actividades que nos sirve como bitácora del trabajo a realizar. (Ver Anexo 09 - INEISGSI06 - Cronograma de trabajo)

✓ **Actividad 4: Lanzamiento del Proyecto.**

Empieza el proceso de análisis de riesgos y se adopta las técnicas de entrevistas y observación directa hacia los colaboradores de la institución, dichas técnicas permiten la recolección de información.

5.1.6.2 Proceso P2: Análisis De Riesgos

Esta etapa contara con 3 actividades las cuales son:

✓ **Actividad 1: Caracterización y Valoración de los Activos**
Esta actividad abarca las siguientes tareas:

Tarea 1: Identificación de los Activos

La identificación y clasificación de los activos se realizará en base al Libro II de la metodología MAGERIT versión 3, en donde nos presenta el catálogo de elementos. (Ver Anexo 02 - Clasificación De Los Activos)

TIPO DE ACTIVO	CÓDIGO
ESENCIAL	
Documentos de IPC	E01
Documento de Compendio Estadístico del Departamento	E02
Documento de Evolución de las Actividades de Producción	E03
Documento de Registro Nacional de Municipalidades	E04
DATOS / INFORMACIÓN	
Documento de Centro Documentario	D01
Información de Recursos Humanos	D02
Módulo contable	D03
Inventario de hardware	D04
Bandeja de correos electrónicos	D05
CLAVES CRIPTOGRÁFICAS	
Contraseñas de sistema IPC	C01
Contraseñas de correos electrónicos Institucional	C02
SERVICIOS	
Escuela de Capacitación	S01
Información de Estadística	S02
APLICACIONES INFORMÁTICAS (SOFTWARE)	
Sistema IPC	A01

Sistema de Control Encomienda	A02
EQUIPAMIENTO INFORMÁTICO (HARDWARE)	
Servidor Data Center	EI01
PCs de Escritorio	EI02
PCs Portátiles	EI03
Proyectores	EI04
REDES DE COMUNICACIONES	
Cableado de red	RC01
Router	RC02
Switch	RC03
Hub	RC04
SOPORTES DE INFORMACIÓN	
Discos duros externos	SI01
DVDs	SI02
EQUIPAMIENTO AUXILIAR	
Impresoras	EA01
Cámaras de seguridad	EA02
INSTALACIONES	
Local del ODEI Lambayeque	I01
PERSONAL	
Director de Sistema Administ. IV	P01
Asistente Administrativo II	P02
Director de Sistema Administ. II (Difusión)	P03
Asistente Serv. Eco. Finan. I	P04
Técnico en Estadística II	P05
Secretaria IV	P06
Director de Sistema Administ. II (Producción)	P07
Asistente Serv. Econ. Finan. II	P08
Asistente Administrativo I	P09
Operador PAD III	P10
Coordinador de Proyectos	P11
Encuestador	P12
Jefe del O.T. de Administración	P13
Secretaria	P14
Jefe del O.T. de Informática	P15
Encargado de Soporte	P16

Tabla 4: Identificación de los Activos

Tarea 2: Valoración de los Activos

A continuación, se presentan las tablas con las escalas de valoración de disponibilidad, integridad, confidencialidad:

VALORIZACIÓN DE DISPONIBILIDAD			
Concepto por el cual se asegura que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sean requeridos.			
VALOR	CLASIFICACIÓN	DEFINICIÓN	CONSECUENCIA
3	Alta	La no disponibilidad del activo de información puede conllevar a un impacto negativo de índole legal o económica, retrasando sus funciones, o generar pérdidas de imagen severas, impactando negativamente en la continuidad del negocio. Debe estar disponible siempre (100%).	La falta de disponibilidad por periodos prolongados produce: - Podría impedir la ejecución prolongada de las actividades administrativas y operativas en la Institución. - Incremento del costo por horas extras del personal que no puede ser asumido por la institución. - Impacto Negativo de índole Legal.
2	Media	La falta del activo de información impacta negativamente de manera importante al proceso. Debe estar disponible al menos el 50% del tiempo.	La falta de disponibilidad produce: - Podría ocasionar un perjuicio significativo en las actividades administrativas y operativas involucradas en la Institución. - Incremento del costo por horas extras del personal que puede ser asumido por la institución.
1	Baja	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen. Debe estar disponible al menos el 10% del tiempo.	La falta de disponibilidad produce: - No afectaría las actividad administrativas u operativas de la Institución

Tabla 5: Valoración de Disponibilidad

CRITERIO DE VALORIZACIÓN: INTEGRIDAD			
Concepto por el cual se salvaguarda la exactitud y totalidad de la información, tanto en su procesamiento, transmisión y almacenamiento.			
Valor	**Clasificación**	**Definición**	**Consecuencia**
3	Alta	Información o recurso cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a la institución. Tiene que estar correcto y completo en un 100%.	La falta de integridad produce daño de gran magnitud los que se puede expresar como: - Incumplimiento de las metas de la Institución, lo cual generaría un incremento considerable en el presupuesto de la institución. - Problemas en la coordinación entre diferentes procesos que resultarían en errores graves por el problema de integridad en algunos de los procesos; por ejemplo, cuando el proceso "B" debe ejecutarse siempre después del proceso "A" y "B" se ejecuta antes por error. - Pérdida de la confianza de los usuarios en la Institución.
2	Media	La pérdida de exactitud y estado completo del activo de información o recurso impacta negativamente de manera importante al proceso. Tiene que estar correcto y completo al menos en un 50%.	La falta de integridad produce daño de mediana magnitud que se puede expresar como: - Incumplimiento de las metas de las áreas involucradas, lo cual generaría un incremento de menor escala en el presupuesto de la institución. - Problemas en la coordinación entre diferentes procesos que resultan en errores de mediana magnitud por problema de integridad de algunos de los procesos. - Pérdida de la confianza de los usuarios.

1	Baja	Información o recurso cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la institución o entes externos. No es relevante los errores que tenga o la información faltante.	La falta de integridad produce daño de pequeña magnitud que se puede expresar como: - No impacta en el cumplimiento de las metas ni en las ganancias de la institución. - incapacidad de ejecución en los procesos en un periodo de tiempo pero este es manejable por la institución - No genera pérdida de la confianza en los usuarios.

Tabla 6: Valoración de Integridad

CRITERIO DE VALORIZACIÓN: CONFIDENCIALIDAD			
Concepto por el cual se asegura que la información es accedida sólo por las personas autorizadas para ello.			
Valor	Clasificación	Definición	Consecuencia
3	Alta	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente algunos negocios. Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas.	La divulgación no autorizada produce: - Impacto negativo de índole legal u operativa para la institución. - Impacto negativo de imagen o económica para la Institución
2	Media	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. Seria relevantes, el incidente implicaría a otras áreas.	La divulgación no autorizada produce: - Impacto negativo en los procesos involucrados para la Institución. - Impacto medianamente negativo de imagen o económica para la Institución - No se produce impacto de índole legal.
1	Baja	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera leve al proceso. Daños muy bajos, el incidente no trascendería del área afectada.	La divulgación no autorizada de la información no representa ningún perjuicio para la institución.

Tabla 7: Valoración de Confidencialidad

✓ **Actividad 2: Análisis de Amenazas**

En esta actividad se identifica las amenazas a los activos de información de la institución ODEI Lambayeque que pueden ocasionar problemas de seguridad, las amenazas son estandarizadas por Magerit que las clasifican en cuatro grupos como son: Desastres naturales, de origen industrial, errores y fallos no intencionados y ataques intencionados. Dicho análisis se realizó haciendo uso de las diferentes técnicas como observación y entrevista y los resultados obtenidos tras la evaluación del riesgo, en cuanto amenazas sobre los activos, demuestran que los niveles de riesgo presentes son medio y alto. Las amenazas identificadas con un nivel alto de riesgo son:

- **Falla de Equipos:** Afecta a la disponibilidad, es decir la accesibilidad y utilización de la información cuando es requerida por la institución, esta amenaza surge cuando ha superado su ciclo de vida o no se le da el mantenimiento respectivo.
- **Malware:** afecta exactitud y completitud activos de información, es decir la integridad de la información que se encuentra almacenadas tanto en el servidor como en los equipos de los colaboradores, esta amenaza surge por no contar con un software antimalware.

- **Colaboradores desleales o insatisfechos:** afecta a la confidencialidad, e decir entregar los activos de información de la institución y ponerlas a disposición de terceras personas o entidades no autorizados. Esta amenaza se debe a mentalidad de los colaboradores por la falta de motivación o capacitación, además de no haber una adecuada política sobre seguridad de información.
- **Ingreso no autorizado del equipo:** afecta directamente a la integridad y confidencialidad de los activos de información de la institución, esta amenaza surge por no haber una adecuada directiva de control de acceso remoto, políticas de contraseñas seguras y una inadecuada gestión de los Firewall.
- **Pérdida o Manipulación de la información:** afecta directamente a la confidencialidad e integridad de los activos de información de la institución, estas amenazas surgen al no haber una adecuada política de almacenamiento y control de la información.

✓ **Actividad 3: Análisis de las salvaguardas**

Las salvaguardas planteadas han sido elegidas siguiendo los consejos de implantación del estándar NTP ISO/IEC 27001:2014, en esta actividad hemos reconocido las necesidades o falencias en el ámbito de la seguridad de los activos de información. Es importante mencionar que cada acción de protección tiene un costo, por lo que en cada caso se debe evaluar el valor de la información a proteger y los costos que implicaría la pérdida o el sufrimiento de un ataque, y en este sentido planificar las acciones pertinentes para la protección de tal información.

5.1.6.3 Proceso P3: Estimación Del Estado De Riesgo

Actividad realizada con el propósito de analizar los datos recopilados en las actividades anteriores y evaluar el estado de riesgo, donde se incluye la estimación de impacto, probabilidad y riesgo:

✓ **Actividad 1: Estimación Del Impacto y Probabilidad**

Esta actividad se determina el impacto del daño y la probabilidad de que se materializase sobre los activos de información de la institución ODEI Lambayeque. El objetivo fue cuantificar el grado de repercusión que pueda presentar cada activo dentro de las dimensiones de valoración detalladas en las actividades anteriores como son: Disponibilidad, Integridad, Confidencialidad, Amenazas y Vulnerabilidades. Los activos de información que obtiene un valor de nivel menor igual a Intermedios deberán ser reevaluados para mejorar o adaptar diferentes controles para su tratamiento, mientras que los de valor mayor o igual a Alta debe ser objeto de atención critica. A continuación, se presentan las tablas con las escalas de valoración de Impacto y Probabilidad:

VALORACIÓN DE IMPACTO	
VALOR	**CATEGORÍA**
1	Muy bajo
2	Bajo
3	Intermedio
4	Alto
5	Muy alto

Tabla 8: Valoración de Impacto

VALORACIÓN DE PROBABILIDAD	
VALOR	CATEGORÍA
1	Imposible
2	Poco probable
3	Viable
4	Probable
5	Muy probable

Tabla 9: Valoración de Probabilidad

✓ **Actividad 2: Estimación Del Riesgo**

En esta actividad se realiza la valoración cualitativa del riesgo, haciendo uso de la tabla de respuesta al riesgo, tomando como entradas el impacto y la probabilidad. Para la estimación del riesgo de los activos de la institución, se toman los valores de la probabilidad de cada vulnerabilidad y el impacto de cada amenaza. A Una vez que se haya valorizado la probabilidad e impacto de cada uno de los riesgos detectados, se realizará una multiplicación entre estos valores para conocer el valor del riesgo, dependiendo del valor hallado se conocerá el nivel del riesgo con la ayuda de la siguiente matriz de calor:

VALORIZACIÓN DEL RIESGO INHERENTE						
PROBABILIDAD	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
IMPACTO		**1**	**2**	**3**	**4**	**5**

Tabla 10: Valorización Del Riesgo Inherente

RANGOS DE NIVEL DE RIESGO		
1-4	**RIESGO BAJO**	Aquellos riesgos cuyo valor oscila entre 1 y 4. Riesgos inferiores, deben ser tratados con los procedimientos de rutina ya definidos en la organización
5-10	**RIESGO MEDIO**	Aquellos riesgos cuyo valor oscila entre 5 y 10. Riesgos inferiores, deben ser tratados con los procedimientos de rutina ya definidos en la organización. Es hasta este punto en el cual se define el Apetito de Riesgo de SERPOST, es decir, aquellos riesgos que no se encuentren en esta zona deberán ser tratados con ayuda de controles para minimizar su valor.
11-19	**RIESGO ALTO**	Aquellos riesgos cuyo valor oscila entre 11 y 19. Riesgos que deben ser tratados con procedimientos especiales con la ayuda de la implementación de algunos controles de seguridad, la Alta Dirección debe ser consciente de la existencia y tratamiento de estos riesgos.
20-25	**RIESGO EXTREMO**	Aquellos riesgos cuyo valor oscila entre 20 y 25. Riesgos que deben ser tratados de manera inmediata y con alta prioridad debido a lo que podría suceder si se materializa el riesgo, la Alta Dirección debe ser consciente de la existencia y tratamiento de estos riesgos.

Tabla 11: Rangos De Nivel De Riesgo

Habiéndose realizado la calificación de los controles y evaluando su nivel de incidencia en la mitigación de riesgos, si el riesgo inherente se ubica en una zona de riesgo que necesita tratamiento, el tratamiento de riesgos se debe realizar en base a las cuatro opciones que se describen a continuación:

RESPUESTA AL RIESGO		
1	**EVITAR**	Implica tomar medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resuelto de unos adecuados controles y acciones emprendidas.
2	**TRANSFERIR**	Implica reducir su efecto a través del traspaso de posibles impactos a otras organizaciones, como el caso de los seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra entidad.
3	**MITIGAR**	Implica tomar medidas encaminadas a disminuir tanto la probabilidad, como el impacto, a través de la optimización de los procedimientos y la implementación de controles eficientes, eficaces y efectivos.
4	**ACEPTAR**	Una vez el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el Comité de Seguridad de la información o de Riesgos, puede aceptar el riesgo residual (Riesgo Inherente)

Tabla 12: Respuesta de Riesgo

5.1.6.4 Interpretación De Los Resultados

Una vez analizada Matriz de Evaluación de Riesgo, realizado atreves de una valoración sobre la estimación de riesgos teniendo como entrada las necesidades y características de cada activo vistas en los puntos anteriores, se realiza la siguiente interpretación en base a los riesgos más importantes:

- ✓ No disponer de procedimientos técnicos estandarizados para realizar mantenimiento correctivo y preventivo al parque informático, ya que cada personal de soporte que ha laborado en la institución resuelve las incidencias según su experiencia.
- ✓ Inadecuado control de restricciones para el uso de dispositivos de almacenamiento de información (USB, Discos Duras Externos, DVS).
- ✓ No cuenta con controles efectivos para la asignación o desasignación de perfiles de usuario, así como ineficaces procedimientos para realizar el control de software instalados en el parque informático.
- ✓ Falta de conocimientos por parte de los colaboradores de la institución sobre políticas de seguridad en el manejo de contraseñas, así como una inexistente gestión de control de contraseñas.
- ✓ El cableado de red eléctrico y de red en la institución no está certificado por NTCSE (Norma Técnica de Calidad de los Servicios Eléctricos) y a nivel de red de datos CISCO. Así como una inexistente infraestructura de corriente continua.
- ✓ Aunque la institución lleva un control de ingreso y salida de información física (documentos, libros, informes) e información digital, estos controles presentan riesgos de confidencialidad, integridad y disponibilidad por lo tanto tendrán que implementarse controles más adecuados.

5.1.7 Plan de Tratamiento de Riesgo

El propósito del Plan de Tratamiento de Riesgos es definir exactamente quién va a implementar cada control, cuándo, con cuál presupuesto, etc.

Una vez realizado la etapa de "Análisis de Riesgos" y habiendo quedado expuesto los impactos y los riesgos a los que están expuestos la institución ODEI Lambayeque, en esta etapa es la que realmente donde definimos el rumbo de la institución, esto es posible ya que disponemos de la información para tomar decisiones conociendo que activos de la información queremos proteger. El detalle del **"Plan de Tratamiento de Riesgos"** elaborada para la institución se presenta es presentado en el Anexo 11 - INEISGSI08 - Plan de tratamiento del riesgo.

Plantilla del Plan de Tratamiento de Riesgo

A continuación, se presenta la plantilla del documento que será utilizado en el proyecto de investigación.

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO																	
ACTIVO	**RIESGO**	**Estrategia**	**Justificación**	**Detalle de Justificación**	**Controles NTP ISO/IEC 27001:2014**	**Tipo de Control**	**Frecuencia**	**Control de Documentación**	**Registros**	**Métricas / Indicadores**	**Mejora Continua**	**Impacto**	**Probabilidad**	**Riesgo Residual**	**Proyecto**	**Plan de Acción**	**Recursos**	**Responsable**

Tabla 13: Plantilla del Plan de Tratamiento de Riesgo

Proceso – Elaborar el Plan de Tratamiento de Riesgo

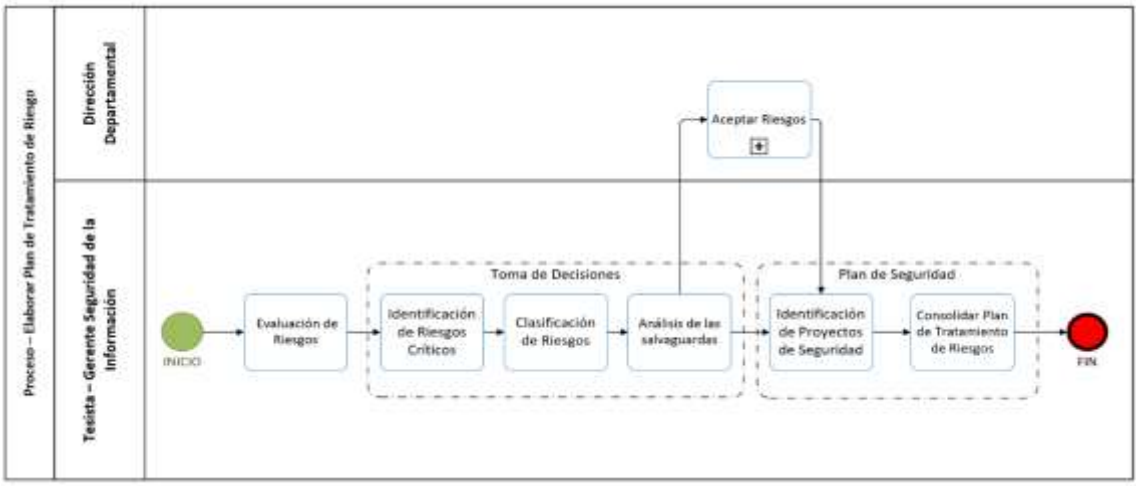


Tabla 14: Proceso – Elaborar el Plan de Tratamiento de Riesgo

Para realizar el plan de tratamiento de riesgos se realizaron los siguientes pasos:

5.1.7.1 Toma de Decisiones

✓ **Identificación de Riesgos Críticos**

Los activos de información siempre estarán expuestos a riesgos en toda empresa, lo importante es conocer cuáles serán los activos a quienes se les debe implementar controles o salvaguardas evitando así que las amenazas se materialicen. Basándonos en la norma NTP ISO/IEC 27001:2014, se realizó en la institución el análisis donde se identificaron los principales activos de información que son vulnerables, para en función de ellos elaborar un plan de seguridad apropiado que mitigue los riesgos. Es por ello que es necesario rectificar que los activos que poseen riesgos de nivel alto o extremo serán ponderados en la matriz de evaluación de riesgos con valores entre 11 y 25.

Una vez evaluado los activos de información y conocido el riesgo a los que están expuestos los mismos, se presenta la siguiente tabla con los activos que poseen un nivel de riesgo críticos y no tan críticos:

Riesgos de Nivel Alto o Extremo (11 - 25)

- Documentos de IPC
- Documento de Compendio Estadístico del Departamento
- Documento de Evolución de las Actividades de Producción
- Documento de Registro Nacional de Municipalidades
- Documento de Centro Documentario
- Información de Recursos Humanos
- Módulo contable
- Bandejas de correos electrónicos
- Contraseñas de correos electrónicos Institucional
- Escuela de Capacitación
- Información de Estadística
- Sistema IPC
- Sistema de Control Encomienda
- Servidor Data Center
- PCs de Escritorio
- PCs Portátiles
- Router
- Switch
- Cableado de red
- Discos Duros Externos
- Impresoras
- Cámaras de seguridad
- Local del ODEI Lambayeque
- Colaboradores(Excepto encuestadores y secretaria)

Riesgos de Nivel Bajo o Medio (1 - 10)

- Inventario de hardware
- Contraseñas del Sistema IPC
- Proyectores
- Hub
- DVDs
- Técnico en Estadística II
- Operador PAD III
- Encuestador y Secretaria

✓ **Clasificación de Riesgos**

En base a la clasificación de los activos de información mostrados anteriormente y enfocándonos en los de nivel alto o extremo, examinaremos el tipo de riesgo críticos a enfrentar. Los mismos se clasificarán en:

- **Riesgo de Integridad:** referido al procesamiento de la información en la institución, debiendo asegurar que la misma sea trasmitida correctamente. Ejemplo: que la información para generar el "Documento de Compendio Estadístico del Departamento" sea alterada.
- **Riesgo de Acceso:** se concentra en el incorrecto acceso a las aplicaciones, datos e información referente a la institución. Ejemplo: que terceros tengan acceso a la "Información de Estadística" que se genera en la institución.
- **Riesgo de Utilidad:** engloba las técnicas de recuperación/ restauración utilizadas para minimizar las rupturas los posesos y están contenidos los backups de información. Ejemplo: inoperatividad del equipo donde se guarda información crítica para la empresa.
- **Riesgo de Infraestructura:** Se refiere a que en la institución no existe una infraestructura tecnológica adecuada para desarrollar las funciones apropiadamente para el cumplimiento de los objetivos estratégicos. Ejemplo: ambiente inadecuado para la operatividad del servidor.
- **Riesgo de imagen:** Se refleja en un impacto de la materialización de cualquier tipo de riesgo, esto podría implicar presencia en cualquiera de las categorías de riesgo descritas anteriormente. Ejemplo: inoperatividad del centro de cómputo cancelando las capacitaciones.
- **Riesgo Legal:** Afecta la capacidad de la institución para dar cumplimiento a la legislación y obligaciones contractuales. Ejemplo: encriptación de la información contenida en el servidor de la institución.

5.1.7.2 Plan de Seguridad

Como siguiente paso y siguiendo la metodología Magerit[3] se describe como se desarrollara el plan de seguridad (PS) para la institución, en el que se identifican 3 tareas:

✓ **T1: Identificación de Proyectos de Seguridad**

En esta tarea tomando como base la fase de análisis de riesgos, se obtiene como resultado la lista de proyectos recomendados, dichos proyectos deberán ayudar a mitigar el riesgo inherente encontrado en la institución y permitir el progreso para el cumplimiento de la norma hasta los niveles apropiados. Se presenta la lista de proyectos propuestos con sus respectivas descripciones, dichos proyectos están basados en las 5 dimensiones que fueron definidas el

[3] Libro I: Método, capitulo 6

alcance del proyecto de investigación (Cultura organizacional, Recursos humanos, Control de accesos, Seguridad física y ambiental, Continuidad de negocio):

Nº	PROYECTOS	DESCRIPCIÓN
1	Aplicar encuestas de niveles de satisfacción para los trabajadores.	Elaborar encuestas y ejecutarlas al personal de la institución para medir los niveles de satisfacción y poder gestionar el sobretiempo o horas extras elaborando planes para su compensación.
2	Diseño e implementación de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como la seguridad del respaldo de los medios que contienen la información (física y virtual).
3	Establecer políticas de contraseñas robustas para sistemas informáticos y correos institucionales	Definir políticas, procedimientos e implementar mecanismos de seguridad para las cuentas y sistemas, además de capacitar al personal en la gestionar contraseñas fuertes. Definir contraseña para cada usuario(que no se comparta).
4	Implementar Controles de Impresiones	Implementar Software para Control de Impresión y Contador de Impresión (CZ Print Job Tracker 11).
5	Implementación de un Sistema Integrado de Gestión.	Implementar programas de auditoria para el adecuado tratamiento de la información en los sistemas y sus activos asociados y contratar servicios de Hackeo ético. Incluir en el programa la gestión de perfiles para un mejor control de las operaciones de sistemas de encomienda, permitiendo un tratamiento de la información correcto y uso aceptable de los activos.
6	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.
7	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética).
8	Plan de mantenimiento preventivo y correctivo de los equipos informáticos.	Elaborar plan para mantenimientos preventivos.
9	Elaborar e implementar controles de seguridad para el parque informático.	Implementar controles de seguridad para incrementar la seguridad de los activos de información críticos.
10	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Plan para la adquisición e instalación de antivirus y Antimalware. Así como la adquisición de Actualizaciones del Sistema Operativo (Parches). Además realizar y ejecutar planes para mantenimientos preventivos. Mejorar la infraestructura tecnológica para capacitaciones
11	Plan para la adquisición de licencias antivirus y antimalware de estaciones de trabajo y servidor institucional	Plan para la adquisición e instalación de antivirus y antimalware. Así como la instalación de Actualizaciones del Sistema Operativo (Parches).
12	Revisión y clasificación de soportes de información	Adquisición de discos duros externos de respaldo. Revisión de discos duros externos

Tabla 15: Identificación de Proyectos de Seguridad

✓ **T2: Plan de Ejecución**

Esta tarea tiene como objetivo principal ordenar temporalmente los programas de seguridad planteados, aplicando en primera instancia las salvaguardas con prioridad mayor y luego las salvaguardas con niveles superiores. Se deberá tener en cuenta los siguientes factores para dar ejecución a cada uno de los proyectos planteados:

- La criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, teniendo máxima prioridad los proyectos que afronten situaciones críticas.
- El costo del proyecto.
- La disponibilidad del personal propio para responsabilizarse de la dirección (y, en su caso, ejecución) de las tareas programadas.

- Otros factores como puede ser la elaboración del presupuesto anual de la Institución, las relaciones con otras organizaciones, la evolución del marco legal, reglamentario o contractual entre otros.

A partir de esta Tarea en adelante, incluyendo desde la fase Monitorear (DO) hasta la fase de Planear(Actuar) del modelo PDCA, será llevado a cabo por la institución ODEI Lambayeque ejecutar y monitorear el plan de tratamiento de riesgo propuesto.

✓ **T3: Ejecución del Plan**

El principal objetivo de esta tarea es alcanzar los objetivos del plan de seguridad para cada proyecto planificado, esto se alcanzará cuando se ejecute las siguientes tareas:

- Implementación de las salvaguardas.
- Mapa de riesgo actualizado.
- Estado de riesgo actualizado.

Pero dicha etapa será llevada a cabo por la institución ODEI Lambayeque.

5.2 MONITOREAR (DO)

Esta etapa del modelo PDCA, es la etapa donde la institución ODEI de Lambayeque deberá implementar y poner en funcionamiento el SGSI, poniendo en práctica las políticas y los controles que de acuerdo al análisis de riesgos se han seleccionado para su cumplimiento. Para ello deberá disponer de procedimientos en los que se identifique claramente quien debe que hacer cada tarea previa capacitación para ello.

Para ello debe cumplirse con los siguientes objetivos:

5.2.1 Aplicación de estándares y procedimientos de seguridad

En esta actividad se tendrá que elaborar y aplicar los estándares de Seguridad de la Información definidos dentro del alcance del SGSI, y una línea base para la Organización, así como los procedimientos correspondientes y complementarios a esos estándares.

5.2.2 Implementación de controles.

Una vez realizado el alcance, políticas, resultado de la evaluación de riesgos (Alto nivel y detallado), declaración de aplicabilidad y plan de tratamiento de riesgo, la siguiente accione es la implementación de cada control, correspondiente a un objetivo de control, debiendo de analizarse como mini-proyecto en el sentido de su estrategia de implementación. Dependiendo de la dimensión del Control, tendrá documentación específica de su fase conceptual y de diseño y por otro lado un nivel más detallado respecto a su implementación concreta con las actividades y aspectos técnicos, instrumentación, planes de capacitación, asesorías, etc. Por todo lo anterior, es conveniente formular un Plan de Implementación de Controles, a los efectos de estimar recursos y tiempo que deberá ser aprobado por la Dirección Departamental. Es por ello habiendo mencionamos en el inicio de nuestro caso de estudio, que dicha investigación se basaría en la propuesta de un SGSI, queda como responsabilidad de la institución ODEI Lambayeque realizar la implementación del SGSI.

Pero como recomendación para la implementación del SGSI, mencionamos que los controles que contienen niveles no tolerables por la institución, deben tener prioridad de implementación para su mitigación, los activos que tiene un riesgo muy elevado son los siguientes:

✓ **A.5 Las Políticas De Seguridad:** afectan a los activos de tipo personal, entre ellos tenemos Director Departamental, Jefe Dirección Ejecutiva de Difusión Estadística, Dirección Ejecutiva de Producción Estadística, Jefe de O.T. de Administración y Jefe de O.T. de Informática.

✓ **A.6 Aspectos Organizativos De La Seguridad De La Información:** afecta al activo de Centro Documentario (documento).

- ✓ **A.7 Seguridad Ligada A Los Recursos Humanos:** afecta a los activos Compendio Estadístico del Departamento (documento), Evolución de las Actividades de Producción (documento) y Sistema IPC (Aplicación), así como al Coordinador de Proyectos (personal).
- ✓ **A.11 Seguridad Física Y Ambiental:** afecta a los activos Registro Nacional de Municipalidades (Documento), Contraseñas de correos electrónicos Institucional (calves criptográficas) y Cámaras de seguridad (Equipo).
- ✓ **A.12 Seguridad en las Operaciones:** afecta al activo Data Center (servidor).

Es por ello, que en la implementación del SGSI, se tiene que dar prioridad a los siguientes controles:

ID	Controles NTP ISO/IEC 27001:2014	Porcentaje de Cumplimiento	Responsables	Método de Implementación
A.5	**POLÍTICAS DE SEGURIDAD**			
A.5.1	**Directrices de la Dirección en seguridad de la información**			
A.5.1.1	Conjunto de políticas para la seguridad de la información	Menos 10%	CIO / Director de seguridad de la información.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**			
A.6.1	**Organización interna.**			
A.6.1.1	Asignación de responsabilidades para la seguridad de la información.	20%	Encargado de soporte. Especialista en seguridad de información.	Se implementaran (por primera vez) programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**			
A.7.2	**Durante la contratación.**			
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	40%	CIO / Director de seguridad de la información.	Las normas utilizadas para el cumplimiento de los controles presentes son insuficientes, por tal razón se han formalizaran políticas para capacitación al personal
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL.**			
A.11.1	**Áreas seguras.**			
A.11.1.3	Seguridad de oficinas, despachos y recursos.	30%	Director de seguridad de la información	Se implementara formalmente, políticas de controles de Acceso y de áreas seguras.
A.11.1	**Seguridad de los equipos**			
A.11.2.2	Instalaciones de suministro	30%	CIO	Se implementaran plan de mantenimiento y ejecución de respaldos de configuración de equipo
A.11.2.4	Mantenimiento de los equipos	30%	CIO / Director de seguridad de la información	Se Implementara (por primera vez) controles de seguridad para incrementar la seguridad de los activos de información críticos.
A.12	**SEGURIDAD EN LAS OPERACIONES**			
A.12.2	**Protección contra código malicioso**			
A.12.2.1	Controles contra el código malicioso.	Menos 10%	CIO	Se implementaran controles para la adquisición de licencias antivirus y antimalware de puesto de trabajo y servidor institucional

Tabla 16: Priorización de Controles

Elaboración de Políticas y Procedimientos De Seguridad

A continuación, se describirá en que consiste cada uno de los controles a implementar, descritos en el punto anterior:

✓ **Política de Seguridad de la Información**

Esta política tiene por objetivo proporcionar las reglas y lineamientos básicos para la gestión de la seguridad de información, se aplica a todo el alcance del SGSI y sus usuarios son todos los colaboradores del servicio. En la actualidad el activo más importante de la institución es la información del Documento de Compendio Estadístico del Departamento y Documento de Evolución de las Actividades de Producción, por este motivo se está en la obligación de precautelar su confidencialidad, integridad y disponibilidad, para mantener la confiabilidad y reputación frente a sus usuarios. La Política de la Seguridad de la Información provee reglas generales de seguridad, para regular controles de accesos (privilegios y bitácoras) a las áreas seguras, de esta manera se mantenga un nivel adecuado de seguridad de los activos de información; esta política debe ser cumplida por el personal interno como terceros. Los principales responsables para monitorear el cumplimiento de estas políticas son:

- CIO (Oficial de la Información)
- Director de seguridad de la información.

✓ **Política de Organización de la Seguridad de la Información**

Esta política tiene por objetivo proporcionar los lineamientos necesarios para la utilización de los activos y recursos de procesamiento de información en el servicio, se aplica a todo el alcance del SGSI y sus usuarios son todos los colaboradores de la institución, haciéndolos parte de la cultura de la institución. Realizando programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan (físico y virtual). Los principales responsables para monitorear el cumplimiento de estas políticas son:

- Encargado de soporte.
- Especialista en seguridad de información.

✓ **Política de Seguridad de Recursos Humanos**

Estas políticas tienen por objetivo definir las responsabilidades y reglas para para mantener un alto grado de confidencialidad, integridad y disponibilidad de la información, mediante el control de los recursos humanos involucrados en el servicio que brinda la institución; se aplican a todo el alcance del SGSI y sus usuarios son todos los trabajadores de la Institución. La institución deberá elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución como seminarios de ética.

Los principales responsables para monitorear el cumplimiento de estas políticas son:

- CIO (Oficial de la Información)
- Director de seguridad de la información

✓ **Política de Seguridad Física y Ambiental**

Esta política tiene por objetivo proporcionar las reglas para la seguridad física y ambiental en el servicio, se aplica a todo el alcance del SGSI y sus usuarios son todos los trabajadores del mismo. Implementando formalmente, políticas de controles de Acceso y de áreas seguras y un plan de mantenimiento y ejecución de respaldos de configuración de equipo. Los responsables del monitoreo y mantenimiento de estas políticas son:

- CIO (Oficial de la Información)
- Director de seguridad de la información

✓ **Seguridad en las Operaciones**

Esta política tiene por objetivo garantizar el funcionamiento adecuado de los activos y sistemas de procesamiento de información para su mantenimiento seguro, se aplica a todo el alcance del SGSI y sus usuarios son todos los colaboradores del servicio. Se implementarán controles para la adquisición de licencias antivirus y antimalware para los puestos de trabajo y el servidor institucional. Los responsables de monitorear el cumplimiento y resultados de la aplicación de estas políticas son:

- CIO (Oficial de la Información)

5.2.3 Implementación de un programa de gestión de incidentes.

Es fundamental implementar un Programa de entrenamiento o Plan de Capacitación, logrando así la concienciación del colaborador, en todos los niveles y con alcance a toda la institución ODEI Lambayeque (o todo el personal dentro del alcance del SGSI definido); a los efectos de:

- ✓ Evitar rechazo o aversión a los nuevos controles.
- ✓ Entender la importancia de la seguridad de la información, conocer los objetivos y prioridades y las consecuencias que tendría no lograr los niveles de seguridad adecuados / requeridos.
- ✓ Lograr el compromiso y la alineación al SGSI del personal, evitando fallas por falta de comprensión, mala comunicación, negligencia, etc.
- ✓ Capacitar al personal para que estén preparados a nivel conceptual y práctico para la implementación del SGSI en función de sus responsabilidades y sus actividades operativas.
- ✓ Facilitar la adopción e implementación del SGSI y su adecuación con los planes operativos y eventualmente otros planes de Gestión.
- ✓ Conocer los requerimientos de seguridad de la información no sólo a la interna de la empresa sino al momento de interactuar con terceros, y eventualmente incluir esos requerimientos en cláusulas contractuales.

5.2.4 Gestión de recursos para el SGSI.

Para implantar y mantener un SGSI requiere de recursos humanos, tecnológicos y sobre todo económicos. Para ello debe analizarse como un proyecto, con diferentes objetivos e hitos a cumplir en el corto, mediano y largo plazo. Comprendimos que es preciso que el SGSI esté alineado con los objetivos del negocio, por lo tanto, no deben minimizarse las necesidades y requerimientos de seguridad de información, ni las actividades o tareas y recursos necesarios para alcanzarlos.

Es por ello que, que se presenta el siguiente diagrama de Gantt, donde los 12 proyectos identificados en el Plan de Tratamiento de Riesgos, se planifican en 5 actividades formadas por equipos para su implementación. A continuación:

- **Equipo 01:** se desarrolla el proyecto 02 y proyecto 12

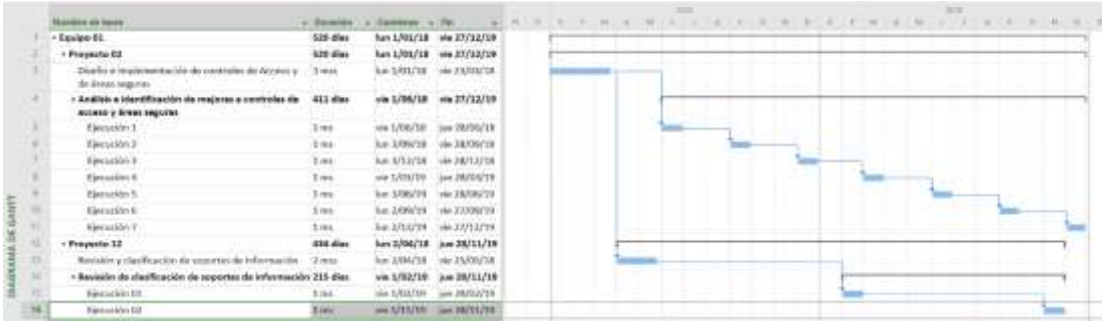


Imagen 9: Diagrama de Gantt - Equipo 01

- **Equipo 02:** se desarrolla el proyecto 03 y proyecto 07

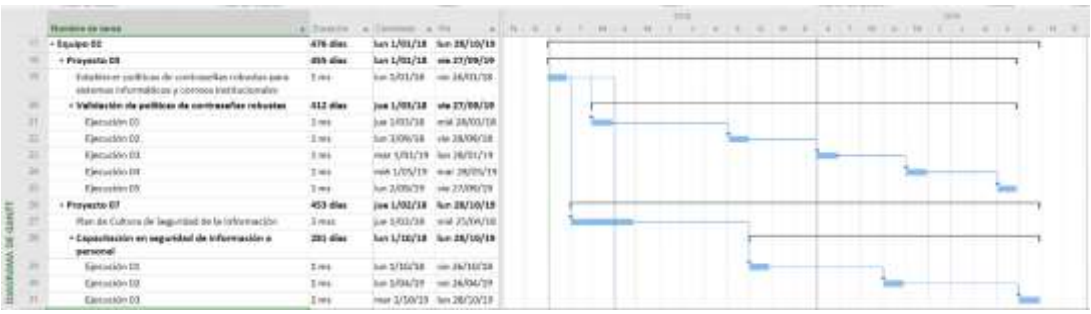


Imagen 10: Diagrama de Gantt - Equipo 02

- **Equipo 03:** se desarrolla el proyecto 10, proyecto 11 y proyecto 08.

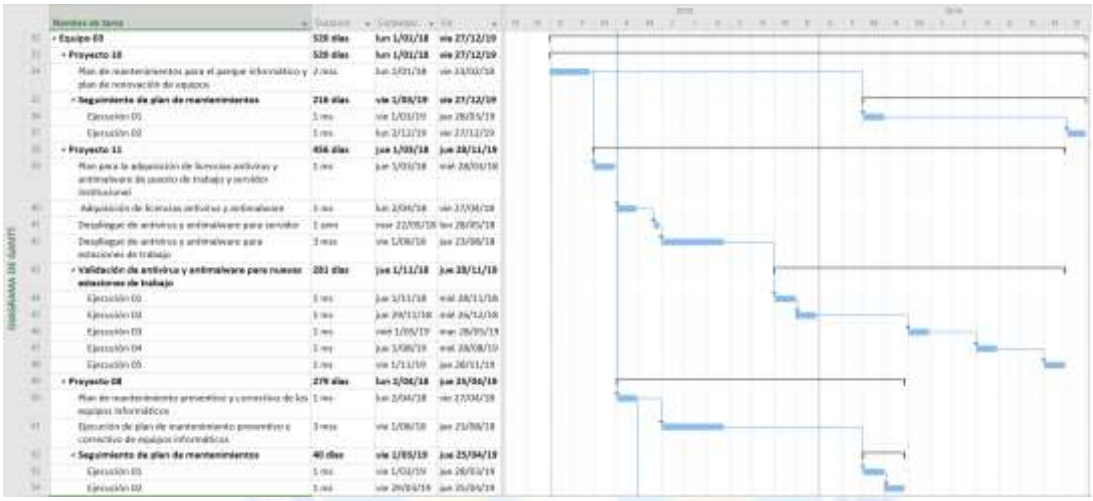


Imagen 11: Diagrama de Gantt - Equipo 03

- **Equipo 04:** se desarrolla el proyecto 05.

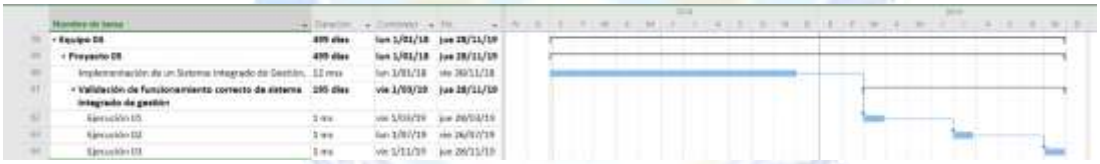


Imagen 12: Diagrama de Gantt - Equipo 04

- **Equipo 05:** se desarrolla el proyecto 09.

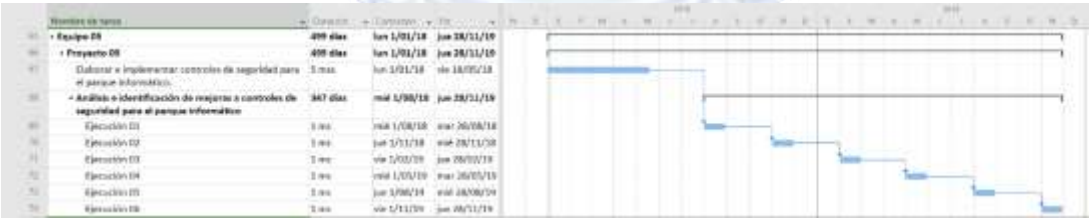


Imagen 13: Diagrama de Gantt - Equipo 05

- **Equipo 06:** se desarrolla el proyecto 06 y proyecto 01

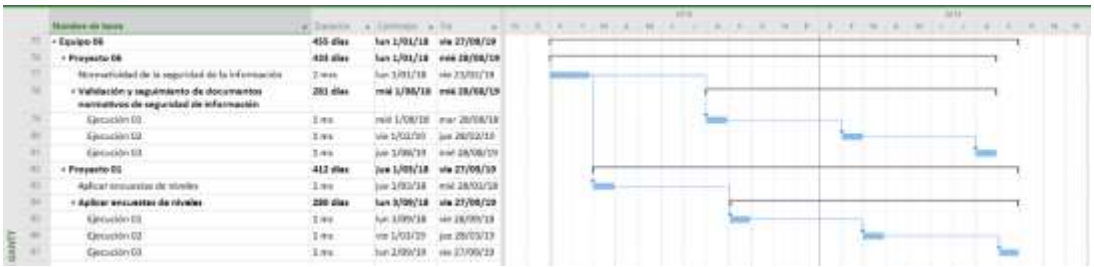


Imagen 14: Diagrama de Gantt - Equipo 06

Información General del Proyecto para su implantación:

RESUMEN DE LA IMPLEMENTACIÓN	
FECHA INICIO :	1/01/2018
FECHA FINAL :	27/12/2019
DURACIÓN :	520 días
TRABAJO :	10,226.00 horas
COSTO :	S/.237,733.45

Tabla 17: Resumen Implementación SGSI

Para mayor detalle de este punto ver el Anexo 12 – Plan de Gestión de Recursos

5.3 MEJORAR (CHECK)

En esta fase, la institución deberá planificar y llevar a cabo las actividades que permitan la monitorización y revisión, permitiendo así evaluar la efectividad y eficiencia del SGSI propuesto, específicamente controlar que los procesos se ejecuten de la manera prevista permitiendo así alcanzar los objetivos planteados en las fases anteriores. A medida que el proyecto avance, va a ver un conjunto de desviaciones, un conjunto de alteraciones en la información del proyecto respecto a cómo se había planificado en un principio. El objetivo de esta etapa será justamente detectar las posibles desviaciones entre los controles que la institución estaría implementando y los controles planificados, cuando más certero sea esta etapa de seguimiento, más rápido podrán ser implantadas las medidas correctoras que podamos llevar a cabo, para corregir ciertas desviaciones en el proyecto. Basándonos en la norma NTP ISO/IEC 27001:2014, esta etapa de monitorización debe realizarse de forma periódica y sus resultados debe ser verificables y reproducibles. Para realizar esta etapa, la institución deberá realizar 4 actividades principales, las cuales son:

5.3.1 Monitoreo

En esta actividad la institución al realizar el monitoreo, podrá observar las variaciones entre el estado de seguridad de ODEI Lambayeque y el estado que se pretende alcanzar, el objetivo es recabar y recolectar datos exactos que permitan establecer el estado real de la seguridad de la información. La institución en esta actividad deberá generar y resguardar los registros de actividad de monitorización generando así un informe para la dirección departamental que sintetice el resultado de esta actividad, así como la de generar un informe con las recomendaciones técnicas en función de los resultaos obtenidos, informe de costos / beneficio sirviendo como apoyo para la toma de decisiones en cuanto a la seguridad de la información.

5.3.2 Métricas

Esta actividad la institución deberá evaluar la efectividad de los controles y también medir la efectividad de cumplimiento del SGSI. Cuando el SGSI propuesto en la fase de planificación sea implementado, la institución deberá analizar si los controles establecidos, no logran los niveles requeridos ya que pueden existir deficiencias o fallas tanto en la fase de planificación y diseño como en la implementación y operación, es por ello que es necesario contar con un conjunto de métricas que permitan levantar un llamado de atención, una alerta en el caso que en la elección de controles o bien en su implementación requieran reajustes o reconsideración.

Para cada control debe establecerse uno o más métricas a los efectos de conocer el grado de satisfacción del objetivo. Una vez conocido este grado, debe ser posible saber de forma concreta si el objetivo fue alcanzado o, dicho de otra manera, si ese grado de seguridad es suficiente o se requieren reajustes.

Para el correcto seguimiento de todo el proceso de incidentes, es necesaria la aplicación de métricas que permitan evaluar de la forma más objetiva posible el funcionamiento del servicio en la Institución ODEI Lambayeque. Algunos de los aspectos clave a considerar son:

NOMBRE DE MÉTRICA	DESCRIPCIÓN
Promedio de tiempo para la resolución de incidentes de prioridad X	Mide el tiempo para la resolución de incidentes con una prioridad específica.
Promedio de tiempo de respuesta para incidentes de prioridad X	Mide el tiempo medio para responder a incidentes con una prioridad específica.
Porcentaje de incidentes escalados	Número de incidentes atendidos por escalonamiento.
Tiempos de resolución clasificados en función de la urgencia impacto de los incidentes.	Se Evaluará: **Urgencia** ¿Con qué rapidez se debe resolver el incidente? **Impacto** ¿Cuánto daño causará si no se soluciona rápido el incidente?
Número total de incidentes cerrados	Cuenta el número de incidentes que se cerraron durante el período de cálculo. Esto mide la eficiencia del servicio de TI.
Número total de incidentes en proceso	Cuenta el número de incidentes que se procesaron durante el período de monitoreo. Esto mide la eficiencia del servicio de asistencia.

Tabla 18: Métricas

5.3.3 Auditorías Internas del SGSI

El estándar NTP ISO/IEC 27001:2014, establece que deben realizarse auditorías internas a intervalos planificados para determinar si los objetivos de control, controles, procesos y procedimientos cumplen:

- ✓ Los requisitos de la norma, la legislación y reglamentaciones
- ✓ Los requisitos identificados de la seguridad de la información.
- ✓ Los controles están implementados y se mantienen de forma eficaz
- ✓ Se desempeñan de acuerdo a lo esperado (eficiencia).

Para ello la institución deberá documentar, los criterios, el alcance, la frecuencia y los métodos que se llevarán a cabo.

5.3.4 Revisión

Esta etapa de revisión, la institución deberá realizarla de forma periódica y planificada, y tiene como objetivos: Evaluar la efectividad del SGSI propuesto.

- ✓ Evaluar los recursos asignados al SGSI.
- ✓ Analizar los riesgos residuales.
- ✓ Actualizar los planes de seguridad.

Se recomienda generar un informe que detalle las mejoras para hacer al SGSI para hacerlo más efectivo, presentar un informe de costo / beneficio que permita a la dirección departamental tomar las decisiones gerenciales con respecto a seguridad de información, así como una redefinición o reajuste del SGSI adaptándolo a nuevos cambios para el cumplimiento de los objetivos de controles trazados.

5.4 PLANEAR (ACTUAR)

De acuerdo a la norma NTP ISO/IEC 27001:2014 en esta etapa se debe, en función de toda la información recabada en las etapas de monitoreo, métricas y revisión del SGSI, la institución deberá adoptar las decisiones y redefiniciones necesarias para corregir los aspectos y controles que no estén logrando la efectividad esperada y replantearse el acierto o no de los controles planteados, así como la vigencia de los objetivos de control.

Es así que en esta etapa deberá tenerse en cuenta:

- ✓ Identificar no conformidades del SGSI y tomar conocimiento.
- ✓ Definir acciones correctivas y preventivas.
- ✓ Evaluar sugerencias y definir la implementación de mejoras.
- ✓ Revisar el plan de mejora continua.
- ✓ Obtener el "ok" de la Dirección Departamental si es necesario de los cambios propuestos.
- ✓ Obtener los recursos para llevarlos a cabo.
- ✓ Comunicar estos cambios y mejoras.
- ✓ Monitorear la implementación de estos cambios.

Algunos de estos cambios y mejoras, podrá trascender al alcance del SGSI en cuestión y por ello, podrá ameritar la aprobación, tanto en la obtención de recursos necesarios como las etapas de avance y ejecución de los mismos. En este caso corresponderá, informar de estas mejoras propuestas y requeridas a la Dirección Departamental del instituto ODEI Lambayeque y a la correspondiente Gerencia de la Seguridad de la Información para su planificación conjunta.

- ✓ **ENTRADA:**
  - Informes de Auditoría interna.
  - Informes de no conformidades de la empresa, que estén dentro del alcance del SGSI en cuestión.
  - Informes de conclusiones y sugerencias surgidos de la etapa de revisión.
  - Propuestas de mejoras de otras áreas y unidades de negocios.

- ✓ **QUIENES DEBERÍAN PARTICIPAR:**
  - Equipo de Planeamiento de la Seguridad de la información: responsable de sugerir las mejoras que pueden obtenerse y estimar los recursos que serían necesarios.
  - Comité de Seguridad: a los efectos de aprobar el plan tentativo o dar lineamientos más generales.
  - Alta Gerencia y Dirección: en caso de ser los cambios propuestos de un impacto considerable o requerir presupuesto adicional al ya otorgado al área.
  - Gerencia de la Seguridad de la Información: en el caso de tratarse de no conformidades provenientes de su propio SGSI o cambios compartidos que deben ser implementados en conjunto.
  - Eventualmente en caso de entenderse necesario, debido a la diferencia entre el estado de seguridad percibido y el que se quiere lograr, podría participar una Consultoría externa con personal especializado en el área.

  Los planes de mejoras deberán ser coordinados para su instrumentación con las áreas afectadas, de forma de interferir lo menos posible en su operativa diaria, al menos de forma no prevista a los efectos de evitar molestias o interferencias no deseadas. La comunicación de las mejoras propuestas debe hacerse a los efectos de permitir un ámbito donde se reciban propuestas y en la medida de lo posible que el área afectada sea también parte integrante y responsable de las mejoras.

- ✓ **ACCIÓN:**

  De acuerdo a la NTP ISO/IEC 27001:2014 se deben realizar las siguientes actividades:

  - Identificación de no conformidades.

- Identificación de acciones correctivas y preventivas.
- Implementación de las mejoras.
- Testeo del logro de las mejoras esperadas.
- Monitoreo.
- Comunicación de los cambios y las mejoras.

✓ **SALIDA:**

Un Informe con el plan de mejoras, describiendo o referenciando las conclusiones más relevantes surgidas de la etapa de revisión y especificando objetivos concretos, el impacto de los cambios y quienes estarían involucrados, así como un plan tentativo para llevarlos a cabo.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6 CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

Un sistema de gestión de seguridad de información apoya a las organizaciones en la dirección, operación y control de forma sistemática y transparente de sus procesos, a fin de lograr con éxito sus actividades, ya que está diseñado para mejorar continuamente el desempeño de la organización, mediante la consideración de las necesidades de todas las partes interesadas.

La propuesta del SGSI ha sido diseñada para la Oficina Departamental de Estadística e Informática del Departamento de Lambayeque centrando la investigación en las áreas de "Dirección Ejecutiva de Producción Estadística" y "Dirección Ejecutiva de Difusión Estadística", los conceptos relacionados a la gestión del riesgo frente a la seguridad de la información y su importancia fueron descritos en el presente proyecto; así como también la de conocer los estándares y metodologías que permiten el desarrollo del análisis de riesgo para una institución.

La norma NTP ISO/IEC 27001:2014 es una solución al problema ante la ausencia gestión de seguridad de la información en ODEI Lambayeque, ya que es una metodología basada en el estándar internacional ISO/IEC 27001:2013; permitiendo implementar un sistema de gestión en la institución con el objetivo de establecer y mantener un ambiente razonablemente seguro para poder fortalecer las salvaguardas en cuanto a confidencialidad, integridad y disponibilidad de los activos de información, así como fortalecer el monitoreo en los procesos CORE de la institución.

La metodología PDCA (planificar, hacer, verificar y actuar) es la utilizada en nuestro caso de estudio como parte de la autoevaluación a la institución, ya que es un modelo muy conocido para la mejora continua de los procesos, permitiéndonos realizar un análisis con el fin de identificar los principales problemas como el uso de sus recursos, colaboradores y la información que en ella se opera.

Para el análisis de riesgo en el caso de estudios elaborado se aplicó la metodología MAGERIT, permitiéndonos conocer las amenazas a las cuales se encuentra expuestas los activos de información en ODEI Lambayeque, esto después de un análisis de riesgos de orden cuantitativo en el cual se concluyó que el nivel de madurez en cuanto a seguridad de la información en la institución era muy bajo.

Finalmente, si bien la Dirección Departamental de ODEI Lambayeque se encargará de revisar y analizar el SGSI propuesto, observara que el objetivo del proyecto, ayudará a la institución a reconocer la necesidad de implementar un plan de gestión de riesgos que permita mitigar los riesgos más críticos, considerando que para desarrollo del Plan de Tratamiento de Riesgo deberá contratar personal especializado en seguridad, análisis de documentos y registros de incidentes.

6.2 RECOMENDACIONES Y TRABAJO FUTUROS

El alto grado de exigencia en cuanto a la eficiencia, fiabilidad, rapidez y trazabilidad que demandan las actividades propias de ODEI Lambayeque, hace de la gestión de la seguridad de la información sea un elemento fundamental para el desarrollo dela institución, es por ello, que como apoyo para lograr la mejora continua se recomienda la implementación del SGSI propuesto y que, al no poseer con la experiencia de implementación en sistemas de gestión, logren adquirir servicios de consultoría que puedan guiarla a una implementación exitosa de la norma.

Una vez que la Dirección Departamental aprueba la implementación del SGSI, se recomienda el desarrollado del Plan de Tratamiento de Riesgos propuesto en este proyecto, que consta de políticas permitiendo así mitigar los riesgos dentro de la institución gracias a las salvaguardas sugeridas, pero cada una de ellas tiene un costo, por lo que, en cada caso deberá evaluarse el valor del activo de información a proteger, planificando así las acciones pertinentes a tomar para su resguardo.

Si bien la Dirección Departamental de ODEI Lambayeque se encarga de revisar el SGSI propuesto, es necesario llevar una revisión permanente, es por ello que se recomienda capacitar a los colaboradores de área de computo en temas de seguridad de información, esto con el fin de que puedan apoyar realizando auditorias para detectar fisuras en cuanto seguridad referidas en la NTP ISO/IEC 27001:2014 y para establecer mejoras en el sistema. También se recomienda que el auditor del sistema que lidere el equipo de auditoria, no debe haber participado en la implementación del mismo, esto como una medida de mantener objetividad y la independencia entre ambos procesos.

Es necesario que Dirección Departamental asigne un presupuesto permanente orientado a la implementación y monitoreo de los controles del SGSI, así como para las capacitaciones y charlas de concientización a los colaboradores de a la institución, los servicios de consultoría y las revisiones periódicas que se darán para asegurar la continuidad del sistema.

Finalmente, y como opción a futuros trabajos, esta propuesta se podría extender adaptándolo o diseñando e implementando un nuevo sistema de gestión de continuidad del negocio, incluyendo los demás procesos que contiene la institución ODEI Lambayeque, debido a que no existe en la institución y sería motivo de observación continua por parte una auditoria externa.

BIBLIOGRAFÍA

7 BIBLIOGRAFÍA

Hernando Bonilla, M. (2013). LEY SOX – Lineamientos de control a considerar en eventos de corrupción, defraudación e irregularidades. *Marcontrol.audit*, 2-5. Obtenido de http://marcontrol.blogspot.pe/2013/06/ley-sox-lineamientos-de-control.html

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). : MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. En M. A. Amutio Gómez, J. Candau, & J. A. Mañas, *: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* (págs. 7-70). Madrid, España: Ministerio de Hacienda y Administraciones Públicas, Gobierno de España.

Baca, U. G. (2016). Introducción a la seguridad informática. En U. G. Baca, *Introducción a la seguridad informática.* (págs. 29-31). Distrito Federal, MÉXICO: Grupo Editorial Patria.

Bertolín, J. A. (2008). Seguridad de la Información. En A. B. Javier, *Seguridad de la Información* (págs. 2-10). España, Madrid: PARANINFO.

Burgos Salazar, J., & G. Campos, P. (10 de 10 de 2010). Modelo Para Seguridad de la Información en TIC. Concepción, Biobío, Chile.

Cano Martínez, J. J. (2016). Inseguridad de la información : una visión estratégica. En J. J. Cano Martínez, *Inseguridad de la información : una visión estratégica* (págs. 15-18). Alfaomega Grupo Editor.

Córsico, R., & Soledad, I. (2009). Trabajo de auditoría normas COBIT. En R. Córsico, & I. Soledad, *Trabajo de auditoría normas COBIT* (págs. 5-6). Córdoba: AR: El Cid Editor.

El Peruano. (14 de 01 de 2016). Presidencia del Consejo de Ministros. Resolución Ministerial Nº 004-2016-PCM - Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. 2a. Edición". Normas Lega. *Norma Técnica Peruana "NTP ISO/IEC 27001:2014*, pág. 2.

Escrivá Gascó, G., Romero Serrano, R., & Ramada, D. (2017). Seguridad informática. En G. Escrivá Gascó, R. M. Romero Serrano, & D. J. Ramada, *Seguridad informática* (pág. 13). Madrid: ProQuest ebrary.

Gaona Vásquez, K. (17 de 10 de 2013). Aplicación De La Metodología Magerit Para El Análisis Y Gestión De Riesgos De La Seguridad De La Información Aplicado A La Empresa Pesquera E Industrial Bravito S.A. En La Ciudad De Machala. Cuenca, Azuay, Ecuador.

Gómez Fernández, L., & Fernández Rivero, P. P. (2015). Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. En L. Gómez Fernández, & P. P. Fernández Rivero, *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.* (págs. 11-12). España: AENOR.

Gómez Gómez, C. (27 de 09 de 2010). TRABAJO DE INVESTIGACION ASOCIADO A LA ASIGNATURA: AUDITORIA II. Manizales, Caldas, Colombia. Obtenido de https://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi81OaYxOjWAhUOlpAKHS9rBzMQFggoMAE&url=https%3A%2F

%2Fauditoiraunal20102.wikispaces.com%2Ffile%2Fview%2FT_ISO%2Bserie%2B27000ISO%2B17799_2010_2_906047.docx&usg=AOvV

Gómez, F. L., & Andrés, Á. A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. En F. L. Gómez, & Á. A. Andrés, *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* (págs. 13-16). Madrid: ES: AENOR - Asociación Española de Normalización y Certificación.

Guzmán, Á. (27 de 07 de 2012). ITIL v3 -Gestión de Servicios de TI. *Revista ECORFAN*, 803-805. Obtenido de ITIL v3 -Gestión de Servicios de TI: https://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi1r5y5sObWAhUHfpAKHTb9CFMQFggkMAA&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F4001967.pdf&usg=AOvVaw3Zb3FzrX-uhZTvufvGSGGP

INTECO - Instituto de Normas Técnicas de Costa Rica. (21 de 05 de 2002). SGSI - Conceptos Básicos sobre la Seguridad de la Información. *Conceptos Básicos sobre la Seguridad de la Información*. Costa Rica.

ISOTools Excellence. (01 de 05 de 2015). *Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Información: http://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

Morales, F. E. (01 de 01 de 2004). *La gestión y los gestores de la información. "Bibliodocencia". vol. 4, n. 4*. Obtenido de La gestión y los gestores de la información. "Bibliodocencia". vol. 4, n. 4: http://www.bibliodocencia.com/4/4_6.pdf

Nahum, F. (12 de 03 de 2016). *Red Global de Conocimientos en Auditorñía y Control Interno.* Obtenido de http://www.auditool.org/blog/control-interno/700-administracion-de-riesgos-conceptos-fundamentales-parte-1

Núñez Ponce, J. (01 de 03 de 2016). *julionunezderechoinformatico.blogspot.pe*. Obtenido de julionunezderechoinformatico.blogspot.pe: http://julionunezderechoinformatico.blogspot.pe/2016/01/norma-tecnica-de- gestion-de-seguridad.html

NÚÑEZ PONCE, J. (15 de 01 de 2016). *julionunezderechoinformatico.blogspot.pe*. Obtenido de julionunezderechoinformatico.blogspot.pe: http://julionunezderechoinformatico.blogspot.pe/2016/01/norma-tecnica-de-gestion-de-seguridad.html

Oficina Nacional de Gobierno Electrónico e Informática. (15 de 08 de 2017). *Perú Gobierno Digital.* Obtenido de Perú Gobierno Digital: http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

Real Academia Española. (La 23ª edición (2014)). *Diccionario de la lengua española | Edición del Tricentenario*. Obtenido de Diccionario de la lengua española | Edición del Tricentenario: http://www.rae.es/la-institucion/presentacion/informacion

ANEXOS

9 ANEXOS

9.1 ANEXO 01: Solicitud para Realizar Investigación

SOLICITUD: Permiso para realizar
Trabajo de Investigación

LIC. ROSA NIZAMA NACIMIENTO.
Directora Departamental INEI – Lambayeque

Presente. -

Yo, Nilton Rogger Niño Morante, identificado con D.N.I. 42535756, C.I.P. Nº 148385 y con domicilio en P.J. San Martin, Prolongación Miguel Grau Nº 1285 - Lambayeque. Ante Ud. Respetuosamente me presento y expongo lo siguiente:

Que, habiendo culminado mis estudios de maestría en la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo en Ingeniera de Sistemas con mención en Gerencia de TI y Gestión de Software, recurro a Ud. para **solicitar autorización para realizar un trabajo de investigación en la entidad,** respecto a un "Sistema de Gestión de la Seguridad de la Información – SGSI", a fin de complementar la formación recibida en la institución para finalmente optar el grado de Magister.

POR LO EXPUESTO:

Ruego a Ud. acceder a esta petición.

Chiclayo, 15 de enero de 2016

Nilton Rogger Niño Morante
DNI: 42535756

18 ENE 2016

9.2 ANEXO 02: Clasificación de los Activos

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Los datos son el combustible con el que opera una organización. La información es un activo abstracto que será almacenado en equipos o soportes de información y que puede ser transferido de un lugar a otro por los medios de transmisión de datos. Pertenecen a este grupo: ficheros, copias de respaldo, datos de configuración , datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad, código fuente, código ejecutable y datos de prueba.
[S] Servicios	Función que satisface una necesidad de los usuarios, como: Word Wide Web, acceso remoto a cuenta local , correo electrónico , almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, servicio de directorio, gestión de identidades , gestión de privilegios , PKI - infraestructura de clave pública.
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos, que han sido automatizadas para su desempeño por un equipo informático, entre ellos están: desarrollo propio , desarrollo a medida (subcontratado), estándar, navegador web, servidor de presentación, servidor de aplicaciones, cliente de correo electrónico, servidor de correo electrónico, servidor de ficheros , sistema de gestión de bases de datos, monitor transaccional, ofimática, anti virus, sistema operativo, gestor de máquinas virtuales, servidor de terminales, sistema de Backups.
[HW] Equipamiento informáticos (Hardware)	Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, entre ellos podemos identificar: agendas electrónicas , equipo virtual, equipamiento de respaldo, periféricos dispositivos criptográficos, dispositivo de frontera, soporte de la red, concentradores, conmutadores, encaminadores, firewall, punto de acceso inalámbrico, etc.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros. Medios de comunicación que tiene por objetivo transportar datos de un sitio a otro.
[Media] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o por largos periodos de tiempo. Ejemplo: CD-ROM, DVD, USB, Material Impreso.
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos; como: fuentes de alimentación, cableado, armarios, mobiliario, equipos de climatización.
[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones. Ejemplo: cuartos, edificios, instalaciones de respaldo.
[P] Personal	Personal relacionado con los sistemas de información; como: personal interno y externo, operadores, administradores de sistemas, desarrolladores de sistemas, contratistas y proveedores.
[SI] Sistema de Información	Conjunto de elementos interrelacionados que permiten la obtención, procesamiento, almacenamiento y distribución de la información para apoyar la toma de decisiones y el control en una organización.

Tabla 19: Clasificación de los activos

9.3 ANEXO 03: Procesos CORE

La ODEI Lambayeque es el órgano desconcentrado del INEI, responsable de promover, orientar, desarrollar y coordinar las acciones de capacitación e investigación en los campos de la estadística e informática y áreas afines en su Sede Departamental.

Los procesos de la institución tienen que responder ante la gerencia, los cuales reciben como salida un producto físico o servicio. Estos establecen las condiciones de satisfacción o declaran que el producto o servicio es aceptable o no. Se realizó el proceso de levantamiento de la información para proceder a identificar los procesos de la institución, los cuales son:

A. Área de Dirección Ejecutiva de Producción Estadística

- ✓ Gestión del Compendio Estadístico Departamental
- ✓ Gestión de la Evolución de las Actividades de Producción
- ✓ Gestión del Registro Nacional de Municipalidades

B. Área de Dirección Ejecutiva de Difusión Estadística

- ✓ Gestión del IPC (Índice del Precio Consumidor)
- ✓ Gestión del Centro Documentario

C. Área de Oficina de Proyectos (Censos y Encuestas)

- ✓ Proyecto ENAHO: Encuesta Nacional De Hogares
- ✓ Proyecto ENAPRES: Encuesta Nacional De Programas Estratégicos.
- ✓ Proyecto ENDES: Encuesta Demográfica Y Salud

D. Área de Oficina Técnica de Administración (O.T. de Administración)

- ✓ Gestión de Pagos
- ✓ Gestión de Presupuesto
- ✓ Gestión de Recursos Humanos
- ✓ Gestión de Contabilidad (Básica)

E. Área de Oficina Técnica de Informática (O.T. de Informática)

- ✓ Escuela de Capacitación
- ✓ Soporte Técnico

Se abarca la gestión de la seguridad de la información en los principales procesos del ODEI-Lambayeque los cuales son:

- ✓ **Proceso 01:** Generar el Compendio Estadístico del Departamento de Lambayeque.
- ✓ **Proceso 02:** Generar el Compendio de Evolución de las Actividades de Producción.
- ✓ **Proceso 03:** Generar el Registro Nacional de Municipalidades.
- ✓ **Proceso 04:** Generar el Índice de Precio Consumidor.

El detalle de cada proceso Core se detalle a continuación:

PROCESO 01: GENERAR EL COMPENDIO ESTADÍSTICO DEL DEPARTAMENTO DE LAMBAYEQUE

Este proceso se origina en el área de "Dirección Ejecutiva de Producción Estadística" el cual maneja información básica sectorial y el cual tiene una duración entre 5 a 6 meses para generarlo.

El proceso tiene una periodicidad anual y se origina cuando el área mencionada genera los formatos para ser completados con información administrativa por los diferentes sectores del departamento del Lambayeque tales como sector del Medio Ambiente, Población y Demografía, Educación y Cultura, Salud, Vivienda, Trabajo, Interior, Justicia, Desarrollo Social, Cuentas Departamentales, Agrícola, Turismo, Financiero y Finanzas Públicas, a continuación el área recopila toda la información completada en los formatos (física o email) e inicia el proceso de

validación el cual consiste en que los formatos sean completados adecuadamente según sus normas establecidas, una vez completado este paso, los datos obtenidos de los diferentes sectores pasan a ser digitalizados y ser tabulados para ser presentados como información estadística actualizada y detallada, dicha información contiene cuadros y gráficos estadísticos y su cobertura está referida al ámbito geográfico del departamento de Lambayeque. También, incluye series históricas de las variables más importantes que contribuirán al estudio y mejor comprensión de la realidad departamental en el mediano y largo plazo.

Toda la información es consolidad en un informe llamado "Compendio Estadístico del Departamento de Lambayeque" que será editado como un libro e impreso para la posterior venta al público en el centro documentario.

Para finalizar, los resultados del informe del departamento de Lambayeque se son enviados a la central del INEI, a través de los siguientes productos: base de datos, sistemas de información y publicaciones.

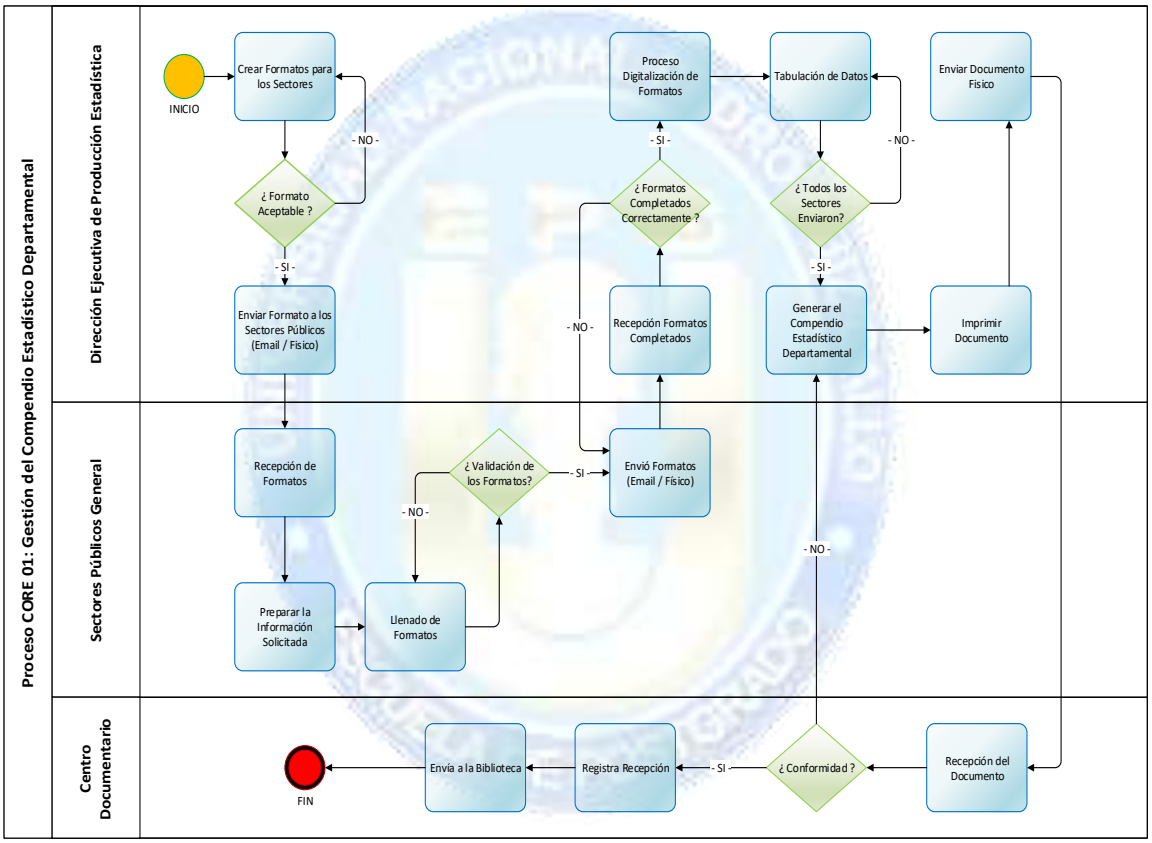


Imagen 15: Generar El Compendio Estadístico

PROCESO 02: GENERAR EL COMPENDIO DE EVOLUCIÓN DE LAS ACTIVIDADES DE PRODUCCIÓN

Este proceso se inicia en el área de "Dirección Ejecutiva de Producción Estadística" el cual maneja análisis de los sectores económicos es decir de aquellos sectores que requieren producción y para su generación tiene una duración de 2 semanas y se nos informa sobre la producción del departamento del Lambayeque mostrando la evolución de la actividad productiva y sectorial a corto plazo.

El proceso tiene una periodicidad mensual y normalmente viene ligado al proceso del "Compendio Estadístico del Departamento", una vez obtenido la información de los sectores productivos tales como Sector Agropecuario, Sector Pesca, Sector Minería e Hidrocarburos, Sector Manufactura, Sector Electricidad, Gas y Agua, Sector Construcción, Sector Comercio, Sector Transporte, Almacenamiento y Mensajería, Alojamiento y Restaurantes,

Telecomunicaciones y Otros Servicios de Información, Sector Financiero y Seguros, Servicios Prestados a Empresas, Administración Pública se digitan los datos y se determina en función al comportamiento de un subconjunto de variables seleccionadas en cada rama de actividad económica, cuantificándolas a través de cuadros y gráficos estadísticos informándonos sobre evolución de la producción sectorial, dicho informe está dirigido a los principales agentes productivos del sector del departamento de Lambayeque.

Toda la información es consolidad en un informe llamado "Evolución de las Actividades de Producción del Departamento de Lambayeque" que será editado como un libro e impreso para la posterior venta al público en el centro documentario.

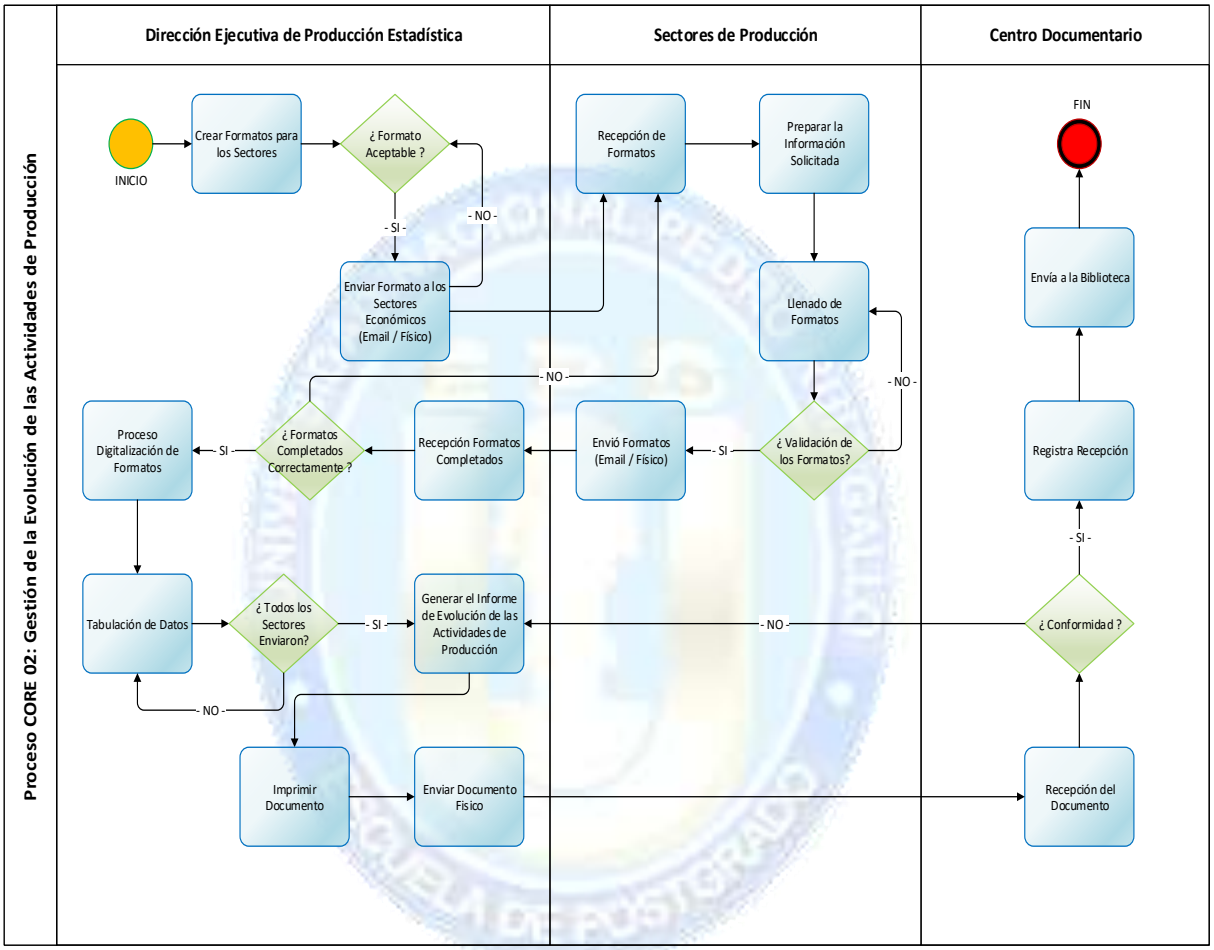


Imagen 16: Compendio De Evolución De Las Actividades De Producción

PROCESO 03: GENERAR EL REGISTRO NACIONAL DE MUNICIPALIDADES

Se crea mediante Ley Nº 27563 a cargo del Instituto Nacional de Estadística e Informática (ODEI) Lambayeque, con el objetivo de integrar y disponer de información estadística de las Municipalidades Provinciales y Distritales, así como de las Municipalidades de Centros Poblados identificadas en el departamento de Lambayeque, a fin de generar indicadores municipales que sirvan de apoyo a la gestión regional y local para la planificación y la adecuada toma de decisiones.

El método recolección de la información es por auto- diligenciamiento, es decir, el alcalde o el funcionario municipal designado es responsable del diligenciamiento del formulario y la veracidad de los datos. Para el relevamiento de la información se utiliza dos tipos de formularios; el Formulario 01 en formato impreso y electrónico dirigido a las Municipalidades Provinciales y Distritales, y el Formulario 02 en formato impreso para las Municipalidades de Centros Poblados del departamento de Lambayeque.

Las principales variables investigadas en el RENAMU están referidas a la infraestructura municipal, recursos humanos, planificación municipal, licencias de funcionamiento y edificación, saneamiento ambiental y salubridad, educación y cultura, salud, programas sociales, seguridad ciudadana, defensa civil, promoción del desarrollo económico local, conservación del ambiente, participación vecinal, infraestructura de comunicación, alumbrado público, agua potable y alcantarillado.

Los resultados del RENAMU del departamento de Lambayeque se difunden en la página Web del INEI, a través de los siguientes productos: base de datos, sistemas de información y publicaciones.

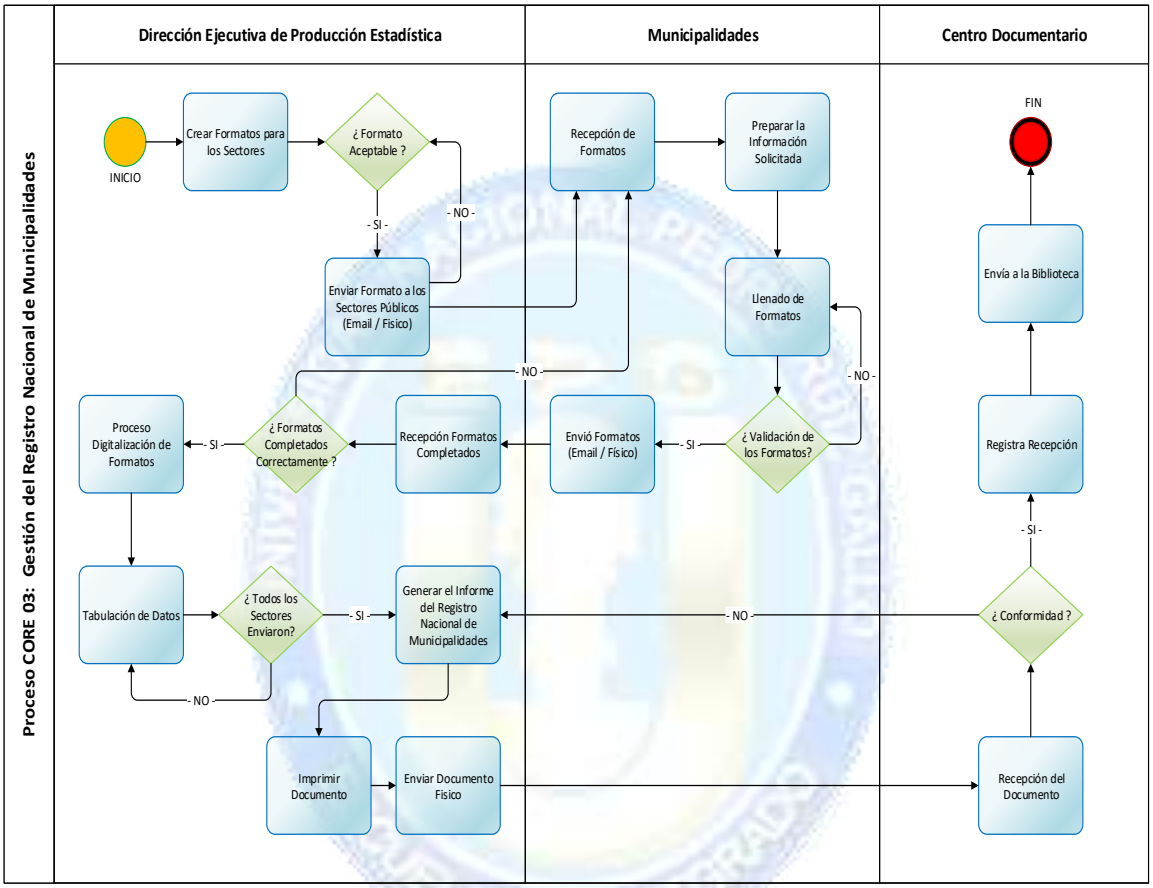


Imagen 17: Generar El Registro Nacional De Municipalidades

PROCESO 04: GENERAR EL IPC (ÍNDICE DE PRECIO CONSUMIDOR)

El Índice de Precios al Consumidor (IPC) es un indicador que registra los precios de los productos de una canasta familiar, el INEI filial Lambayeque genera el indicador macroeconómico y es realizado mensualmente. El proceso comienza cuando se selecciona una muestra de productos (ejemplo 1500 productos utilizados) y el personal encargado sale a diario a investigar los precios de los productos que pertenecen a una canasta familiar en las diferentes empresas del departamento de Lambayeque (bodegas, farmacias, supermercados, mercados) y recopilar los precios de los productos, una vez recopilada toda esta información y tomando como precio el "Año Base 2009" se realiza la comparación para determinar la inflación. Una vez obtenido se procesa la información y se ingresa al sistema gubernamental denominado "SIIE (Sistema de Información de Inflación Estadística". Para finalizar se publica un boletín mensual y se informa a la central del INEI en lima donde concentra toda la información de todas las oficinas departamentales restantes.

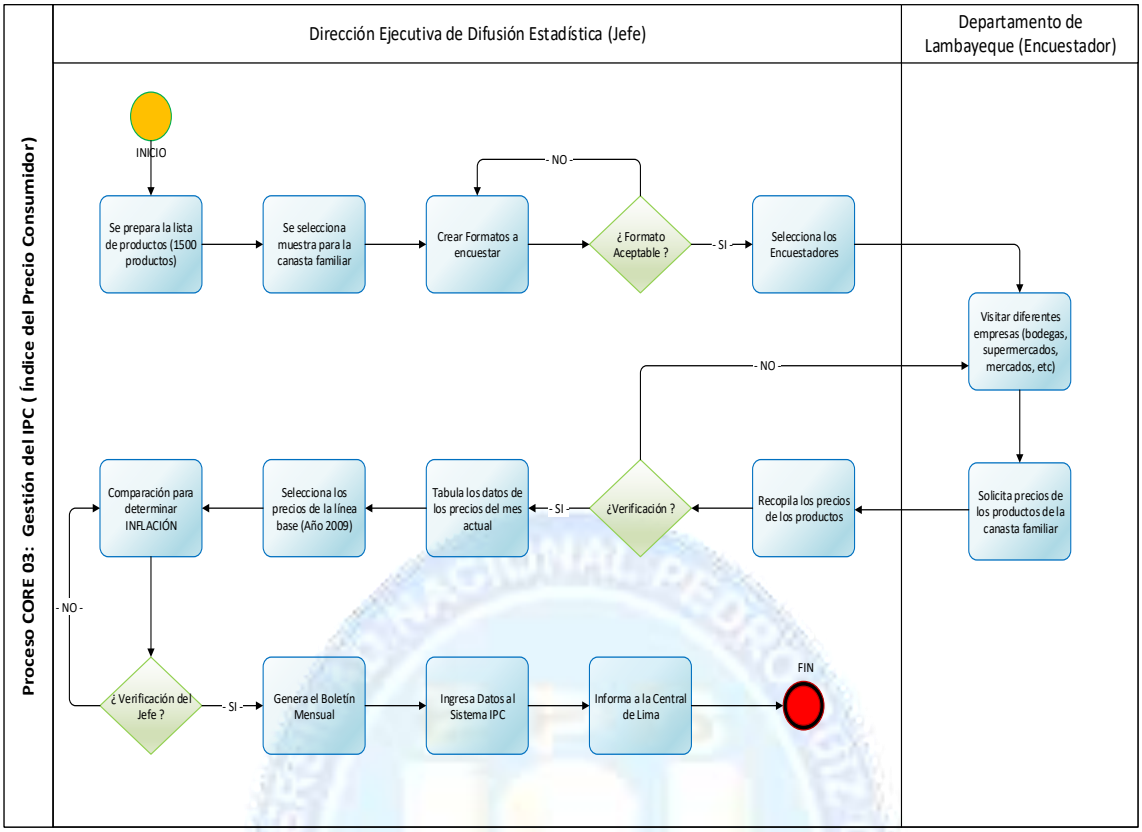


Imagen 18: Generar informe del IPC (Índice De Precio Consumidor)

9.4 ANEXO 04 - INEISGSI01 - EVALUACIÓN DE LA SITUACIÓN DE SEGURIDAD ACTUAL

INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

ODEI LAMBAYEQUE

EVALUACION DE LA SITUACION DE SEGURIDAD ACTUAL
(Línea de Base)

INFORMACIÓN DEL DOCUMENTO	
Evaluación de la Situación De Seguridad Actual (línea de base)	**Código:** INEISGSI01 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 04/08/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** APROBADO **Por:** Ing. Cancino Castañeda Daniel Ismael
Archivo: INEISGSI01 - Evaluación de la situación de seguridad actual (línea de base).docx	

HISTORIAL DE MODIFICACIONES

(Registro de cambios)

Versión #	Realizado por	Fecha Revisión	Aprobado por	Fecha Aprobación	Observación
1.0	Nilton Rogger Niño Morante	06/08/17	Ing. Cancino Castañeda Daniel Ismael	06/04/17	Descripción básica del documento.

INEISGSI01 - EVALUACIÓN DE LA SITUACIÓN DE SEGURIDAD ACTUAL (LÍNEA DE BASE)

A continuación, se presenta una lista de chequeo de la documentación con la que se cuenta en la ODEI (Oficina Departamental de Estadística e Informática) - Lambayeque, la cual nos muestra el estado y la situación actual con respecto a la documentación requerida por el estándar internacional NTP ISO/IEC 27001:2014.

N	Documento	Existe	Referencia NTP ISO/IEC 27001:2014
1	Alcance del SGSI	No	4.3
2	Políticas y objetivos de seguridad de información	No	5.2, 6.2
3	Metodología de evaluación y tratamiento de riesgos	No	6.1.2
4	Declaración de aplicabilidad	No	6.1.3 d)
5	Plan de tratamiento del riesgo	No	6.1.3 e), 6.2
6	Informe de evaluación de riesgos	No	8.2
7	Definición de funciones y responsabilidades de seguridad	No	A.7.1.2, A.13.2.4
8	Inventario de activos	No	A.8.1.1
9	Uso aceptable de los activos	No	A.8.1.3
10	Política de control de acceso	No	A.9.1.1
11	Procedimientos operativos para gestión de TI	No	A.12.1.1
12	Principios de ingeniería para sistema seguro	No	A.14.2.5
13	Política de seguridad para proveedores	No	A.15.1.1
14	Procedimiento para gestión de incidentes	No	A.16.1.5
15	Procedimientos de la continuidad del negocio	No	A.17.1.2
16	Requisitos legales, normativos y contractuales	Sí	A.18.1.1

Tabla 20: Evaluación De La Situación De Seguridad Actual

9.5 ANEXO 05 - INEISGSI02 - ANÁLISIS DE BRECHAS

INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

ODEI LAMBAYEQUE

ANÁLISIS DE BRECHAS

INFORMACIÓN DEL DOCUMENTO	
Análisis de Brechas	**Código:** INEISGSI02 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 14/08/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** APROBADO **Por:** Ing. Cancino Castañeda Daniel Ismael
Archivo: INEISGSI02 - Análisis de Brechas.xlsx	

HISTORIAL DE MODIFICACIONES

(Registro de cambios)

Versión #	Realizado por	Fecha Revisión	Aprobado por	Fecha Aprobación	Observación
1.0	Nilton Rogger Niño Morante	14/08/17	Ing. Cancino Castañeda Daniel Ismael	14/08/17	Descripción básica del documento.

INEISGSI02 - ANÁLISIS DE BRECHAS

✓ Leyenda

Leyenda	**C**	Cumple
	NC	No cumple
	CP	Cumple parcialmente
	N/A	No Aplica

✓ Análisis

INEI SGSI 02 - ANÁLISIS DE BRECHAS							
Dim.	**Cláusula**	**Descripción**	**C**	**NC**	**CP**	**Control**	**Referencia de la NTP ISO/IEC 27001:2014**
Cultura organizacional.	**6.1.1**	**Roles y responsabilidades para la seguridad de la información.**		**X**		Contar con roles y responsabilidades para la seguridad de la información.	Todas las responsabilidades para la seguridad de la información deben ser definidas y asignadas.
	6.1.2	**Segregación de funciones.**		**X**		Contar con roles y responsabilidades para la seguridad de la información.	Se deben segregar los deberes conflictivos en áreas de seguridad para reducir oportunidades para modificaciones no autorizadas o no intencionadas o mal uso de los activos de la organización.
	6.1.3	**Contacto con autoridades.**		**X**		Elaborar procedimientos para contactarse con autoridades y proveedores, que brinden soporte.	Se deben mantener contactos apropiados con autoridades relevantes.
	6.1.4	**Contacto con grupos de interés especiales.**		**X**		Definir a un encargado en el área de TI, para lectura de boletines de seguridad.	Se debe mantener contactos apropiados con grupos de interés especiales u otros foros de seguridad especializados y asociaciones.
	6.1.5	**Seguridad de la información en gestión de proyectos.**		**X**		Considerar que todo proyecto, independientemente del tipo, debe contar en la planificación del mismo, con enfoques de seguridad de información.	Se debe atender la seguridad de la información en la gestión de proyectos al margen del tipo de proyecto.
	6.2.1	**Política para dispositivos móviles.**		**X**		Considerar en el reglamento interno, políticas de uso de dispositivos móviles.	Se deben adoptar políticas y medidas de apoyo a la seguridad para gestionar los riesgos introducidos al usar dispositivos móviles.
	6.2.2	**Teletrabajo.**	N/A				

Recursos humanos.	**7.1.1**	**Revisión.**			**X**	Documentar el procedimiento para reclutamiento y selección de personal en base a la legislación y normas internas.	Se deben llevar a cabo verificaciones y chequeos de antecedentes de todos los candidatos para empleos en concordancia con leyes relevantes, regulaciones y ética y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a ser acezada y los riesgos percibidos.
	7.1.2	**Términos y condiciones de empleo.**		**X**		Se deberán considerar secciones referentes a seguridad de información en los contratos.	Los acuerdos contractuales con empleados y contratistas deben estipular su responsabilidad y las de la organización por la seguridad de la información.
	7.2.1	**Responsabilidades gerenciales.**		**X**		Contar con roles y responsabilidades para la seguridad de la información.	La gerencia debe requerir a todos los empleados y contratistas que apliquen la seguridad de la información en concordancia con las políticas establecidas y procedimientos de la organización.
	7.2.2	**Capacitación, educación y toma de conciencia para la seguridad de información.**		**X**		Capacitar y concientizar a los StakeHolders.	Todos los empleados de la organización y contratistas relevantes, deben recibir apropiada toma de conciencia, educación, capacitación y actualizaciones regulares de las políticas organizacionales y procedimientos relevantes para su función en el puesto de trabajo.
	7.2.3	**Proceso disciplinario.**		**X**		Considerar en el reglamento interno, sanciones para los empleados que atenten contra la seguridad de la información.	Debe haber un proceso disciplinario formal comunicado establecido para tomar acciones contra los empleados que hayan cometido un rompimiento en la seguridad de la información.
	7.3.1	**Terminación o cambio de responsabilidades del empleo.**		**X**		Documentar procedimiento para validación luego de término de contrato.	Las responsabilidades y deberes para la seguridad de la información que se mantienen válidos después de la terminación o cambio del empleo, deben ser definidos, comunicados al empleado o contratistas e implementados.
Control de accesos	**9.1.1**	**Política de control de acceso.**		**X**		Elaborar una política que abarque el control de acceso físico y acceso a redes.	Se debe establecer, documentar y revisar una política de control de acceso, basada en los requerimientos de seguridad de información del negocio.
	9.1.2	**Acceso a redes y a servicios de redes.**			**X**	Elaborar una política que abarque el control de acceso físico y acceso a redes.	Los usuarios deben sólo ser provistos de acceso a la red y a servicios de red los que han sido específicamente autorizados para su uso.
	9.2.1	**Registro y des-registro de usuarios.**		**X**		Establecer procedimiento de alta y baja de usuarios que incluya la asignación y desagnicación de permisos.	Se debe implementar un proceso formal de registro y des-registro de usuarios para asegurar la asignación de derechos de acceso.
	9.2.2	**Aprovisionamiento de derecho de acceso de usuarios.**		**X**		Establecer procedimiento de alta y baja de usuarios que incluya la asignación y desagnicación de permisos.	Se debe implementar un sistema formal de aprovisionamiento de acceso de usuarios para asignar o revocar el derecho de acceso a todo tipo de usuario para todos los sistemas y servicios.
	9.2.3	**Gestión de privilegios para el derecho de acceso.**			**X**	Establecer procedimiento de alta y baja de usuarios que incluya la asignación y desagnicación de permisos.	La asignación y uso de derechos de privilegios de acceso debe ser restringida y controlada.
	9.2.4	**Gestión de autenticación secreta**		**X**		Elaborar mecanismos de encriptación para la información de acceso de los usuarios.	La asignación de la autenticación secreta de usuarios debe ser controlada a través de un proceso de gestión formal.

		de información de usuarios.					
	9.2.5	**Revisión de los derechos de acceso de usuarios.**		**X**		Establecer procedimiento de alta y baja de usuarios que incluya la asignación y desagnicación de permisos.	Los propietarios de activos deben revisar los derechos de acceso a intervalos regulares.
	9.2.6	**Eliminación o ajuste a derechos de acceso.**		**X**		Establecer procedimiento de alta y baja de usuarios que incluya la asignación y desagnicación de permisos.	El derecho de acceso de todos los empleados y los usuarios de tercera parte a la información, debe ser eliminado al término del empleo, contrato u acuerdo, o ajustado al haber cambios.
	9.3.1	**Uso de autenticación secreta de la información.**		**X**		Contratar empresa para elaboración de programa de capacitación a usuarios.	A los usuarios se les debe requerir que sigan las prácticas organizacionales en el uso de la autenticación secreta de la información.
	9.4.1	**Restricción de acceso a la información.**			**X**	Establecer procedimiento de alta y baja de usuarios que incluya la asignación y desagnicación de permisos.	El acceso a la información y a las funciones del sistema de asignaciones debe ser restringido en concordancia con la política de control de acceso.
	9.4.2	**Procedimientos para comienzo de sesión segura.**		**X**		Implementar protocolos de autenticación segura y certificados digitales.	Cuando sea requerido por la política de control de accesos, los accesos a sistemas y aplicaciones deben ser controlados por un procedimiento de comienzo de sesión segura.
	9.4.3	**Sistema de gestión de contraseña.**	N/A				
	9.4.4	**Uso de privilegios de programas de utilidad.**	N/A				
	9.4.5	**Control de acceso a programas de código fuente.**			**X**	Proteger el código fuente de los aplicativos desarrollados y utilizados.	Los accesos a los programas de código de fuente deben restringirse.
Seguridad física y ambiental.	**11.1.1**	**Perímetro de seguridad física.**		**X**		Establecer los ambientes que cuentan con información sensible.	Los perímetros de seguridad física deben definirse y usarse para proteger áreas que contienen información sensible o crítica y ambientes de procesamiento de información.
	11.1.2	**Controles de entrada física.**		**X**		Las áreas con información sensible deberán contar con mecanismos de protección de acceso.	Las áreas seguras deben protegerse a través de apropiados controles de entrada para asegurar que sólo se permite el ingreso a personas autorizadas.
	11.1.3	**Seguridad de oficinas, cuartos y ambientes.**			**X**	Colocar cámaras de seguridad en las áreas con información sensible.	La seguridad física para las oficinas, cuartos y ambientes debe asignarse y aplicarse.
	11.1.4	**Protección contra amenazas externas y ambientales.**		**X**		Obtener alarmas contra incendios, inundaciones y antirrobo.	Protección física contra desastres naturales, ataques maliciosos o accidentes debe ser diseñada y aplicada.
	11.1.5	**Trabajando en áreas seguras.**	N/A				
	11.1.6	**Áreas de entrega y descarga.**	N/A				

	11.2.1	**Ubicación del equipo y protección.**		**X**		Implementar una sala de servidores y telecomunicaciones	El equipo debe ser ubicado y protegido para reducir los riesgos de amenazas ambientales, peligros y oportunidades para el acceso no autorizado.
	11.2.2	**Apoyo de servicios públicos.**		**X**		Contar con UPS para el servidor y los equipos de telecomunicaciones.	El equipo debe estar protegido de fallas eléctricas y otras alteraciones causadas por fallas de los servicios públicos.
	11.2.3	**Seguridad en el cableado.**	**X**			Mejorar el cableado actual cumpliendo con los estándares internacionales.	El cableado de energía y de telecomunicaciones transportando datos o servicios de apoyo de información, debe protegerse de intercepción, interferencia o daño.
	11.2.4	**Mantenimiento de equipos.**			**X**	Planificar el mantenimiento de los equipos y establecer bitácora de mantenimientos.	El equipo debe mantenerse correctamente para asegurar su continua disponibilidad e integridad.
	11.2.5	**Traslado de activos.**		**X**		Generar bitácora para traslado de equipos con la debida autorización.	Los equipos, información o software no deben sacarse de las instalaciones sin una autorización previa.
	11.2.6	**Seguridad del equipo y activos fuera de las instalaciones.**		**X**		Aplicar mecanismos de encriptación para la información sensible en los equipos informáticos.	La seguridad debe ser aplicada a activos fuera de las instalaciones, considerando los distintos riesgos de estar trabajando fuera de las instalaciones de la organización.
	11.2.7	**Segura disposición o reúso de equipos.**		**X**		Desplegar la verificación de los equipos que cuentan con información sensible y plasmar en inventario digital.	Todos los elementos de los equipos que contengan almacenamiento de medios, deben ser verificados para asegurar que cualquier dato sensitivo y software con licencia ha sido removido o sobrescrito de manera segura, previo a la disposición o reúso.
	11.2.8	**Equipo de usuario desatendido.**		**X**		Contratar empresa para elaboración de programa de capacitación a usuarios.	Los usuarios deben asegurar que el equipo desatendido tiene la protección apropiada.
	11.2.9	**Política de escritorio y pantalla limpia.**		**X**		Contratar empresa para elaboración de programa de capacitación a usuarios.	Se debe adoptar una clara política para papeles, y medios de almacenamiento removibles, y una política sobre pantalla limpia para ambientes de procesamiento de información.
Continuidad de negocio.	**17.1.1**	**Planificando la continuidad de la seguridad de la información.**		**X**		Se deberá realizar el plan de continuidad de negocio en el cual se abarque un ítem para la continuidad de la seguridad de la información.	La organización debe determinar sus requerimientos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, ej. Durante una crisis o un desastres.
	17.1.2	**Implementando la continuidad de la seguridad de información.**		**X**		Se deberá realizar el plan de continuidad de negocio en el cual se abarque un ítem para la continuidad de la seguridad de la información.	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el requerido nivel de continuidad para la seguridad de información durante una situación adversa.
	17.1.3	**Verificación, revisión y evaluación de la continuidad de la seguridad de la información.**		**X**		Se deberá realizar el plan de continuidad de negocio en el cual se abarque un ítem para la continuidad de la seguridad de la información.	La organización debe verificar el establecimiento e implementación de los controles de la continuidad de la seguridad de información a intervalos regulares, para así poder asegurar que son válidos y eficaces durante una situación adversa.
	17.2.1	**Disponibilidad del ambiente para el procesamiento de la información.**		**X**		Se deberá realizar el plan de continuidad de negocio en el cual se abarque un ítem para la continuidad de la seguridad de la información.	Se deben implementar ambientes para el procesamiento de la información con suficiente redundancia para alcanzar requerimientos de disponibilidad.

9.6 ANEXO 06 - INEISGSI03 - Definición del Alcance

INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

ODEI LAMBAYEQUE

DEFINICIÓN DEL ALCANCE

INFORMACIÓN DEL DOCUMENTO	
Definición del Alcance	**Código:** INEISGSI03 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 04/08/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** APROBADO **Por:** Ing. Cancino Castañeda Daniel Ismael
Archivo: INEISGSI03 - Definición del alcance.docx	

HISTORIAL DE MODIFICACIONES

(Registro de cambios)

Versión #	Realizado por	Fecha Revisión	Aprobado por	Fecha Aprobación	Observación
1.0	Nilton Rogger Niño Morante	04/08/17	Ing. Cancino Castañeda Daniel Ismael	05/08/17	Descripción básica del documento.

ODEI-LAMBAYEQUESGSI02 - DEFINICIÓN DEL ALCANCE

A. INTRODUCCIÓN

Este documento forma parte del Sistema de Gestión de Seguridad de la Información del Instituto Nacional de Estadística e Informática - Lambayeque, en el cual se distinguen procesos y actividades de negocio que tienen relación con la seguridad de la información.

B. DESCRIPCIÓN DEL ALCANCE A ALTO NIVEL

Se abarca la gestión de la seguridad de la información en los principales procesos del ODEI-Lambayeque los cuales son:

- ✓ Generar el Compendio Estadístico del Departamento de Lambayeque.
- ✓ Generar el Compendio de Evolución de las Actividades de Producción.
- ✓ Generar el Registro Nacional de Municipalidades.
- ✓ Generar el IPC [4].

Dichos procesos están alineados a la Declaración de Aplicabilidad y son generados en las áreas de Dirección Ejecutiva de Producción Estadística y Dirección Ejecutiva de Difusión Estadística.

C. OBJETIVO, ALCANCE Y USUARIOS

El objetivo de este documento es definir los límites del Sistema de gestión de seguridad de la información en el ODEI-LAMBAYEQUE. Este documento abarca toda la documentación y actividades dentro del SGSI. Los usuarios de este documento son los miembros de la alta gerencia del área de Dirección de Sistema Administrativo IV (Dirección Departamental), los miembros del equipo del proyecto que realizarán la implementación del SGSI y los jefes de área de Difusión, Producción y Dirección Departamental (áreas que definirás en base a los procesos que abarcará)

D. DOCUMENTOS DE REFERENCIA

- ✓ Norma NTP ISO/IEC 27001:2014, punto 4,3
- ✓ (Determinando el alcance del SGSI).
- ✓ Decreto Legislativo Nº 276, "Ley de Bases de la Carrera Administrativa y de Remuneraciones del Sector Público" y su Reglamento aprobado mediante Decreto Supremo Nº 005-90-PCM.
- ✓ Decreto Legislativo Nº 604, "Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática".
- ✓ Decreto Supremo Nº 043-2001-PCM, que aprueba el "Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática".
- ✓ Resolución Suprema Nº263-2001-PCM, que aprueba el "Cuadro para Asignación de Personal del ODEI-LAMBAYEQUE".
- ✓ Resolución Jefatural Nº095-95-INAP/DNR, que aprueba la Directiva Nº 001-95- INAP/DNP sobre "Normas para la Formulación de Manuales de Organización y Funciones".
- ✓ Resolución de Contraloría Nº072-98-CG, que aprueba las "Normas Técnicas de Control Interno para el Sector Público".
  Visión y Misión
- ✓ Reglamento interno
- ✓

E. DEFINICIÓN DEL ALCANCE DEL SGSI

Se establecerán los límites del SGSI debido a que se plasmará la información a proteger. Dado que la información no es un activo al cual se le dé la debida importancia y protección, se busca con el SGSI proteger la información y no llegue a personas sin la debida autorización. Tomando en cuenta los requisitos legales, normativos y de otra índole, el alcance se define en base a los siguientes aspectos:

[4] Índice del Precio Consumidor

- ✓ **Perfil de la organización**

ODEI Lambayeque es el órgano desconcentrado del INEI-Lima, responsable de promover, orientar, desarrollar y coordinar las acciones de capacitación e investigación en los campos de la estadística e informática y áreas afines en su sede departamental. Para el cumplimiento de sus objetivos, cuenta con la siguiente estructura orgánica:

- Oficina Departamental de Estadística e Informática de Lambayeque
- Dirección Ejecutiva de Difusión Estadística
- Dirección Ejecutiva de Producción Estadística

Su misión es ser un organismo líder a nivel nacional e internacional, que utiliza los más altos estándares metodológicos y tecnológicos para la producción y difusión de estadísticas oficiales que contribuyan eficazmente en el diseño de políticas públicas para el desarrollo del país.

Las funciones de ODEI–Lambayeque son las contempladas, en el Decreto Supremo Nº 043-2001-PCM Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática - INEI:

- Coordinar, orientar, supervisar y evaluar, la ejecución del Plan Estadístico Departamental y Local y, Administrar el banco de Datos Departamental.
- Normar, dirigir, coordinar y supervisar las actividades estadísticas en el ámbito departamental.
- Administrar los recursos presupuestales, materiales y el personal asignado.
- Apoyar a las autoridades departamentales con información estadística oportuna, confiable y útil.
- Centralizar, publicar y difundir las estadísticas Departamentales oportunamente, de acuerdo a las normas técnicas emitidas por los órganos de Línea del ODEI-LAMBAYEQUE.

La aplicación del presente estudio permite definir el alcance del SGSI en la organización incluyendo las áreas funcionales principales que permitan lograr el cumplimiento y éxito de la misión de la organización con el apoyo del área Dirección Departamental.

Para esta aplicación del SGSI se sigue el modelo de P.D.C.A. (planificar, hacer, controlar y actuar) basada en la metodología DEMMING.

- ✓ **Procesos y servicios**

Los procesos de la institución tienen que responder ante la gerencia, los cuales reciben como salida un producto físico o servicio. Estos establecen las condiciones de satisfacción o declaran que el producto o servicio es aceptable o no.

Se realizó el proceso de levantamiento de la información para proceder a identificar los procesos “CORE de Negocio”, procesos de Soporte y Procesos Operativos.

A continuación, se describirán los principales procesos que soportan las distintas áreas de la institución ODEI– Lambayeque:

Imagen 19: Mapa de Procesos Nivel I

Dentro de los procesos y servicios que se incluirán en el presente estudio de investigación, nos centraremos en las áreas más importantes (Dirección Ejecutiva de Producción Estadística y Dirección Ejecutiva de Difusión Estadística) para lo cual se nombra los siguientes procesos a tomar en cuenta:

- Gestión del Compendio Estadístico del Departamento.
- Gestión de la Evolución de las Actividades de Producción.
- Gestión del Registro Nacional de Municipalidades.
- Gestión del IPC.

Cabe indicar que, como parte de la mejora continua, se podrán incluir procesos o servicios adicionales y estos podrían ser analizados y considerados a futuro, dentro del SGSI.

✓ **Unidades organizativas**

Imagen 20: Diagrama de la Empresa

En el ODEI - Lambayeque las áreas de negocio más significativas y que será incluida en el presente estudio son:

- Dirección Ejecutiva de Producción Estadística
- Dirección Ejecutiva de Difusión Estadística

✓ **Redes e infraestructura de TI**

La organización no cuenta con un área específica de tecnologías de información propiamente dicha, sin embargo, cuenta con un área de Capacitación e Informática, el cual tiene como función principal brindar las capacitaciones de ingeniería a profesionales, brindar mantenimiento de los laboratorios de cómputo y administrar los sistemas de información (IPC-Índice de Precio Consumidor y Sitio Web).

- ✓ **Exclusiones del alcance.**

No se incluye en el presente estudio a las áreas y procesos de:

Áreas.
Dirección Departamental
Oficina de Proyectos (Censos y Encuestas)
Oficina Técnica de Administración (O.T. de Administración)
Oficina Técnica de Informática (O.T. de Informática)
Procesos.
Gestión del Centro Documentario
Proyecto ENAHO: Encuesta Nacional De Hogares
Proyecto ENAPRES: Encuesta Nacional De Programas Estratégicos.
Proyecto ENDES: Encuesta Demográfica Y Salud
Gestión de Pagos
Gestión de Presupuesto
Gestión de Recursos Humanos
Gestión de Contabilidad
Escuela de Capacitación
Soporte Técnico

DEFINICIÓN DEL ALCANCE DEL SGSI – ODEI LAMBAYEQU

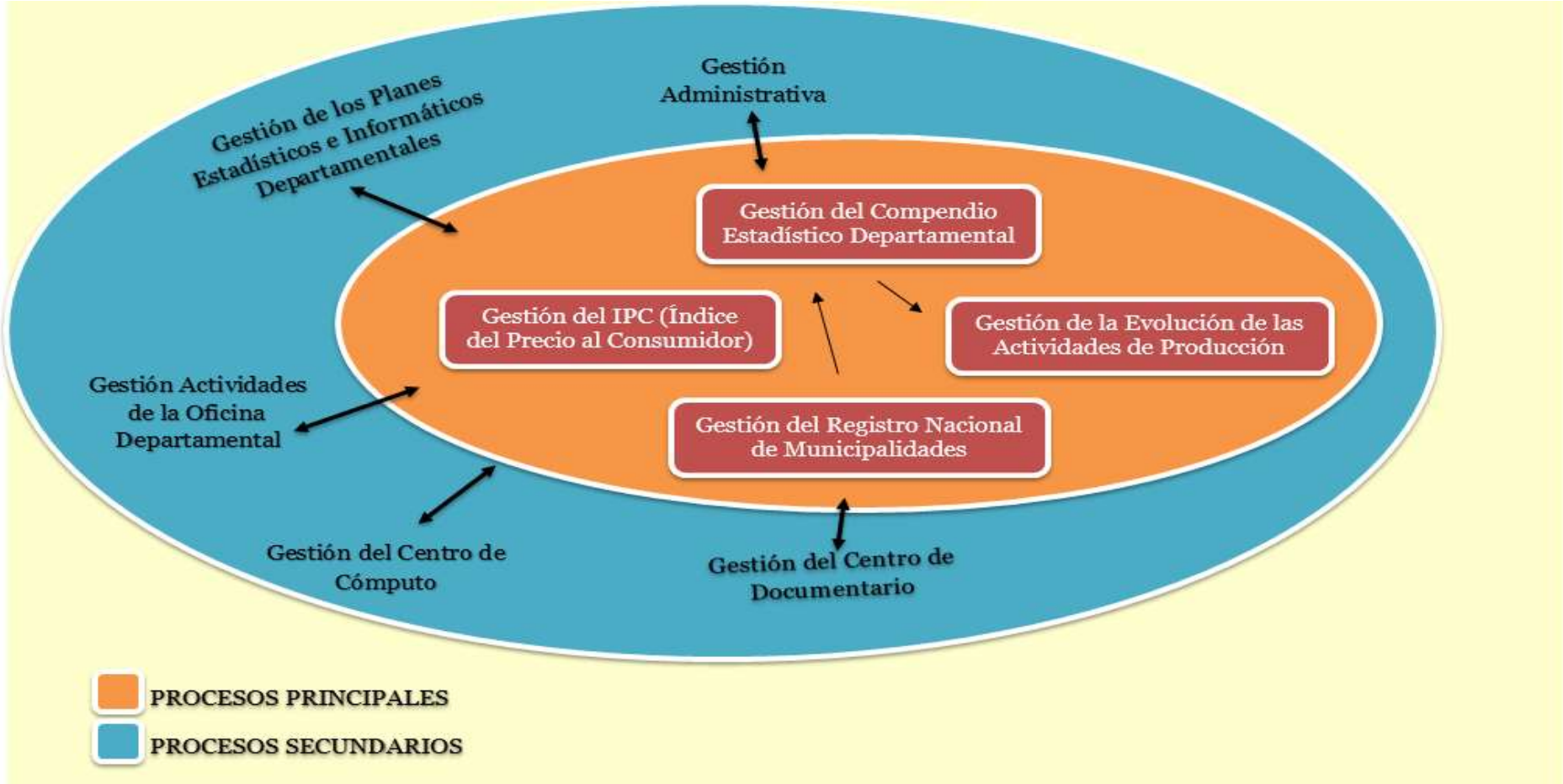


Imagen 21: Mapa de Procesos Nivel II

9.7 ANEXO 07 - INEISGSI04 - POLÍTICA SEGURIDAD INFORMACIÓN

ODEI LAMBAYEQUE

POLÍTICA SEGURIDAD INFORMACIÓN

INFORMACIÓN DEL DOCUMENTO	
Política Seguridad Información	**Código:** INEISGSI04 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 09/08/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** APROBADO **Por:** Ing. Cancino Castañeda Daniel Ismael
Archivo: INEISGSI04 - Política Seguridad Información.docx	

HISTORIAL DE MODIFICACIONES

(Registro de cambios)

Versión #	Realizado por	Fecha Revisión	Aprobado por	Fecha Aprobación	Observación
1.0	Nilton Rogger Niño Morante	09/08/17	Ing. Cancino Castañeda Daniel Ismael	09/08/17	Descripción básica del documento.

INEISGSI04 - POLÍTICA SEGURIDAD INFORMACIÓN

A. OBJETIVO, ALCANCE Y USUARIOS

La política busca definir el horizonte que deberá tener el ODEI Lambayeque para gestionar la seguridad de la información. La política se aplica en la Oficina Departamental de Estadística e Informática - ODEI Lambayeque Este documento tiene como miembros al director departamental de ODEI Lambayeque, el área de oficina técnica de informática, el área de oficina técnica administrativa, área de dirección ejecutiva de producción estadística y el área de dirección ejecutiva de difusión estadística La dirección departamental deberá establecer un cronograma de revisión de la política, según sea la necesidad y las nuevas vulnerabilidades detectadas en el transcurso de la operación.

B. DOCUMENTOS DE REFERENCIA

- ✓ Norma NTP ISO/IEC 27001:2014.
- ✓ Documento sobre el alcance del SGSI.
- ✓ Metodología de evaluación y tratamiento de riesgos.
- ✓ Declaración de aplicabilidad.
- ✓ ODEI-Lambayeque: Normas Técnicas de Control Interno para el Sector Público: Misión y Visión
- ✓ ODEI-Lambayeque: Normas para la Formulación de Manuales de Organización y Funciones (MOF)
- ✓ ODEI-Lambayeque: Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática (ROF)

C. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

a. **Activo de Seguridad de Información:** Algo que tiene valor para la Institución. Los Activos pueden ser:
   - ✓ De información: archivos, bases de datos, manuales, material de formación, proyectos, procedimientos operativos o de soporte, planes de continuidad, configuración del soporte de recuperación, información archivada;
   - ✓ De software: software de aplicación, software del sistema, herramientas y programadas de desarrollo.
   - ✓ Físicos: instalaciones, equipos de cómputo, de comunicaciones, medios magnéticos (discos y cintas) u otro equipo técnico.
   - ✓ De servicios: servicios informáticos y comunicaciones, servicios generales (energía eléctrica, telefonía, iluminación).
   - ✓ Personas: sus calificaciones, habilidades y experiencia.
   - ✓ Intangibles: como la reputación y la imagen institucional.

b. **Propietario de los Activos de Seguridad de Información:** Persona o unidad orgánica que administra los activos de seguridad de información y tiene la responsabilidad de inventariar, actualizar, registrar y custodiar los activos de seguridad de información.

c. **Análisis del riesgo:** Uso sistemático de la información para identificar fuentes y estimar el impacto y riesgo de ocurrencia.

d. **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

e. **Integridad:** Se refiere a que la información y su procesamiento son exactos y completos.

f. **Confidencialidad:** Busca prevenir el acceso no autorizado a la información ya sea en forma intencional o no intencional.

g. **Disponibilidad:** Para la seguridad de información. la disponibilidad busca el acceso confiable y oportuno a los datos, información o recursos por el personal autorizado.

h. **Control del tratamiento de riesgo:** Es la práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

i. **Evento de seguridad de la información:** Ocurrencia identificada del estado de un sistema, servicio o red que indica un posible incumplimiento de la política de seguridad de la información o falla de las protecciones, o situación previamente desconocida que puede estar relacionada con la seguridad.

j. **Impacto:** Es la valorización de las consecuencias del uso no apropiado de la información.
k. **Incidente de seguridad de la información:** Hecho único o serie de hechos no deseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
l. **Backup:** es una copia de seguridad de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.
m. **Política de Seguridad de la Información:** Es el documento que dirige y da soporte a la gestión de la seguridad de la información en concordancia con los requerimientos de la Institución, las leyes y las regulaciones.
n. **Seguridad de la información:** Conservación de la confidencialidad, integridad y disponibilidad de la información en general.
o. **Sistema de gestión de seguridad de la información. (SGSI):** Aquella parte del sistema de gestión general, basada en un enfoque de riesgos de la Institución, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

D. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

a. Objetivos, Políticas y medición.

Objetivos: proteger la información producida en la institución para que no se altere, modifique o elimine ante las amenazas (internas y externas)

Políticas:

General de seguridad de la información.

En el ODEI se instituye las siguientes políticas de seguridad de la información:

- ✓ Definir al personal encargado de formar un comité de seguridad, el cual entre otras funciones velará por la revisión continua de la política de seguridad de información.
- ✓ Todos los activos de la organización se codificarán y se clasificarán, con el fin de llevar un control exhaustivo.
- ✓ Se implementará la gestión de accesos a las áreas que cuentan con información sensible, tanto en físico como en archivos digitales.
- ✓ Todos los proveedores externos que sean contratados para diversas funciones, y manejen información sensible, deberán tener controles para evitar pérdida, alteración, destrucción o uso indebido de la misma.
- ✓ El comité de seguridad deberá proponer un cronograma de auditorías y controles.
- ✓ Se deberá contar con una política de escritorios limpios, en la cual se revisará periódicamente cualquier medio que contenga usuarios o contraseñas de acceso.
- ✓ No se permitirá el uso de discos portátiles en los activos informáticos que cuenten con información clasificada.
- ✓ Solo se deberá utilizar software que haya sido adquirido legalmente y aprobado por el comité de seguridad de información.
- ✓ Todo el personal, incluidos los contratistas / proveedores de servicio que trabajen para el INEI deberán reportar cualquier incidente que altere o pueda alterar la seguridad de información.

b. Responsabilidades

La dirección departamental deberá establecer los roles y responsabilidades para las tareas y procedimientos referentes a la seguridad de la información. La dirección departamental debe asignar los roles y responsabilidad con el fin de:

- ✓ Asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos del estándar ISO 27001-2; y

- ✓ Generar el reporte reportar de desempeño del sistema de gestión de seguridad de la información para la sede central.

c. Comunicación de la política

La dirección departamental deberá comunicar la política y velar por su cumplimiento en toda la organización, así como también cualquier actualización que se de en la misma.

E. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI

La dirección departamental debe transmitir la importancia del SGSI, para así todas las áreas y todo el personal aporte con la implementación del SGSI.

F. SANCIONES PREVISTAS POR INCUMPLIMIENTO

El personal de la institución que no cumpla con lo dispuesto en la presente política será sancionado administrativamente en conformidad con el reglamento interno.

9.8 ANEXO 08 - INEISGSI05 - Declaración de Aplicabilidad

ODEI LAMBAYEQUE

DECLARACIÓN DE APLICABILIDAD

INFORMACIÓN DEL DOCUMENTO	
INEISGSI05 - Declaración de aplicabilidad	**Código:** INEISGSI05 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 01/09/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** APROBADO **Por:** Ing. Cancino Castañeda Daniel Ismael
Archivo: INEISGSI05 - Declaración de aplicabilidad.xls	

HISTORIAL DE MODIFICACIONES

(Registro de cambios)

Versión #	Realizado por	Fecha Revisión	Aprobado por	Fecha Aprobación	Observación
1.0	Nilton Rogger Niño Morante	28/08/17	Ing. Cancino Castañeda Daniel Ismael	01/09/17	Descripción básica del documento.

INEISGSI05 - DECLARACIÓN DE APLICABILIDAD

La presente declaración los controles que son relevantes para el SGSI de la institución y aplicables al mismo. Adicionalmente en ella se encuentran justificada la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades empresariales de la organización en materia de seguridad de la información:

INEISGSI05 - DECLARACIÓN DE APLICABILIDAD					
Dim.	**ID**	**Controles NTP ISO/IEC 27001:2014**	**Aplica**	**Justificación**	**Control**
Cultura organizacional.	A.6	Organización de la seguridad de la Información			
	A.6.1	**Organización interna**	**Objetivo:** establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización		
	A.6.1.1	Roles y responsabilidades sobre seguridad de la información	Si	Cada uno de los responsables deben asociarse a la seguridad de la información en ODEI Lambayeque teniendo asignado sus roles.	Control. Todas las responsabilidades para la seguridad de la información deben ser definidas y asignadas.
	A.6.1.2	Segregación de deberes.	Si	Se definen funciones distintas con el fin de proteger los activos de información del ODEI Lambayeque.	Control Los deberes y las áreas de responsabilidad en conflictos se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
	A.6.1.3	Contacto con autoridades	Si	Se debe mantener relación con entidades gubernamentales dedicadas a la seguridad de información.	Control Convenios u contratos con entidades terceras concernientes a la seguridad de la información.
	A.6.1.4	Contacto con grupos de interés especial	Si	Establecer convenios con entidades especializadas en seguridad de información.	Control Se deben tener contactos u convenios apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
	A.6.1.5	Seguridad de la información en gestión de proyectos	Si	Todos los proyectos que se realicen en ODEI Lambayeque deberán planificarse incluyendo la seguridad de información.	Control Implicaciones de seguridad de información deberán dirigirse y ser revisados con regularidad en todos los proyectos.
	A.6.2	Dispositivos móviles y tele-trabajo	**Objetivos:** garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		

	A.6.2.1	Política para dispositivos móviles.	Si	Se debe prevenir que información sensible pueda ser extraída de la organización	Control Se deben adoptar una política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de los dispositivos móviles
	A.6.2.2	Tele-trabajo.	No	No se realiza trabajo de manera remota en ODEI Lambayeque.	Una política y el apoyo a las medidas de seguridad se deben implementar para proteger la información visitada, procesada o almacenada en los sitios de teletrabajo.
Recursos Humanos.	A.7	Seguridad de los recursos humanos			
	A.7.1	Antes del empleo	**Objetivo:** asegurar que los empleados y contratistas comprendan sus responsabilidades y son idóneos en los roles para los que se consideran.		
	A.7.1.1	Revisión	Si	Se debe realizar una verificación exhaustiva y cumpliendo con la normativa legal e interna para la contratación de personal.	Control Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos del negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
	A.7.1.2	Términos y condiciones del empleo.	Si	Todos los contratos deberán contar con las responsabilidades definidas y claras.	Control Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
	A.7.2	Durante el empleo	**Objetivo:** asegurarse de que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.		
	A.7.2.1	Responsabilidades de la gerencia.	Si	Todos los colaboradores (internos o externos) deberán cumplir con la política de seguridad de información del ODEI Lambayeque.	Control La gerencia debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
	A.7.2.2	Conciencia, educación y formación en la seguridad de la información.	Si	La capacitación y concientización en seguridad de información es de suma importancia para cumplir con	Control Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la

				los objetivos de seguridad de información del ODEI Lambayeque.	formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
	A.7.2.3	Proceso disciplinario	Si	El reglamento interno del ODEI Lambayeque debe contener ítems que consideren la seguridad de información.	Control Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
	A.7.3	Terminación y cambio de empleo	**Objetivo :** Proteger los intereses organizacionales como parte del proceso de cambio o terminación del empleo.		
	A.7.3.1	Terminación o cambio de responsabilidades de empleo.	Si	Al término de contrato o cambio de responsabilidades en la institución, se debe comunicar de manera formal al colaborador o contratista.	Control Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
Control de Accesos	A.9	Control de accesos			
	A.9.1	Requerimientos del negocio de control de acceso	**Objetivo:** limitar el acceso a la información y a los centros de procesamiento de información.		
	A.9.1.1	Política de control de acceso.	Si	La política de control de acceso de la organización deberá contemplar a todas las áreas con la información a proteger.	Control Se debe establecer, documentar y revisar una política de control de acceso, basada en los requerimientos de seguridad de información del negocio.
	A.9.1.2	Acceso a redes y a servicios de redes.	Si	Todos los colaboradores deben contar con los permisos según los recursos de la red que necesitan para realizar sus labores.	Control Los usuarios deben sólo ser provistos de acceso a la red y a servicios de red los que han sido específicamente autorizados para su uso.
	A.9.2	Gestión de Acceso a usuarios	**Objetivo:** Asegurar el uso autorizado de acceso a usuarios y prevenir el acceso no autorizado a sistemas y servicios		
	9.2.1	Alta y baja de usuarios.	Si	El proceso de alta y baja de usuarios se deberá establecer, monitorear y verificar en ODEI Lambayeque.	Control Se debe implementar un proceso formal de alta y baja de usuarios para asegurar la asignación de derechos de acceso.
	9.2.2	Aprovisionamiento de derecho de acceso de usuarios.	Si	Los derechos de acceso de los colaboradores serán habilitados según los recursos que requieran.	Control Se debe implementar un sistema formal de aprovisionamiento de acceso de usuarios para asignar o revocar el

					derecho de acceso a todo tipo de usuario para todos los sistemas y servicios.
	9.2.3	Gestión de privilegios para el derecho de acceso.	Si	Los derechos de acceso de los colaboradores deberán registrarse y monitorearse en una hoja de control.	Control La asignación y uso de derechos de privilegios de acceso debe ser restringida y controlada.
	9.2.4	Gestión de autenticación secreta de información de usuarios.	Si	Todos los colaboradores cambiarán de contraseña luego de su primer inicio de sesión.	Control La asignación de la autenticación secreta de usuarios debe ser controlada a través de un proceso de gestión formal.
	9.2.5	Revisión de los derechos de acceso de usuarios.	Si	La gerencia del ODEI coordinará la revisión periódica de los derechos de acceso según las responsabilidades y roles.	Control Los propietarios de activos deben revisar los derechos de acceso a intervalos regulares.
	9.2.6	Eliminación o ajuste a derechos de acceso.	Si	Los derechos de acceso se revisarán cada vez que se presente término de contrato de cualquier colaborador o contratista externo.	Control El derecho de acceso de todos los empleados y los usuarios externos a la información e instalaciones de procesamiento de información debe ser eliminado al término del empleo, contrato u acuerdo, o ajustado al haber cambios.
	A.9.3	Responsabilidades del usuario	**Objetivo:** hacer que los usuarios sean responsables por la salvaguarda de su autenticación de información		
	9.3.1	Uso de autenticación secreta de la información.	Si	Las prácticas de la ODEI para el uso de la información con autenticación se seguirán por todos los colaboradores y contratistas externos.	Control A los usuarios se les debe requerir que sigan las prácticas organizacionales en el uso de la autenticación secreta de la información.
	A.9.4	Control de Acceso a aplicaciones y sistemas	**Objetivo:** Prevenir el acceso no autorizado a sistemas y aplicaciones		
	9.4.1	Restricción de acceso a la información.	Si	El acceso a los sistemas IPC y Control de encomienda estará bajo la política de control de acceso definida.	El acceso a la información y a las funciones del sistema de aplicaciones debe ser restringido en concordancia con la política de control de acceso.
	9.4.2	Procedimientos para comienzo de sesión segura.	Si	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Cuando sea requerido por la política de control de accesos, los accesos a sistemas y aplicaciones deben ser controlados por un procedimiento de comienzo de sesión segura.

	9.4.3	Sistema de gestión de contraseña.	No	El ODEI Lambayeque ha decidido no contar con un sistema de gestión de contraseñas. Las contraseñas se definen según la política de seguridad de información.	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad
	9.4.4	Uso de privilegios de programas de utilidad.	No	Por restricciones de INEI (Lima),no permite el uso de utilitarios para modificar información en sistemas.	Control El uso de programas de utilidad que pudieran tener la capacidad de modificar controles de los sistemas y las aplicaciones deberían restringirse y controlarse
	9.4.5	Control de acceso a programas de código fuente.	Si	El código fuente de los sistemas en ODEI Lambayeque se encuentra restringido, el uso es exclusivo por el personal de sistemas encargado.	Control Los accesos a los programas de código de fuente deben restringirse.
Seguridad Física y Ambiental.	A.11	Seguridad Física y Ambiental			
	A.11.1	Áreas Seguras	**Objetivo:** prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
	11.1.1	Perímetro de seguridad física.	Si	Todos los ambientes que contienen información importante serán establecidos dentro del perímetro de seguridad física.	Control Los perímetros de seguridad física deben definirse y usarse para proteger áreas que contienen información sensible o crítica y ambientes de procesamiento de información.
	11.1.2	Controles de entrada física.	Si	Se limitará el ingreso a las áreas seguras, solo a personal autorizado mediante controles de acceso apropiados a los ambientes que contienen información confidencial o crítica.	Control Las áreas seguras deben protegerse a través de apropiados controles de entrada para asegurar que sólo se permite el ingreso a personas autorizadas.
	11.1.3	Seguridad de oficinas, cuartos y ambientes.	Si	Todo ambiente que contenga y se procese información importante deberá contar con seguridad física.	Control La seguridad física para las oficinas, cuartos y ambientes debe asignarse y aplicarse.
	11.1.4	Protección contra amenazas externas y ambientales.	Si	Se deberá contar con un plan de recuperación de desastres en caso	Control Protección física contra desastres naturales, ataques maliciosos o

				suceda algún desastre natural o ataque externo.	accidentes debe ser diseñada y aplicada.
	11.1.5	Trabajando en áreas seguras.	No	No existen procesos industriales en el ODEI Lambayeque, todos los procesos son administrativos.	Control Se debe diseñar y aplicar procedimientos para el trabajo en áreas seguras.
	11.1.6	Áreas de entrega y descarga.	No	No se cuenta con un área en la que se haga entrega o descarga en el ODEI Lambayeque.	Control Puntos de Acceso tales como entrega y áreas de descarga y otros puntos donde el personal no autorizado pudiera penetrar a las instalaciones deben ser controlados y si es posible, aislados de ambientes de procesamiento de la información para evitar accesos no autorizados.
	A.11.2	Equipo	**Objetivo:** prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
	11.2.1	Ubicación del equipo y protección.	Si	Se deberá evaluar la ubicación del equipamiento con información importante y ser reubicado según la evaluación realizada.	Control El equipo debe ser ubicado y protegido para reducir los riesgos de amenazas ambientales, peligros y oportunidades para el acceso no autorizado.
	11.2.2	Apoyo de servicios públicos.	Si	Los equipos contarán con estabilizadores, supresores de picos y UPS según sea el caso.	Control El equipo debe estar protegido de fallas eléctricas y otras alteraciones causadas por fallas de los servicios públicos.
	11.2.3	Seguridad en el cableado.	Si	El cableado eléctrico y de telecomunicaciones se ciñe los estándares y normas internacionales.	Control El cableado de energía y de telecomunicaciones transportando datos o servicios de apoyo de información, debe protegerse de intercepción, interferencia o daño.
	11.2.4	Mantenimiento de equipos.	Si	ODEI Lambayeque planifica el mantenimiento de equipos cada tres meses.	Control El equipo debe mantenerse correctamente para asegurar su continua disponibilidad e integridad.
	11.2.5	Traslado de activos.	Si	Todo traslado de equipos, información o software se realizara con la debida autorización.	Control Los equipos, información o software no deben retirarse de las instalaciones sin una autorización previa.

	11.2.6	Seguridad del equipo y activos fuera de las instalaciones.	Si	Los equipos deberán contar con mecanismos de encriptación y estarán bajo custodia del responsable que procedió con el retiro del equipo fuera de las instalaciones.	Control La seguridad debe ser aplicada a activos fuera de las instalaciones, considerando los distintos riesgos de estar trabajando fuera de las instalaciones de la organización.
	11.2.7	Segura disposición o reúso de equipos.	Si	Todo el equipamiento que sea dispuesto para reutilización deberá ser validado y verificado con el fin de que la información importante sea removida.	Control Todos los elementos de los equipos que contengan almacenamiento de medios, deben ser verificados para asegurar que cualquier dato sensitivo y software con licencia ha sido removido o sobrescrito de manera segura, previo a la disposición o reúso.
	11.2.8	Equipo de usuario desatendido.	Si	Todos los colaboradores deberán brindar una protección adecuada a sus equipos (pc, laptop, Tablet, etc.) al momento de alejarse de las mismas.	Control Los usuarios deben asegurar que el equipo desatendido tiene la protección apropiada.
	11.2.9	Política de escritorio y pantalla limpia.	Si	Tanto los papeles y medios de almacenamiento removibles como los escritorios y las pantallas no se deberá contar con información de accesos o información clasificada.	Control Se debe adoptar una clara política para papeles, y medios de almacenamiento removibles, y una política sobre pantalla limpia para ambientes de procesamiento de información.
Continuidad de Negocio.	A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio.			
	A.17.1	Continuidad de seguridad de la información.	**Objetivo:** la continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización		
	17.1.1	Planificando la continuidad de la seguridad de la información.	Si	Los planes de continuidad de negocio deberán ser elaborados y contemplarán con ítems que abarquen la continuidad de seguridad de información.	Control La organización debe determinar sus requerimientos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, ej. Durante una crisis o un desastres.
	17.1.2	Implementando la continuidad de la seguridad de información.	Si	Los planes de continuidad de negocio serán implementados	Control La organización debe establecer, documentar, implementar y

				según los requerimientos del ODEI Lambayeque.	mantener procesos, procedimientos y controles para asegurar el requerido nivel de continuidad para la seguridad de información durante una situación adversa.
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Si	La continuidad de negocio y continuidad de seguridad de información será revisada de manera semestral , con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Control La organización debe verificar el establecimiento e implementación de los controles de la continuidad de la seguridad de información a intervalos regulares, para así poder asegurar que son válidos y eficaces durante una situación adversa.
	A.17.2	Redundancias	**Objetivo:** asegurar la disponibilidad de instalaciones de procesamiento de información.		
	17.2.1	Disponibilidad del ambiente para el procesamiento de la información.	Si	Se deberá contar con equipamiento para la redundancia de información suficiente para cumplir con los requisitos de disponibilidad.	Se deben implementar ambientes para el procesamiento de la información con suficiente redundancia para alcanzar requerimientos de disponibilidad.

9.9 ANEXO 09 - INEISGSI06 - Cronograma de Trabajo

INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

ODEI LAMBAYEQUE

CRONOGRAMA DE TRABAJO

INFORMACIÓN DEL DOCUMENTO	
INEISGSI06 - Cronograma de trabajo	**Código:** INEISGSI06 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 11/09/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** APROBADO **Por:** Ing. Cancino Castañeda Daniel Ismael
Archivo: INEISGSI06 - Cronograma de trabajo.xlsx	

HISTORIAL DE MODIFICACIONES

(Registro de cambios)

Versión #	Realizado por	Fecha Revisión	Aprobado por	Fecha Aprobación	Observación
1.0	Nilton Rogger Niño Morante	11/09/17	Ing. Cancino Castañeda Daniel Ismael	11/09/17	Descripción básica del documento.

INEISGSI06 - CRONOGRAMA DE TRABAJO

INEI SGSI 06 - CRONOGRAMA DE TRABAJO																				
FASES / ACTIVIDADES	**AGOSTO**				**SEPTIEMBRE**				**OCTUBRE**				**NOVIEMBRE**				**DICIEMBRE**			
Semanas	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
PLANIFICAR:																				
1. Definir alcance																				
2. Elaborar política de seguridad de información																				
3. Obtener inventario de activos.																				
4. Establecer línea base mediante evaluación de la situación de seguridad actual y análisis de brechas																				
5. Definir la declaración de aplicabilidad																				
6. Evaluar los riesgos																				
7. Elaborar plan de tratamiento de riesgos																				
HACER:																				
1. Evaluar controles de seguridad																				
2. Identificar métricas e indicadores.																				
3. Definir políticas y procedimientos del SGSI																				
4. Asignación y distribución de recursos																				
5. Propuesta de capacitación																				
6. Elaboración de propuestas de proyectos y planes de acción																				
7. Definición de responsables.																				
VERIFICAR:																				
1. Revisión de métricas e indicadores																				
2. Revisión del nivel de riesgo residual																				
3. Llevar a cabo una auditoría interna SGSI.																				
ACTUAR (Mejora Continua):																				
1. Definir e implementar mejoras																				
2. Ejecutar acciones correctivas y preventivas.																				
3. Comunicar resultados a los StakeHolders																				
4. Asegurar el cumplimiento																				

9.10 ANEXO 10 - INEISGSI07 - Evaluación de Riesgos

INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

ODEI LAMBAYEQUE

EVALUACIÓN DE RIESGOS

INFORMACIÓN DEL DOCUMENTO	
Evaluación de riesgos	**Código:** INEISGSI07 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 09/10/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** APROBADO **Por:** Ing. Cancino Castañeda Daniel Ismael
Archivo: INEISGSI07 - Evaluación de riesgos.xlsx	

HISTORIAL DE MODIFICACIONES

(Registro de cambios)

Versión #	Realizado por	Fecha Revisión	Aprobado por	Fecha Aprobación	Observación
1.0	Nilton Rogger Niño Morante	09/10/17	Ing. Cancino Castañeda Daniel Ismael	09/10/17	Descripción básica del documento.

INEISGSI07 – EVALUACIÓN DE RIESGOS

✓ CARACTERIZACIÓN

INEISGSI09 - EVALUACIÓN DE RIESGOS						
TIPO DE ACTIVO	**Código**	**Descripción**	**Unidad**	**Responsable**	**Ubicación**	**Cant.**
Esencial						
Documentos de IPC	E-01	Es el documento en físico que reporta los precios de los productos de una canasta familiar, el INEI filial Lambayeque generando el indicador macroeconómico, que es realizado mensualmente	Dirección Ejecutiva de Difusión Estadística	Jefe Dirección Ejecutiva de Difusión Estadística	ODEI Lambayeque	1
Documento de Compendio Estadístico del Departamento	E-02	Es el documento en físico Informe de los diversos sectores de la actividad pública y de algunas empresas de todo el departamento de Lambayeque demostrando como está la actividad económica y social en el departamento y que dicha información, sirva como herramienta para la toma de decisiones al estado peruano	Dirección Ejecutiva de Producción Estadística	Jefe Dirección Ejecutiva de Producción Estadística	ODEI Lambayeque	1
Documento de Evolución de las Actividades de Producción	E-03	El documento físico que se genera para mostrar la evolución de la producción sectorial, dicho informe está dirigido a los principales agentes productivos del sector del departamento de Lambayeque	Dirección Ejecutiva de Producción Estadística	Jefe Dirección Ejecutiva de Producción Estadística	ODEI Lambayeque	1
Documento de Registro Nacional de Municipalidades	E-04	Documento físico que contiene información a la infraestructura municipal, recursos humanos, planificación municipal, licencias de funcionamiento y edificación, saneamiento ambiental y salubridad, educación y cultura, salud, programas sociales, seguridad ciudadana, defensa civil, etc.	Dirección Ejecutiva de Producción Estadística	Jefe Dirección Ejecutiva de Producción Estadística	ODEI Lambayeque	1
Datos / Información						
Documento de Centro Documentario	D1	Documentos en físico	Dirección Ejecutiva de Difusión Estadística	Jefe Dirección Ejecutiva de Difusión Estadística	ODEI Lambayeque	variable
Información de Recursos Humanos	D2	Documento en físico e información digital (Excel)	O.T. de Administración	Encargado de Administración	ODEI Lambayeque	variable
Módulo contable	D3	Documento en físico e información digital (Excel)	O.T. de Administración	Encargado de Administración	ODEI Lambayeque	variable
Inventario de hardware	D4	Documentos en físico e información digital (Excel)	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	variable
Bandeja de correos electrónicos	D5	Información digital.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	variable

Claves criptográficas						
Contraseñas de sistema IPC	C1	Claves de usuarios para entrar a los módulos de IPC.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	2
Contraseñas de correos electrónicos Institucional	C2	Clave de usuarios de dominio propio para los correos de los empleados de las áreas de producción y difusión estadística.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	37
Servicios						
Escuela de Capacitación	S1	Laboratorio de computo que ofrece los servicios de capacitación de los diferente SW en el mercado	O.T. de Informática	Jefe del O.T. de Informática	ODEI Lambayeque	1
Información de Estadística	S2	Biblioteca al público donde se muestra la información estadística generada por el INEI - Lambayeque	Dirección Ejecutiva de Difusión Estadística	Secretaria IV (Difusión Estadística)	ODEI Lambayeque	1
Aplicaciones informáticas (software)						
Sistema IPC	A1	Sistema IPC (Índice de precio consumidor) No se tiene código fuente.	Dirección Ejecutiva de Difusión Estadística	Encargado de soporte	ODEI Lambayeque	1
Sistema de Control Encomienda	A2	Sistema de Control de Encomiendas enviadas a los ODEI de los distintos departamentos.	O.T. de Administración	Encargado de soporte	ODEI Lambayeque	1
Equipamiento informático (hardware)						
Servidor Data Center	EI1	Pc compatible que contiene las aplicaciones informáticas que tiene la organización.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	1
PCs de Escritorio	EI2	Equipos de cómputo distribuidos en las áreas correspondientes del Departamento de INEI y laboratorios de cómputo.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	68
PCs Portátiles	EI3	Laptops disponibles para las áreas correspondientes y la utilización de diversas direcciones del Departamento del INEI.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	10
Proyectores	EI4	Proyectores disponibles para las áreas correspondientes y la utilización de diversos eventos del CIP.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	10

Redes de comunicaciones						
Cableado de red	RC1		O.T. de Informática	Encargado de soporte	ODEI Lambayeque	-
Router	RC2		O.T. de Informática	Encargado de soporte	ODEI Lambayeque	1
Switch	RC3		O.T. de Informática	Encargado de soporte	ODEI Lambayeque	4
Hub	RC4		O.T. de Informática	Encargado de soporte	ODEI Lambayeque	1
Soportes de información						
Discos duros externos	SI1	Para realizar copias de seguridad.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	2
DVDs	SP2	Instaladores	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	Variables
Equipamiento auxiliar						
Impresoras	EA1	Impresoras para las áreas correspondientes del CIP.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	5
Cámaras de seguridad	EA2	Instaladas en los pisos del CIP.	O.T. de Informática	Encargado de soporte	ODEI Lambayeque	3
Instalaciones						
Local del ODEI Lambayeque	I1	Edificio de 2 pisos	Dirección	Director Departamental	ODEI Lambayeque	1
Personal						
Director de Sistema Administ. IV (Director Departamental)	P-01	Director departamental	-	INEI Lima	ODEI Lambayeque	1
Asistente Administrativo II	P-02	Secretaria	Dirección	Director Departamental	ODEI Lambayeque	1
Director de Sistema Administ. II (Jefe Dirección Ejecutiva de Difusión Estadística)	P-03	Jefe Dirección Ejecutiva de Difusión Estadística	Dirección	Director Departamental	ODEI Lambayeque	1
Asistente Serv. Eco. Finan. I	P-04	Pertenece a Difusión estadística	Dirección	Director Departamental	ODEI Lambayeque	1
Técnico en Estadística II	P-05	Pertenece a Difusión estadística	Dirección	Director Departamental	ODEI Lambayeque	2
Secretaria IV	P-06	Pertenece a Difusión estadística	Dirección	Director Departamental	ODEI Lambayeque	1

Director de Sistema Administ. II (Dirección Ejecutiva de Producción Estadística)	P-07	Dirección Ejecutiva de Producción Estadística	Dirección	Director Departamental	ODEI Lambayeque	1
Asistente Serv. Econ. Finan. II	P-08	Pertenece a Producción Estadística	Dirección	Director Departamental	ODEI Lambayeque	2
Asistente Administrativo I	P-09	Pertenece a Producción Estadística	Dirección	Director Departamental	ODEI Lambayeque	1
Operador PAD III	P-10	Pertenece a Producción Estadística	Dirección	Director Departamental	ODEI Lambayeque	2
Coordinador de Proyectos	P-11	Proyectos de Censos y Encuestas	Dirección	Director Departamental	ODEI Lambayeque	1
Encuestador	P-12	Proyectos de Censos y Encuestas	Dirección	Director Departamental	ODEI Lambayeque	Variable
Jefe del O.T. de Administración	P-13	Pertenece a O.T. de Administración	Dirección	Director Departamental	ODEI Lambayeque	1
Secretaria	P-14	Pertenece a O.T. de Administración	Dirección	Director Departamental	ODEI Lambayeque	1
Jefe del O.T. de Informática	P-15	Pertenece a O.T. de Informática	Dirección	Director Departamental	ODEI Lambayeque	1
Encargado de Soporte	P-16	Pertenece a O.T. de Informática	Dirección	Director Departamental	ODEI Lambayeque	1

Los detalles de la evaluación de riesgos a continuación:

a. Esenciales
b. Datos – Información
c. Claves Criptográficas
d. Servicios
e. Aplicaciones Informáticas
f. Equipamiento Informático
g. Redes de Comunicación
h. Soporte de Información
i. Equipamiento Auxiliar
j. Instalaciones
k. Personal

Leyenda

A continuación, se presentan las tablas con las escalas de valoración de disponibilidad, integridad, confidencialidad, impacto, probabilidad, respuesta al riesgo y rangos de nivel de riesgo:

D: DISPONIBILIDAD	
VALOR	CLASIFICACIÓN
3	Alta
2	Media
1	Baja

I: INTEGRIDAD	
VALOR	CLASIFICACIÓN
3	Alta
2	Media
1	Baja

C: CONFIDENCIALIDAD	
VALOR	CLASIFICACIÓN
3	Alta
2	Media
1	Baja

V: VALORACIÓN

Formula = (Confidencialidad x 1/3 + Integridad x 1/3 + Disponibilidad x 1/3) * 10
Es decir:
V = (C x 33% + I x 33% + D x 33%) x 10

IMPACTO	
VALOR	CATEGORÍA
1	Muy bajo
2	Bajo
3	Intermedio
4	Alto
5	Muy alto

PROBABILIDAD	
VALOR	CATEGORÍA
1	Imposible
2	Poco probable
3	Viable
4	Probable
5	Muy probable

RESPUESTA AL RIESGO	
1	Evitar
2	Transferir
3	Mitigar
4	Aceptar

RI: RIESGO INHERENTE
Formula = Nivel de Impacto x Nivel de Probabilidad
Es decir:
RI = Nivel de Impacto x Nivel de Probabilidad

Donde:
C = Confidencialidad **I** = Integridad **D** = Disponibilidad **V** = Valoración **RI** = Riesgo inherente

a. Esenciales

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Documentos de IPC	3	3	3	10	Inexistente / Escaso control de acceso a documentación	Colaboradores desleales / personal externo	Fuga de información	4	Alto	3	Viable	**12**	Establecer políticas para el control de acceso. Generar bitácora para entrada y salida de documentación	Mitigar
	3	3	3	10	Falta de un debido control de acceso a usuarios y de una protección física	Alteración de la información	Corrupción de la información	4	Alto	3	Viable	**12**		Mitigar
Documento de Compendio Estadístico del Departamento	3	3	3	10	Inexistente / Escaso control de acceso a documentación	Colaboradores desleales / personal externo	Fuga de información	5	Muy alto	4	Probable	**20**	Establecer políticas para el control de acceso. Generar bitácora para entrada y salida de documentación	Mitigar
	3	3	3	10	Insuficiente entrenamiento de empleados	Alteración de la información	Corrupción de la información	5	Muy alto	4	Probable	**20**		Mitigar
Documento de Evolución de las Actividades de Producción	3	3	3	10	Inexistente / Escaso control de acceso a documentación	Colaboradores desleales / personal externo	Fuga de información	5	Muy alto	4	Probable	**20**	Establecer políticas para el control de acceso. Generar bitácora para entrada y salida de documentación	Mitigar
	3	3	3	10	Insuficiente entrenamiento de empleados	Alteración de la información	Corrupción de la información	5	Muy alto	4	Probable	**20**		Mitigar
Documento de Registro Nacional de Municipalidades	3	3	3	10	Inexistente / Escaso control de acceso a documentación	Colaboradores desleales / personal externo	Fuga de información	5	Muy alto	3	Viable	**15**	Establecer políticas para el control de acceso. Generar bitácora para entrada y salida de documentación	Mitigar
	3	3	3	10	Falta de un debido control de acceso a usuarios y de una protección física	Alteración de la información	Corrupción de la información	5	Muy alto	3	Viable	**15**		Mitigar

b. Datos – Información

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Documento de Centro Documentario	3	3	2	9	Inexistente / Escaso control de acceso a documentación	Colaboradores desleales / personal externo	Fuga de información	5	Muy alto	3	Viable	**15**	Establecer políticas para el control de acceso. Generar bitácora para entrada y salida de documentación	Mitigar
	3	3	2	9	Almacenamiento no protegido	Ingreso no autorizado del equipo	Corrupción de la información	5	Muy alto	3	Viable	**15**		Mitigar
Información de Recursos Humanos	3	2	2	8	Controles de seguridad deficientes / inexistentes	Colaboradores desleales / piratas informáticos	Fuga de información	4	Alto	3	Viable	**12**	Establecer controles de seguridad para la información digitalizada	Mitigar
	3	2	2	8	Insuficiente entrenamiento de empleados	Manipulación de la información	Corrupción de la información	4	Alto	3	Viable	**12**		Mitigar
Módulo contable	3	3	2	9	Controles de seguridad deficientes / inexistentes	Colaboradores desleales / piratas informáticos	Fuga de información	4	Alto	3	Viable	**12**	Establecer controles de seguridad para la información digitalizada	Mitigar
	3	3	2	9	Almacenamiento no protegido	Ingreso no autorizado del equipo	Corrupción de la información	4	Alto	3	Viable	**12**		Mitigar
Inventario de hardware	3	2	2	8	Controles de seguridad deficientes / inexistentes	Colaboradores desleales / piratas informáticos	Fuga de información	3	Intermedio	3	Viable	**9**	Establecer controles de seguridad para la información digitalizada	Mitigar
	3	2	2	8	Almacenamiento no protegido	Ingreso no autorizado del equipo	Corrupción de la información	3	Intermedio	3	Viable	**9**		Mitigar
Bandejas de correos electrónicos	3	3	2	9	Inexistencia de política de contraseñas / Contraseñas débiles	Piratas informáticos	Acceso no autorizado a bandejas de correo electrónico	4	Alto	3	Viable	**12**	Establecer política de contraseñas	Mitigar

c. Claves Criptográficas

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Contraseñas del Sistema IPC	2	2	1	6	Contraseñas Débiles	Colaborador insatisfecho / desleal	Fuga de información	3	Intermedio	3	Viable	**9**	Políticas de seguridad en el manejo de contraseñas	Mitigar
	2	2	1	6	Insuficiente entrenamiento de empleados	Alteración de la información	Corrupción de la información	3	Intermedio	3	Viable	**9**		Mitigar
Contraseñas de correos electrónicos Institucional	3	3	2	9	Incorrecta Gestión de Contraseñas	Colaborador insatisfecho / desleal	Fuga de información	5	Muy alto	3	Viable	**15**	Políticas de seguridad en el manejo de contraseñas	Mitigar
	2	2	1	6	Usurpación de identidad	Acceso no autorizado	Corrupción de la información	5	Muy alto	3	Viable	**15**		Mitigar

d. Servicios

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Escuela de Capacitación	2	3	3	9	Infraestructura tecnológica desfasada / inadecuada	Instituciones educativas	Deserción / escasez de estudiantes	4	Alto	3	Viable	**12**	Plan de adquisición de parque informático.	Mitigar
Información de Estadística	2	3	3	9	Inexistente / Escaso control de acceso a documentación	Personal externo malintencionado	Pérdida de libros / folletos / boletines informativos	4	Alto	3	Viable	**12**	Establecer políticas para el control de acceso. Generar bitácora para entrada y salida de documentación	Mitigar

e. Aplicaciones Informáticas

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Sistema IPC	2	3	2	8	Error de configuración del sistema IPC	Ataque software Malicioso	Perdida de la información.	5	Muy alto	3	Viable	**15**	Auditorías a la información contenida en el sistema utilizados en el área de difusión estadística/ Plan de respaldo de información.	Mitigar
	2	3	2	8	Falta de backups de información	Manipulación de información con software	Alteración de la Información	5	Muy alto	3	Viable	**15**		

Sistema de Control Encomienda	2	3	1	7	Digitalización de Datos Incorrectos.	Manipulación / robo / pérdida de la información	Información no actualizada	4	Alto	3	Viable	**12**	Asignación de perfiles en el sistema de acuerdo con las funciones que se va a desempeñar	Mitigar

f. Equipamiento Informático

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Servidor Data Center	3	3	3	10	Mantenimiento irregulares o inexistente de SW o HW	Malware (virus ransomware)	Encriptación del Servidor por Malware	5	Muy alto	3	Viable	15	Instalación de parches de software para servidores (Actualización de Sistema Operativo)	Mitigar
	3	3	3	10	Ambiente inadecuado para su operatividad	Corte del suministro eléctrico	Pérdida de la disponibilidad	5	Muy alto	3	Viable	15	Implementación de Infraestructura para la red Eléctrica de UPS y Cableado Estructurado.	Mitigar
PCs de Escritorio	2	3	3	9	Ausencia de respaldo de Información	Averías Físicas.(mecánicos o eléctricos) y lógicas (formateos)	Pérdida o robo de Información	4	Alto	3	Viable	12	Plan Anual de mantenimiento de los equipos informáticos y plan de Respaldo de Información en la Nube	Mitigar
	2	3	3	9	Mantenimiento irregular o inexistente de HW y SW	Malware (virus ransomware)	Encriptación de PC por malware	4	Alto	3	Viable	12	Instalación de parches de software para servidores (Actualización de Sistema Operativo)	Mitigar
PCs Portátiles	2	2	2	7	Ausencia de respaldo de Información	Averías Físicas.(mecánicos o eléctricos) y lógicas (formateos)	Pérdida o robo de Información	4	Alto	3	Viable	12	Plan Anual de mantenimiento de los equipos informáticos y plan de Respaldo de Información en la Nube	Mitigar
	2	2	2	7	Mantenimiento irregular o inexistente de HW y SW	Malware (virus ransomware)	Encriptación de PC por malware	4	Alto	3	Viable	12	Instalación de parches de software para servidores (Actualización de Sistema Operativo)	Mitigar
Proyectores	1	1	1	3	Mantenimiento irregulares o inexistente de HW.	Corte del suministro eléctrico	Inoperatividad	3	Muy bajo	3	Poco probable	9	Plan de mantenimiento de los equipos informáticos	Mitigar

g. Redes de Comunicación

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Router	2	2	3	8	Verificación irregular / inexistente	Daños / Averías	Caída / indisponibilidad de servicios informáticos	4	Alto	3	Viable	12	Plan de adquisición de parque informático.	Mitigar
					Configuraciones de seguridad inexistentes / incorrectas	Piratas informáticos	Manipulación configuración / Pérdida de servicio	5	Muy alto	3	Viable	15	Contratación de especialista de seguridad para configuraciones de seguridad. Respaldo de archivo de configuración.	Transferir
Switch	2	2	2	7	Verificación irregular / inexistente	Daños / Averías	Caída / indisponibilidad de servicio	4	Alto	3	Viable	12	Plan de adquisición de parque informático.	Mitigar
Cableado de red	2	2	2	7	Exposición / deterioro / desorden	Desastres naturales / artificiales	Pérdida de servicio	4	Alto	3	Viable	12	Planificación para aplicación de cableado estructurado	Mitigar
Hub				0	Verificación irregular / inexistente	Daños / Averías	Caída / indisponibilidad de servicio	3	Intermedio	3	Viable	9	Plan de adquisición de parque informático.	Aceptar

El plan de adquisición de parque informático abarca también considerar los respaldos de los equipos críticos, en este caso también el reemplazo de los hubs cuando se malogren por Switch y a la larga se eliminarán, los hubs son equipos obsoletos e inservibles.

h. Soporte de Información

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Discos Duros Externos	2	2	2	7	Verificación irregular / inexistente	Daño / Avería	Pérdida de información	4	Alto	3	Viable	12	Planificación para revisión de discos duros externos. Plan de adquisición de parque informático.	Mitigar
DVDs	2	2	1	6	Verificación irregular / inexistente	Daño / Avería	Pérdida de información	3	Intermedio	3	Viable	9	Planificación para revisión de DVDs. Plan de adquisición de parque informático.	Mitigar

i. Equipamiento Auxiliar

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Impresoras	1	2	1	4	Mantenimiento irregular o inexistente de HW.	Corte del suministro eléctrico.	Inoperatividad	4	Alto	3	Viable	12	Plan para el uso de los activos asociados a la infraestructura.	Mitigar
	1	2	1	4	Ausencia de Controles de impresión (Que persona puede imprimir)	personal externo (pueda imprimir en la institución)	Fuga de Información	4	Alto	3	Viable	12		Mitigar
Cámaras de seguridad	2	3	3	8.9	Control de acceso a las cámaras inadecuada	Piratas Informáticos	Intromisión en tiempo real (Terceros de las actividades de los trabajadores)	5	Muy alto	4	Probable	20	Establecer políticas de configuración de seguridad de las cámaras	Mitigar

j. Instalaciones

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categoría			
Local del ODEI Lambayeque	1	3	3	8	Control de acceso deficiente	Robos / Daños	Sustracción de documentación / bienes	4	Alto	3	Viable	12	Establecer políticas para el control de acceso.	Mitigar
					Cableado eléctrico antiguo	Cortos circuitos / Incendios	Pérdida / daño de bienes	4	Alto	3	Viable	12	Elaborar plan para revisión de cableado eléctrico	Mitigar

k. Personal

ACTIVO	C	I	D	V	VULNERABILIDAD	AMENAZAS	RIESGO	Impacto		Probabilidad		RI	CONTROLES / SALVAGUARDA	Respuesta al riesgo
								Nivel	Categoría	Nivel	Categ.			
Director de Sistema Administ. IV (Director Departamental)	3	3	3	10	Desconocimiento de políticas de seguridad de información	Abuso de privilegios de acceso	Divulgación de Información sensible	5	Muy alto	3	Viable	15	- Elaborar cronograma de capacitación de políticas de seguridad de información. - Elaborar controles de seguridad de información.	Mitigar
Asistente Administrativo II	3	3	3	10	Desconocimiento de políticas para la recepción de datos	Colaboradores desleales	Divulgación de la Información sensible	4	Alto	3	Viable	12	- Elaborar cronograma de capacitación de políticas de seguridad de información.	Mitigar

Director de Sistema Administ. II (Jefe Dirección Ejecutiva de Difusión Estadística)	3	3	3	10	Desconocimiento de políticas de seguridad	Abuso de privilegios de acceso	Divulgación de la Información sensible	5	Muy alto	3	Viable	15	- Elaborar cronograma de capacitación de políticas de seguridad de información. - Elaborar controles de seguridad de información.	Mitigar
Asistente Serv. Eco. Finan. I	3	3	3	10	Desconocimiento técnico de los equipos	Colaboradores desleales, delincuentes	Divulgación / Daño de Información sensible	4	Alto	3	Viable	12	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información - Elaborar cronograma de capacitación de políticas de seguridad de información. - Elaborar controles de seguridad de información.	Mitigar
	3	3	3	10	Falta de capacitación al personal	Abuso de privilegios de acceso	Escaso personal para las operaciones	4	Alto	3	Viable	12		Mitigar
Técnico en Estadística II	3	3	3	10	Desconocimiento técnico de los equipos	Colaboradores desleales, delincuentes	Divulgación / Daño de Información sensible	3	Intermedio	3	Viable	9	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información. - Elaborar cronograma de capacitación de políticas de seguridad de información. - Elaborar controles de seguridad de información.	Mitigar
	3	3	3	10	Falta de personal capacitado	Abuso de privilegios de acceso	Escaso personal para las operaciones	3	Intermedio	3	Viable	9		Mitigar
Secretaria IV	3	3	3	10	Desconocimiento de políticas para la recepción de datos	Colaboradores desleales, delincuentes	Divulgación de la Información sensible	4	Alto	3	Viable	12	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información.	Mitigar
Director de Sistema Administ. II (Dirección Ejecutiva de Producción Estadística)	3	3	3	10	Desconocimiento de políticas de seguridad	Abuso de privilegios de acceso	Divulgación de la Información sensible	5	Muy alto	3	Viable	15	- Elaborar cronograma de capacitación de políticas de seguridad de información. - Elaborar controles de seguridad de información.	Mitigar
Asistente Serv. Econ. Finan. II	3	3	3	10	Falta de cultura de seguridad	Colaboradores desleales, delincuentes	Divulgación / Daño de Información sensible	4	Alto	3	Viable	12	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información. - Elaborar cronograma de capacitación de políticas de seguridad de información. - Elaborar controles de seguridad de información. - Medir el nivel de satisfacción de los colaboradores	Mitigar
	3	3	3	10	Falta de personal capacitado	Abuso de privilegios de acceso	Escaso personal para las operaciones	4	Alto	3	Viable	12		
Asistente Administrativo I	3	3	3	10	Desconocimiento técnico de los equipos	Colaboradores desleales, delincuentes	Divulgación / Daño de Información sensible	4	Alto	3	Viable	12	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información. - Elaborar cronograma de capacitación de	Mitigar

	3	3	3	10	Falta de personal capacitado	Abuso de privilegios de acceso	Escaso personal para las operaciones	4	Alto	3	Viable	12	políticas de seguridad de información. - Elaborar controles de seguridad de información. - Medir el nivel de satisfacción de los colaboradores.	
Operador PAD III	3	3	3	10	Falta de cultura de seguridad	Colaboradores desleales, delincuentes	Divulgación de la Información sensible	3	Intermedio	3	Viable	9	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información.	Mitigar
Coordinador de Proyectos	3	3	3	10	Desconocimiento de políticas de seguridad	Abuso de privilegios de acceso	Divulgación de Información sensible	5	Muy alto	3	Viable	15	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información.	Mitigar
Encuestador	3	3	3	10	Desconocimiento técnico de los equipos	Colaboradores desleales, delincuentes	Divulgación / Daño de Información sensible	3	Intermedio	3	Viable	9	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información.	Mitigar
Jefe del O.T. de Administración	3	3	3	10	Desconocimiento de políticas de seguridad	Abuso de privilegios de acceso	Divulgación / Daño de Información sensible	5	Muy alto	3	Viable	15	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información. - Elaborar controles de seguridad de información.	Mitigar
Secretaria	3	3	3	10	Desconocimiento de políticas para la recepción de datos	Colaboradores desleales, delincuentes	Divulgación de Información sensible	3	Intermedio	3	Viable	9	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información.	Mitigar
Jefe de O.T. de Informática	3	3	3	10	Desconocimiento de políticas de seguridad	Abuso de privilegios de acceso	Divulgación / Daño de Información sensible	5	Muy alto	3	Viable	15	Elaborar controles de seguridad de información	Mitigar
Encargado de Soporte	3	3	3	10	Desconocimiento técnico de los equipos	Colaboradores desleales, delincuentes	Divulgación de Información sensible	4	Alto	3	Viable	12	- Establecer políticas, reglas y procedimientos relacionadas con la seguridad de la información.	Mitigar

9.11 ANEXO 11 - INEISGSI08 - Plan de Tratamiento del Riesgo

INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

ODEI LAMBAYEQUE

PLAN DE TRATAMIENTO DEL RIESGO

INFORMACIÓN DEL DOCUMENTO	
Plan de tratamiento del riesgo	**Código:** INEISGSI08 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 13/10/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** APROBADO **Por:** Ing. Cancino Castañeda Daniel Ismael
Archivo: INEISGSI08 - Plan de tratamiento del riesgo.xlsx	

HISTORIAL DE MODIFICACIONES

(Registro de cambios)

Versión #	Realizado por	Fecha Revisión	Aprobado por	Fecha Aprobación	Observación
1.0	Nilton Rogger Niño Morante	12/10/17	Ing. Cancino Castañeda Daniel Ismael	13/10/17	Descripción básica del documento.

INEISGSI08 - PLAN DE TRATAMIENTO DEL RIESGO

Una vez identificados aquellos riesgos que amenazan a la institución de ODEI Lambayeque, se deberá evaluar con la ayuda de la NTP ISO/IEC 27001:2014, cuales son los controles que se deben implementar para el tratamiento de riesgos.

✓ **Leyenda**

ESTRATEGIA [E]		
A	Aceptar	En este escenario se decide no tratar el riesgo debido a no haber identificado controles adecuados para el tratamiento de los riesgos o haber identificado que el costo de implementar algún control es mayor que los beneficios que se obtendrán. Toda aceptación del riesgo debe ser documentada y firmada por el Comité de Seguridad de la Información indicando los criterios de esta decisión. Por último, deberán ser constantemente monitoreados en caso evolucionen y se conviertan en riesgos más graves.
E	Eliminar	Una de las alternativas más difíciles de implementar y más costosas ya que puede implicar la eliminación de un activo, proceso o del área del negocio que es fuente de riesgo. Este plan de tratamiento debe estar debidamente justificado y documentado en caso se decida implementar. Adicionalmente se debe realizar un nuevo Análisis de Riesgo teniendo en cuenta el cambio realizado en la organización.
M	Mitigar	En este escenario se debe reducir los riesgos mediante la ejecución de controles que reduzcan el riesgo a un nivel aceptable. Estos controles deberán presentar una documentación adecuada para su implementación y puesta en marcha.
T	Transferir	Alternativa más económica en caso sea muy costoso o difícil reducir o controlar un riesgo. Sin embargo, al transferir un riesgo no se transfiere las responsabilidades por lo que deberán ser constantemente monitoreadas para asegurarnos de su correcto tratamiento.

De igual forma, los controles pueden ser clasificados de la siguiente forma:

TIPO DE CONTROL [TC]		
C	Correctivo	Son controles que se encargan de corregir alguna incidencia minimizando el impacto del daño o pérdida originada por el riesgo, es decir facilitan la vuelta a la normalidad cuándo se han producido incidencias.
D	Detectivo	Cuando fallan los preventivos para tratar de conocer cuanto antes el evento, es decir son tipos de controles que busca descubrir nuevos riesgos antes que se materialicen, de tal forma, que puedan ser controlados con anticipación.
P	Preventivo	Para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema, estos son controles que buscan prevenir la materialización de un riesgo, mediante un adecuado control de las vulnerabilidades de un activo.

FRECUENCIA [FRE]		
P.Ade	Periódico Adecuado	Planificar con periodicidad.
P.Ind	Periódico Inadecuado	Mantenimiento Rutinario.
P.Esp	Sorpresivo/Esporádico	Se hace con poca frecuencia.

MEJORA CONTINUA [MC]	
D	Diario
S	Semanal
B	Bimensual
QN	Quincenal
MN	Mensual
BM	Bimestral
TM	Trimestral
SM	Semestral
A	Anual
P	Permanente
NA	No Aplica

REGISTROS [REG]		
RegC	Genera Registros Conservados	Guardar copias de registros en forma de señales electrónicas en medios magnéticos o papel.
RegNC	Genera Registros No Conservados	No Guardar copias de registros en forma de señales electrónicas en medios magnéticos o papel.
NoReg	No Genera Registros	Ningún informe.

LEYENDA CABECERAS	
I	Impacto
P	Probabilidad
RR	Riesgo Residual
Res	Responsable

CONTROL DE DOCUMENTACIÓN [DOC]	
DocN	No Documentado
DocI	Documento Interno
DocF	Documento Formal

RIESGO RESIDUAL

RR= Impacto x Probabilidad

✓ **Plan de Tratamiento de Riesgos – Esenciales**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
ESENCIAL																		
DOCUMENTOS DE IPC	Fuga de información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe resguardar la información del departamento de Lambayeque.	A.5.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Total de documentos extraviados, dañados o copiados sin el permiso correspondiente / Trimestral	SM	3	3	9	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).	Encargado de soporte. Especialista en seguridad informática Coordinador de capacitaciones. Equipos tecnológicos de seguridad.	CIO / Director de seguridad de la información.
					A. 6.1.1	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 11.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
	Corrupción de la información	M			A. 11.1.3	***P***	***P.Ade***	***DocF***	***RegNC***		SM	3	3	9	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética cada **6 meses**).		
DOCUMENTO DE COMPENDIO ESTADÍSTICO DEL DEPARTAMENTO	Fuga de información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe resguardar la información del departamento de Lambayeque.	A.5.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Total de documentos extraviados, dañados o copiados sin el permiso correspondiente / Semestral	A	4	4	16	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).	Encargado de soporte. Especialista en seguridad informática Coordinador de capacitaciones. Equipos tecnológicos de seguridad.	CIO / Director de seguridad de la información.
					A.7.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 11.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
					A.13.2.3	***P***	***P.Ade***	***DocF***	***RegNC***									
	Corrupción de la información	M			A.7.2.2	***P***	***P.Ade***	***DocF***	***RegNC***		A	4	4	16	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética **anual**).		
					A.9.1.1	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 11.1.3	***P***	***P.Ade***	***DocF***	***RegNC***									

DOCUMENTO DE EVOLUCIÓN DE LAS ACTIVIDADES DE PRODUCCIÓN	Fuga de información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe resguardar la información del departamento de Lambayeque.	A.5.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Total de documentos extraviados, dañados o copiados sin el permiso correspondiente / Semestral	A	4	4	16	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).	Encargado de soporte.Especialista en seguridad informáticaCoordinador de capacitaciones.Equipos tecnológicos de seguridad.	CIO / Director de seguridad de la información.
					A.7.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 11.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
					A.13.2.3	***P***	***P.Ade***	***DocF***	***RegNC***									
	Corrupción de la información	M			A.7.2.2	***P***	***P.Ade***	***DocF***	***RegNC***		A	4	4	16	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética).		
					A.9.1.1	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 11.1.3	***P***	***P.Ade***	***DocF***	***RegNC***									
DOCUMENTO DE REGISTRO NACIONAL DE MUNICIPALIDADES	Fuga de información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe resguardar la información del departamento de Lambayeque.	A.5.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Total de documentos extraviados, dañados o copiados sin el permiso correspondiente / Trimestral	SM	4	3	12	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).	Encargado de soporte. Especialista en seguridad informática Coordinador de capacitaciones. Equipos tecnológicos de seguridad.	CIO / Director de seguridad de la información.
					A. 6.1.1	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 11.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
	Corrupción de la información	M			A. 11.1.3	***P***	***P.Ade***	***DocF***	***RegNC***		SM	4	3	12	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética cada **6 meses**).		

✓ **Plan de Tratamiento de Riesgos – Datos / Datos / Información**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
DATOS / INFORMACIÓN																		
DOCUMENTO DE CENTRO DOCUMENTARIO	Fuga de información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe custodiar la información y cumplir con los requerimientos legales.	A. 6.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Número de documentos perdidos, modificados, copiados sin autorización / Semestral	A	4	3	12	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).	Encargado de soporte. Especialista en seguridad de información.	CIO / Director de seguridad de la información.
					A. 11.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
	Corrupción de la información	M			A. 11.1.3	***P***	***P.Ade***	***DocF***	***RegNC***		A	4	3	12	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (**Programar** seminarios de ética **anual**).	Especialista en seguridad de información.	Director de seguridad de la información.
INFORMACIÓN DE RECURSOS HUMANOS	Fuga de información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe custodiar la información y cumplir con los requerimientos legales.	A. 6.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Cantidad de fugas o corrupción de información / Trimestral	SM	3	3	9	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).	Encargado de soporte. Especialista en seguridad de información.	CIO / Director de seguridad de la información.
					A. 11.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
	Corrupción de la información	M			A. 11.1.3	***P***	***P.Ade***	***DocF***	***RegNC***		SM	3	3	9	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética cada **6 meses**).	Especialista en seguridad de información.	Director de seguridad de la información.
MÓDULO CONTABLE	Fuga de información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe custodiar la información y cumplir con los	A. 6.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Cantidad de fugas o corrupción de información / Mes	TM	3	3	9	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).	Encargado de soporte. Especialista en seguridad de información.	CIO / Director de seguridad de la información.
					A. 11.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									

	Corrupción de la información	M			A. 11.1.3	***P***	***P.Ade***	***DocF***	***RegN C***		TM	3	3	9	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética **trimestral**).	Especialista en seguridad de información.	Director de seguridad de la información.
INVENTARIO DE HARDWARE	Fuga de información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe custodiar la información y cumplir con los requerimientos legales.	A. 6.1.1	***P***	***P.Ade***	***DocF***	***RegN C***	Cantidad de fugas o corrupción de información / Semestral	A	2	3	6	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles para incrementar la seguridad de los activos de información críticos con el propósito de mantener su confidencialidad, integridad y disponibilidad. Tales como control de acceso (privilegios y bitácoras) y de seguridad del respaldo de los medios que contienen la información (física y virtual).	Encargado de soporte. Especialista en seguridad de información.	CIO / Director de seguridad de la información.
	Corrupción de la información	M			A. 11.1.3	***P***	***P.Ade***	***DocF***	***RegN C***		A	2	3	6	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética **anual**).	Especialista en seguridad de información.	Director de seguridad de la información.
BANDEJAS DE CORREOS ELECTRÓNICOS	Acceso no autorizado a bandejas de correo electrónico	M	Objetivos de seguridad de la información / Requerimiento legal.	Las bandejas de correo electrónico deben ser custodiadas.	A. 6.1.1	***P***	***P.Ade***	***DocI***	***RegN C***	Número de bandejas accedidas sin autorización / Mes	TM	3	3	9	Establecer políticas de contraseñas robustas para sistemas informáticos y correos institucionales	Definir políticas, procedimientos e implementar mecanismos de seguridad para las cuentas y sistemas, además de capacitar al personal en la gestionar contraseñas fuertes. Definir contraseña para cada usuario(que no se comparta).	Especialista en seguridad de información.	Director de seguridad de la información.
					A. 6.1.4	***P***	***P.Ade***	***DocI***	***RegN C***									
					A. 7.2.2	***P***	***P.Ade***	***DocI***	***RegN C***									

✓ **Plan de Tratamiento de Riesgos – Datos / Claves criptográficas**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
CLAVES CRIPTOGRÁFICAS																		
CONTRASEÑAS DE SISTEMA IPC	Fuga de información	M	Objetivos de Negocio/ objetivo de seguridad de información	La institución debe gestionar el uso y administración de las contraseñas para la protección de la información en la institución	A. 6.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de accesos no autorizados/ Trimestral	SM	2	3	6	Establecer políticas de contraseñas robustas para sistemas informáticos y correos institucionales	Definir políticas, procedimientos e implementar mecanismos de seguridad para las cuentas y sistemas, además de capacitar al personal en la gestionar contraseñas fuertes. Definir contraseña para cada usuario(que no se comparta).	Especialista en seguridad informática	CIO
					A. 7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A. 10.1.1	***P***	***P.Ade***	***DocI***	***RegC***									
					A. 10.1.2	***P***	***P.Ade***	***DocI***	***RegC***									
					A. 16.1.1	***P***	***P.Ade***	***DocI***	***RegC***									
	Corrupción de la información	M			A. 11.1.3	***P***	***P.Ade***	***DocI***	***RegC***		SM	2	3	6				
CONTRASEÑAS DE CORREOS ELECTRÓNICOS INSTITUCIONAL	Fuga de información	M	Objetivos de Negocio/ objetivo de seguridad de información	La institución debe gestionar el uso y administración de las contraseñas para la protección de la información en la institución	A. 6.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de accesos no autorizados/ mes	TM	3	3	9	Establecer políticas de contraseñas robustas para sistemas informáticos y correos institucionales	Definir políticas, procedimientos e implementar mecanismos de seguridad para las cuentas y sistemas, además de capacitar al personal en la gestionar contraseñas fuertes. Definir contraseña para cada usuario(que no se comparta).	Especialista en seguridad informática	CIO
					A. 7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.9.4.3	***P***	***P.Ade***	***DocF***	***RegC***									
					A. 10.1.1	***P***	***P.Ade***	***DocI***	***RegC***									
					A. 10.1.2	***P***	***P.Ade***	***DocI***	***RegC***									
					A. 16.1.1	***P***	***P.Ade***	***DocI***	***RegC***									
	Corrupción de la información	M			A. 11.1.3	***P***	***P.Ade***	***DocI***	***RegC***		TM	4	3	12				

✓ **Plan de Tratamiento de Riesgos – Datos / Servicios**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
SERVICIOS																		
ESCUELA DE CAPACITACIÓN	Deserción / escasez de estudiantes	M	Objetivos de negocio	Se requiere crecimiento de la escuela de capacitación, como uno de los objetivos estratégicos de la institución	A. 6.1.1	***C***	***P.Ade***	***DocI***	***RegNC***	Cantidad de estudiantes desertados / Por capacitación	SM	3	3	9	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	**Añadir** la mejorar la infraestructura tecnológica para capacitaciones	Coordinador de capacitaciones. Encargado de soporte	Director de seguridad de la información.
					A. 7.2.2	***C***	***P.Ade***	***DocI***	***RegNC***									
INFORMACIÓN DE ESTADÍSTICA	Pérdida de libros / folletos / boletines informativos	M	Objetivos de seguridad de la información	La documentación con información sensible y clasificada deberá permanecer en la institución	A. 6.1.1	***C***	***P.Ade***	***DocI***	***RegC***	Cantidad de libros / folletos / boletines extraviados / mes	SM	3	3	9	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles de seguridad para incrementar la seguridad de los activos de información críticos. Por ejemplo custodiar documentos bajo llave.	Especialista en seguridad informática	CIO
					A. 7.2.2	***C***	***P.Ade***	***DocI***	***RegC***									

✓ **Plan de Tratamiento de Riesgos – Datos / Aplicaciones Informáticas (software)**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
Aplicaciones Informáticas (software)																		
SISTEMA IPC	Perdida de la Información	M	Objetivos de seguridad de la información / Requerimiento legal	La institución debe asegurar la disponibilidad e integridad de la información y cumplir con los requerimientos legales.	A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***	Cantidad de registros perdidos / Trimestral	SM	4	3	12	Implementación de un Sistema Integrado de Gestión.	Implementar programas de auditoria para el adecuado tratamiento de la información en los sistemas y sus activos asociados y contratar servicios de hackeo ético.	Encargado de sistemas. Oficial de seguridad de la información.	CIO
					A.12.3.1	***P***	***P.Ade***	***DocF***	***RegC***									
	Alteración de la Información	M			A.5.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Cantidad de registros alterados / mes	TM	4	3	12				
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.9.4.1	***P***	***P.Ade***	***DocF***	***RegC***									
					A.9.1.1	***P***	***P.Ade***	***DocF***	***RegC***									
SISTEMA DE CONTROL ENCOMIENDA	Información no actualizada	M	Objetivos de seguridad de la información.	La institución debe controlar la información sobre el ingreso/salida de las encomiendas, dicha información debe estar siempre actualizada.	A.5.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Cantidad de entregas o Recepciones erradas / Mes	TM	3	3	9	Implementación de un Sistema Integrado de Gestión.	**Incluir** en el programa la gestión de perfiles para un mejor control de las operaciones de sistemas de encomienda, permitiendo un tratamiento de la información correcto y uso aceptable de los activos.	Encargado de sistemas. Oficial de seguridad de la información.	CIO
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.9.2.2	***P***	***P.Ade***	***DocF***	***RegC***									

✓ **Plan de Tratamiento de Riesgos – Datos / Equipamiento informático (hardware)**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
Equipamiento informático (hardware)																		
SERVIDOR DATA CENTER	Encriptación del Servidor por Malware	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe custodiar la información del servidor, asegurar su integridad y velar por la disponibilidad de la misma, además cumplir con los requerimientos legales	A.12.2.1	***P***	***P.Ade***	***DocF***	***RegNC***	Número malware detectado / mes	BM	4	3	12	Plan para la adquisición de licencias antivirus y antimalware de estaciones de trabajo y servidor institucional	Plan para la adquisición e instalación de antivirus y antimalware. Así como la instalación de Actualizaciones del Sistema Operativo (Parches).	Encargado de soporte. Encargado de sistemas.	CIO.
					A.16.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 17.1.1	***P***	***P.Ade***	***DocF***	***RegNC***									
	Pérdida de la disponibilidad	M	Objetivos de seguridad de la información.	Asegurar el menor tiempo posible en restablecer las operaciones del servicio.	A. 11.1.4	***P***	***P.Ade***	***DocF***	***RegNC***	Número de incidencias (hardware y software) / mes.	TM	5	2	10	Diseño e Implementación de controles de Acceso y de áreas seguras.	**Adicionar** al diseño y la implementación una infraestructura con las condiciones de seguridad y ambiente adecuado(red eléctrica, ups, cableado estructurado y aire acondicionado), así como la implementación de estructura redundante.	Encargado de soporte. Encargado de colegiatura. Coordinador de capacitaciones. Equipos tecnológicos de seguridad.	CIO / Director de seguridad de la información.
					A.17.2.1	***P***	***P.Ade***	***DocF***	***RegNC***									
PCS DE ESCRITORIO	Perdida o robo de Información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe custodiar la información de las computadoras y cumplir con los requerimientos legales.	A.9.2.3	***P***	***P.Ade***	***DocF***	***RegNC***	Número malware detectado / mes	BM	3	3	9	Plan para la adquisición de licencias antivirus y antimalware de estaciones de trabajo y servidor institucional	Plan Anual de mantenimiento de los equipos informáticos y plan de Respaldo de Información en la Nube	Encargado de soporte. Encargado de sistemas.	CIO.
					A.11.2.4	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 17.1.1	***P***	***P.Ade***	***DocF***	***RegNC***									
	Encriptación de PC por malware	M	Objetivos de seguridad de la información.	Asegurar el menor tiempo posible en restablecer las operaciones del servicio.	A.12.2.1	***P***	***P.Ade***	***DocF***	***RegNC***	Número de incidencias (hardware y software) / mes.	TM	3	3	9	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Plan para la adquisición e instalación de antivirus y antimalware. Así como la adquisición de Actualizaciones del Sistema Operativo (Parches). Además realizar y ejecutar planes para mantenimientos preventivos.	Encargado de soporte.	Director de seguridad de la información.
					A. 11.2.1	***P***	***P.Ade***	***DocF***	***RegNC***									

PCS PORTÁTILES	Pérdida o robo de Información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe custodiar la información de las computadoras y cumplir con los requerimientos legales.	A.9.2.3	***P***	***P.Ade***	***DocF***	***RegNC***	Número malware detectado / mes	BM	3	3	9	Plan para la adquisición de licencias antivirus y antimalware de estaciones de trabajo y servidor institucional	Plan Anual de mantenimiento de los equipos informáticos y plan de Respaldo de Información en la Nube.	Encargado de soporte. Encargado de sistemas.	CIO.
					A.11.2.4	***P***	***P.Ade***	***DocF***	***RegNC***									
					A. 17.1.1	***P***	***P.Ade***	***DocF***	***RegNC***									
	Encriptación de PC por malware	M	Objetivos de seguridad de la información.	Asegurar el menor tiempo posible en restablecer las operaciones del servicio.	A.12.2.1	***P***	***P.Ade***	***DocF***	***RegNC***	Número de incidencias (hardware y software) / mes.	TM	3	3	9	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Plan para la adquisición e instalación de antivirus y antimalware. Así como la adquisición de Actualizaciones del Sistema Operativo (Parches). Además realizar y ejecutar planes para mantenimientos preventivos.	Encargado de soporte.	Director de seguridad de la información.
					A. 11.2.1	***P***	***P.Ade***	***DocF***	***RegNC***									
Proyectores	Pérdida o robo de Información	M	Objetivos de seguridad de la información / Requerimiento legal.	La institución debe custodiar la información de las computadoras y cumplir con los requerimientos legales.	A. 17.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Cantidad de averías / Trimestral	A	3	2	6	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Plan Anual de mantenimiento de los equipos informáticos y bitácora de registro de incidencias.	Encargado de soporte. Encargado de sistemas.	CIO.

✓ **Plan de Tratamiento de Riesgos – Datos / Redes de comunicaciones**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
Redes de comunicaciones																		
ROUTER	Caída / indisponibilidad de servicios informáticos	M	Objetivos de negocio / Objetivos de seguridad de la información	La institución debe contar con el servicio constante de redes y conectividad	A 17.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Número de caídas de servicio / mes	TM	3	3	9	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Ejecución de mantenimientos programados. Validación de equipo para renovación	Encargado de soporte	CIO.
					A 17.1.2	***P***	***P.Ade***	***DocF***	***RegNC***									
	Manipulación configuración / Pérdida de servicio	M		La institución debe velar por la seguridad de la infraestructura de redes	A. 11.2.2	***P***	***P.Ade***	***DocF***	***RegNC***	Número de ataques detectados / mes	TM	4	3	12	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Programar y ejecutar respaldos de configuración de equipo	Encargado de soporte	CIO.
					A. 11.2.4	***P***	***P.Ade***	***DocF***	***RegNC***									

SWITCH	Caída / indisponibilidad de servicio	M	Objetivos de negocio / Objetivos de seguridad de la información	La institución debe contar con el servicio constante de redes y conectividad	A. 11.2.2	***P***	***P.Ade***	***DocF***	***RegNC***	Número de caídas de servicio / mes	TM	3	3	9	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Ejecución de mantenimientos programados. Validación de equipo para renovación	Encargado de soporte	CIO.
					A. 11.2.4	***P***	***P.Ade***	***DocF***	***RegNC***									
CABLEADO DE RED	Pérdida de servicio	M			A. 11.2.3	***D***	***P.Esp***	***DocN***	***RegNC***	Número de caídas de servicio / mes	TM	3	3	9	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Reestructuración de cableado en base a las normas de cableado estructurado.	Encargado de soporte	CIO.
HUB	Caída / indisponibilidad de servicio	M			A. 11.2.4	***P***	***P.Esp***	***DocF***	***RegNC***	Número de caídas de servicio / mes	TM	2	3	6	Plan de mantenimientos para el parque informático y plan de renovación de Equipos.	Ejecución de mantenimientos programados. Validación de equipo para renovación	Encargado de soporte	CIO.

✓ **Plan de Tratamiento de Riesgos – Datos / Soportes de información.**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
Soportes de información.																		
DISCOS DUROS EXTERNOS	Pérdida de información	M	Objetivos de seguridad de la información	La institución debe custodiar la información.	A 17.1.1	***C***	***P.Ade***	***DocF***	***RegC***	Número de incidencias / mes	TM	3	3	9	Revisión y clasificación de soportes de información	Adquisición de discos duros externos de respaldo. Revisión de discos duros externos	Encargado de soporte	CIO.
					A 17.1.2	***C***	***P.Ade***	***DocF***	***RegC***									
DVDS	Pérdida de información	M			A 17.1.1	***C***	***P.Ade***	***DocF***	***RegC***	Número de incidencias / mes	TM	3	2	6	Revisión y clasificación de soportes de información	Revisión de DVDs	Encargado de soporte	CIO.
					A 17.1.2	***C***	***P.Ade***	***DocF***	***RegC***									

✓ **Plan de Tratamiento de Riesgos – Datos / Equipamiento auxiliar**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
Equipamiento auxiliar																		
IMPRESORAS.	Inoperatividad	M	Objetivos de seguridad de la información.	Restablecer y asegurar en el menor tiempo posible continuidad del servicio	A.9.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Cantidad de impresoras no operativas / Trimestral	SM	4	2	8	Plan de mantenimiento preventivo y correctivo de los equipos informáticos.	Elaborar plan para mantenimientos preventivos.	Encargado de soporte.	Director de seguridad de la información.
					A.11.1.3	***P***	***P.Ade***	***DocF***	***RegC***									
					A. 11.2.4	***P***	***P.Ade***	***DocF***	***RegC***									
	Fuga de Información	M		Elaborar políticas que aborde las restricciones de acceso al servicio, con el propósito de controlar el uso de las impresiones.	A.16.1.2	***P***	***P.Ade***	***DocF***	***RegC***	Cantidad de Impresiones Sin Autorización/ Mes	TM	3	3	9	Implementar Controles de Impresiones	Implementar Software para Control de Impresión y Contador de Impresión (CZ Print Job Tracker 11).	Encargado de soporte.	Director de seguridad de la información.
CÁMARAS DE SEGURIDAD.	Intromisión en Tiempo Real	M	Objetivos de seguridad de la información.	Cerciorar que solo acceda el personal autorizado	A. 11.2.4	***P***	***P.Ade***	***DocF***	***RegC***	Número de accesos no autorizados detectados / Mes	TM	5	3	15	Elaborar e implementar controles de seguridad para el parque	Implementar controles de seguridad para incrementar la seguridad de los activos de información críticos.	Encargado de soporte. Especialista en seguridad informática	CIO / Director de seguridad de la información.
					A.13.1.1	***P***	***P.Ade***	***DocF***	***RegC***									
					A. 17.1.1	***P***	***P.Ade***	***DocF***	***RegC***									

✓ **Plan de Tratamiento de Riesgos – Datos / Instalaciones**

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
Instalaciones																		
Local del ODEI Lambayeque	Sustracción de documentación / bienes	M	Objetivos de seguridad de la información / Requerimiento legal	La integridad del patrimonio de la institución	A. 11.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Número de casos detectados / mes.	TM	4	2	8	Diseño e Implementación de controles de Acceso y de áreas seguras.	Implementar controles de seguridad.	Encargado de soporte. Especialista en seguridad informática	CIO / Director de seguridad de la información.
	Pérdida / daño de bienes	M	Objetivos de negocio		A. 11.1.1	***P***	***P.Ade***	***DocF***	***RegNC***	Número de casos detectados / mes.	TM	4	2	8	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética **trimestral**).	Especialista en seguridad informática	Director de seguridad de la información.

✓ Plan de Tratamiento de Riesgos – Datos / Personal

INESGSI10 - PLAN DE TRATAMIENTO DEL RIESGO

ACTIVO	RIESGO	Estrategia	Justificación	Detalle de Justificación	Controles NTP ISO/IEC 27001:2014	Tipo de Control	Frecuencia	Control de Documentación	Registros	Métricas / Indicadores	Mejora Continua	Impacto	Probabilidad	Riesgo Residual	Proyecto	Plan de Acción	Recursos	Responsable
Personal																		
Director de Sistema Administ. IV (Director Departamental)	Divulgación de la Información sensible	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con los	A. 5.1.1 A.7.1.1 A.7.1.2 A.7.2.1 A.7.2.2 A.7.2.3 A.7.3.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	4	3	12	Normatividad de la seguridad de la información Elaborar e implementar controles de seguridad para el parque informático.	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información. Implementar controles de seguridad para incrementar la seguridad de los activos de información críticos.	Encargado de soporte. Especialista en seguridad informática Encargado de soporte. Especialista en seguridad informática	CIO / Director de seguridad de la información.
Asistente Administrativo II	Divulgación de la Información sensible	M	Objetivos de seguridad de la información	La Institución debe salvaguardar y realizar una adecuada administración la	A. 5.1.1 A.7.2.2 A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Mes	TM	3	3	9	Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética **anual**).	Especialista en seguridad de información.	CIO / Director de seguridad de la información.
Director de Sistema Administ. II (Jefe Dirección Ejecutiva de Difusión Estadística)	Divulgación de la Información sensible	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con los requerimientos legales.	A. 5.1.1 A.7.1.1 A.7.1.2 A.7.2.1 A.7.2.2 A.7.2.3 A.7.3.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	4	3	12	Normatividad de la seguridad de la información Elaborar e implementar controles de seguridad para el parque informático.	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información. Implementar controles de seguridad para incrementar la seguridad de los activos de información críticos.	Encargado de soporte. Especialista en seguridad informática Encargado de soporte. Especialista en seguridad informática	CIO / Director de seguridad de la información.
Asistente	Divulgaci	M	Objetivos de	La Institución	A.7.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Inci	SM	3	3	9	Normatividad de la seguridad de la infor		Encargado de sistemas. Enca	CIO / Dire

					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***							Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.		
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***										
					A.11.2.8	***P***	***P.Ade***	***DocF***	***RegC***						Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética) y ***elaborar políticas de equipos desatendidos y escritorios limpios.***	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de	Director de seguridad de la
					A.11.2.9	***P***	***P.Ade***	***DocF***	***RegC***						Elaborar e implementar controles de seguridad para el parque informático.		Encargado de soporte. Especialista en seguridad de información.	CIO / Director de seguridad de
	Escaso personal para		Objetivo del Negocio	La institución debe custodiar la información.	A.7.2.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	3	3	9	Aplicar encuestas de niveles de satisfacción para los trabajadores.	Elaborar encuestas y ejecutarlas al personal de la institución para medir los niveles de satisfacción y poder gestionar el sobretiempo o horas extras elaborando planes para su compensación.	Oficial de seguridad de la información.	Director de seguridad de la información.
Técnico en Estadística II	Divulgación / Daño de Información sensible	M	Objetivos de seguridad de la información	La institución debe custodiar la información	A.7.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Trimestral	SM	2	3	6	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de	CIO / Director de seguridad de la información.
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***										
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***										
					A.11.2.8	***P***	***P.Ade***	***DocF***	***RegC***						Plan de Cultura de Seguridad de la Información	Bloqueo de las pc y laptop cuando los usuarios no se encuentren utilizándolas, no resguardar la información esencial en el área de escritorio o dejarlo en pantalla. Y capacitar a los colaboradores Normatividad de la seguridad de la información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de	Director de seguridad de la información.
					A.11.2.9	***P***	***P.Ade***	***DocF***	***RegC***						Plan de mantenimientos para el parque informático y plan de renovación de Equipos.		Encargado de soporte. Especialista en seguridad de información.	CIO / Director de seguridad de la información.
	Escaso personal para las operaciones	M	Objetivo del Negocio		A.7.2.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	2	3	6	Aplicar encuestas de niveles de satisfacción para los trabajadores.	Elaborar encuestas y ejecutarlas al personal de la institución para medir los niveles de satisfacción y poder gestionar el sobretiempo o horas extras elaborando planes para su compensación.	Oficial de seguridad de la información.	Director de seguridad de la información.

Secretaria IV	Divulgación de la Información sensible.	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con los requerimientos	A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	3	3	9	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de información.	Director de seguridad de la información.
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***									
Director de Sistema Administ. II (Dirección Ejecutiva de	Divulgación de la Información sensible	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con los	A. 5.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	4	3	12	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Encargado de soporte. Especialista en seguridad informática	CIO / Director de seguridad de la información.
					A.7.1.1	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.1.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.1	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.3.1	***P***	***P.Ade***	***DocF***	***RegC***						Elaborar e implementar controles de seguridad para el parque informático.	Implementar controles de seguridad para incrementar la seguridad de los activos de información críticos.	Encargado de soporte. Especialista en seguridad informática	
Asistente Serv. Econ. Finan. II	Divulgación / Daño de Información sensible	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con los requerimientos legales.	A.7.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Trimestral	SM	3	3	9	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de	CIO / Director de seguridad de la información.
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***									
					A.11.2.8	***P***	***P.Ade***	***DocF***	***RegC***						Plan de Cultura de Seguridad de la Información	Bloqueo de las pc y laptop cuando los usuarios no se encuentren utilizándolas, no resguardar la información esencial en el área de escritorio o dejarlo en pantalla. Y capacitar a los colaboradores Normatividad de la seguridad de la información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de	Director de seguridad de la información.
					A.11.2.9	***P***	***P.Ade***	***DocF***	***RegC***						Plan de mantenimientos para el parque informático y plan de renovación de Equipos.		Encargado de soporte. Especialista en seguridad de información.	CIO / Director de seguridad de la información.

	Escaso personal para las operaciones		Objetivos de seguridad de la información	La institución debe custodiar la información.	A.7.2.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	3	3	9	Aplicar encuestas de niveles de satisfacción para los trabajadores.	Elaborar encuestas y ejecutarlas al personal de la institución para medir los niveles de satisfacción y poder gestionar el sobretiempo o horas extras elaborando planes para su compensación.	Oficial de seguridad de la información.	Director de seguridad de la información.
Asistente Administrativo I	Divulgación / Daño de Información sensible	M	Objetivos de seguridad de la información	La institución debe custodiar la información	A.7.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Trimestral	SM	3	3	9	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de	CIO / Director de seguridad de la información.
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***									
					A.11.2.8	***P***	***P.Ade***	***DocF***	***RegC***						Plan de Cultura de Seguridad de la Información	Bloqueo de las pc y laptop cuando los usuarios no se encuentren utilizándolas, no resguardar la información esencial en el área de escritorio o dejarlo en pantalla. Y capacitar a los colaboradores Normatividad de la seguridad de la información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de	Director de seguridad de la información.
					A.11.2.9	***P***	***P.Ade***	***DocF***	***RegC***						Plan de mantenimientos para el parque informático y plan de renovación de Equipos.		Encargado de soporte. Especialista en seguridad de información.	CIO / Director de seguridad de la información.
	Escaso personal para las operaciones	M			A.7.2.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	3	3	9	Aplicar encuestas de niveles de satisfacción para los trabajadores.	Elaborar encuestas y ejecutarlas al personal de la institución para medir los niveles de satisfacción y poder gestionar el sobretiempo o horas extras elaborando planes para su compensación.	Oficial de seguridad de la información.	Director de seguridad de la información.
Operador PAD III	Divulgación de la Información	M	Objetivos de seguridad de la información /	La Institución debe salvaguardar y realizar una	A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	2	3	6	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de	Director de seguridad de la información.
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***									
Coordinador de	Divulgación	M	Objetivos de segurid	La Institución debe	A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias	A	4	3	12	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos,	Encargado de sistemas. Encargado de	Director de seguridad

					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***							estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.		
					A.7.3.1	***P***	***P.Ade***	***DocF***	***RegC***									
Encuestador	Divulgación / Daño de Información sensible	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con	A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Trimestral	SM	2	3	6	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de información.	Director de seguridad de la información.
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***									
Jefe del O.T. de Administración	Divulgación / Daño de Información sensible	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con los requerimientos legales.	A. 5.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Trimestral	SM	4	3	12	Normatividad de la seguridad de la información	Añadir clausulas en el proceso de revisión de antecedentes de los colaboradores para el procesos de selección de personal y establecer mecanismos para que no se permita la salida de información.	Encargado de sistemas. Encargado de soporte. Oficial de seguridad de información.	Administrador / Director de seguridad de la información.
					A.7.1.1	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.1.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.1	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***						Plan de Cultura de Seguridad de la Información	Elaborar e implementar programas de sensibilización a los colaboradores para el uso adecuado de la información y los activos que la soportan y procesan, haciéndolos parte de la cultura de la institución (Programar seminarios de ética, **cada 6 meses**).		
					A.7.3.1	***P***	***P.Ade***	***DocF***	***RegC***									
Secretaria	Divulgación de	M	Objetivos de seguridad	La Institución debe salvaguar	A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias	A	2	3	6	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para	Encargado de sistemas. Encargado de	Director de seguridad

					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***							ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.		
Jefe del O.T. de Informática	Divulgación / Daño de Información sensible	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con los requerimientos legales.	A. 5.1.1	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / Semestral	A	4	3	12	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Encargado de soporte. Especialista en seguridad informática	CIO / Director de seguridad de la información.
					A.7.1.1	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.1.2	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.1	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***						Elaborar e implementar controles de seguridad para el parque informático.	Implementar controles de seguridad para incrementar la seguridad de los activos de información críticos.	Encargado de soporte. Especialista en seguridad informática	
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***									
					A.7.3.1	***P***	***P.Ade***	***DocF***	***RegC***									
Encargado de Soporte	Divulgación de Información sensible	M	Objetivos de seguridad de la información / Requerimiento legal.	La Institución debe salvaguardar y realizar una adecuada administración la información y cumplir con los requerimientos legales.	A.7.2.2	***P***	***P.Ade***	***DocF***	***RegC***	Número de Incidencias detectadas / 6 meses	SM	3	3	9	Normatividad de la seguridad de la información	Aprobar, publicar e implementar las políticas, reglamentos, procedimientos, estándares y controles requeridos para ofrecer una adecuada gobernabilidad relacionada con la seguridad de información.	Especialista en seguridad informática Coordinador de capacitaciones. Equipos tecnológicos de seguridad.	Director de seguridad de la información.
					A.7.2.3	***P***	***P.Ade***	***DocF***	***RegC***									

9.12 ANEXO 12 – Plan de Gestión de Recursos

INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

ODEI LAMBAYEQUE

PLAN DE GESTIÓN DE RECURSOS Y COSTOS

INFORMACIÓN DEL DOCUMENTO	
Plan de Gestion de Riesgos	**Código:** INEISGSI09 **Versión:** 1.0
Nivel de confidencialidad: Uso Interno	**Fecha de la versión:** 15/12/2017
Creado por: Nilton Rogger Niño Morante.	**Estado:** PROPUESTO **Por:** Ing. Cancino Castañeda Daniel Ismael

- **TAREAS PROGRAMADAS**

Código	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Equipo 01**	**520 días**	**lun 1/01/18**	**vie 27/12/19**	
2	**Proyecto 02**	520 días	lun 1/01/18	vie 27/12/19	
3	Diseño e Implementación de controles de Acceso y de áreas seguras	3 mss	lun 1/01/18	vie 23/03/18	
4	***Análisis e identificación de mejoras a controles de acceso y áreas seguras***	411 días	vie 1/06/18	vie 27/12/19	
5	Ejecución 1	1 ms	vie 1/06/18	jue 28/06/18	3
6	Ejecución 2	1 ms	lun 3/09/18	vie 28/09/18	5
7	Ejecución 3	1 ms	lun 3/12/18	vie 28/12/18	6
8	Ejecución 4	1 ms	vie 1/03/19	jue 28/03/19	7
9	Ejecución 5	1 ms	lun 3/06/19	vie 28/06/19	8
10	Ejecución 6	1 ms	lun 2/09/19	vie 27/09/19	9
11	Ejecución 7	1 ms	lun 2/12/19	vie 27/12/19	10
12	**Proyecto 12**	434 días	lun 2/04/18	jue 28/11/19	
13	Revisión y clasificación de soportes de información	2 mss	lun 2/04/18	vie 25/05/18	3
14	***Revisión de clasificación de soportes de información***	215 días	vie 1/02/19	jue 28/11/19	
15	Ejecución 01	1 ms	vie 1/02/19	jue 28/02/19	13
16	Ejecución 02	1 ms	vie 1/11/19	jue 28/11/19	15
17	**Equipo 02**	**476 días**	**lun 1/01/18**	**lun 28/10/19**	
18	**Proyecto 03**	455 días	lun 1/01/18	vie 27/09/19	
19	Establecer políticas de contraseñas robustas para sistemas informáticos y correos institucionales	1 ms	lun 1/01/18	vie 26/01/18	
20	***Validación de políticas de contraseñas robustas***	412 días	jue 1/03/18	vie 27/09/19	
21	Ejecución 01	1 ms	jue 1/03/18	mié 28/03/18	19
22	Ejecución 02	1 ms	lun 3/09/18	vie 28/09/18	21
23	Ejecución 03	1 ms	mar 1/01/19	lun 28/01/19	22
24	Ejecución 04	1 ms	mié 1/05/19	mar 28/05/19	23
25	Ejecución 05	1 ms	lun 2/09/19	vie 27/09/19	24
26	**Proyecto 07**	453 días	jue 1/02/18	lun 28/10/19	
27	Plan de Cultura de Seguridad de la Información	3 mss	jue 1/02/18	mié 25/04/18	19
28	***Capacitación en seguridad de información a personal***	281 días	lun 1/10/18	lun 28/10/19	
29	Ejecución 01	1 ms	lun 1/10/18	vie 26/10/18	27
30	Ejecución 02	1 ms	lun 1/04/19	vie 26/04/19	29
31	Ejecución 03	1 ms	mar 1/10/19	lun 28/10/19	30
32	**Equipo 03**	**520 días**	**lun 1/01/18**	**vie 27/12/19**	
33	**Proyecto 10**	520 días	lun 1/01/18	vie 27/12/19	

34	Plan de mantenimientos para el parque informático y plan de renovación de equipos	2 mss	lun 1/01/18	vie 23/02/18	
35	***Seguimiento de plan de mantenimientos***	216 días	vie 1/03/19	vie 27/12/19	
36	Ejecución 01	1 ms	vie 1/03/19	jue 28/03/19	34
37	Ejecución 02	1 ms	lun 2/12/19	vie 27/12/19	36
38	**Proyecto 11**	456 días	jue 1/03/18	jue 28/11/19	
39	Plan para la adquisición de licencias antivirus y antimalware de puesto de trabajo y servidor institucional	1 ms	jue 1/03/18	mié 28/03/18	34
40	Adquisición de licencias antivirus y antimalware	1 ms	lun 2/04/18	vie 27/04/18	39
41	Despliegue de antivirus y antimalware para servidor	1 sem	mar 22/05/18	lun 28/05/18	40
42	Despliegue de antivirus y antimalware para estaciones de trabajo	3 mss	vie 1/06/18	jue 23/08/18	41
43	***Validación de antivirus y antimalware para nuevas estaciones de trabajo***	281 días	jue 1/11/18	jue 28/11/19	
44	Ejecución 01	1 ms	jue 1/11/18	mié 28/11/18	42
45	Ejecución 02	1 ms	jue 29/11/18	mié 26/12/18	44
46	Ejecución 03	1 ms	mié 1/05/19	mar 28/05/19	45
47	Ejecución 04	1 ms	jue 1/08/19	mié 28/08/19	46
48	Ejecución 05	1 ms	vie 1/11/19	jue 28/11/19	47
49	**Proyecto 08**	279 días	lun 2/04/18	jue 25/04/19	
50	Plan de mantenimiento preventivo y correctivo de los equipos informáticos	1 ms	lun 2/04/18	vie 27/04/18	19
51	Ejecución de plan de mantenimiento preventivo y correctivo de equipos informáticos	3 mss	vie 1/06/18	jue 23/08/18	50
52	***Seguimiento de plan de mantenimientos***	40 días	vie 1/03/19	jue 25/04/19	
53	Ejecución 01	1 ms	vie 1/03/19	jue 28/03/19	51
54	Ejecución 02	1 ms	vie 29/03/19	jue 25/04/19	53
55	Proyecto 04	304 días	mar 1/05/18	vie 28/06/19	
56	Implementar Controles de Impresiones	1 ms	mar 1/05/18	lun 28/05/18	50
57	Validación de controles de impresiones	1 ms	lun 3/06/19	vie 28/06/19	56
58	**Equipo 04**	**499 días**	**lun 1/01/18**	**jue 28/11/19**	
59	**Proyecto 05**	499 días	lun 1/01/18	jue 28/11/19	
60	Implementación de un Sistema Integrado de Gestión.	12 mss	lun 1/01/18	vie 30/11/18	
61	***Validación de funcionamiento correcto de sistema integrado de gestión***	195 días	vie 1/03/19	jue 28/11/19	
62	Ejecución 01	1 ms	vie 1/03/19	jue 28/03/19	60
63	Ejecución 02	1 ms	lun 1/07/19	vie 26/07/19	62
64	Ejecución 03	1 ms	vie 1/11/19	jue 28/11/19	63
65	**Equipo 05**	**499 días**	**lun 1/01/18**	**jue 28/11/19**	
66	**Proyecto 09**	499 días	lun 1/01/18	jue 28/11/19	
67	Elaborar e implementar controles de seguridad para el parque informático.	5 mss	lun 1/01/18	vie 18/05/18	
68	***Análisis e identificación de mejoras a controles de seguridad para el parque informático***	347 días	mié 1/08/18	jue 28/11/19	

69	Ejecución 01	1 ms	mié 1/08/18	mar 28/08/18	67
70	Ejecución 02	1 ms	jue 1/11/18	mié 28/11/18	69
71	Ejecución 03	1 ms	vie 1/02/19	jue 28/02/19	70
72	Ejecución 04	1 ms	mié 1/05/19	mar 28/05/19	71
73	Ejecución 05	1 ms	jue 1/08/19	mié 28/08/19	72
74	Ejecución 06	1 ms	vie 1/11/19	jue 28/11/19	73
75	**Equipo 06**	**455 días**	**lun 1/01/18**	**vie 27/09/19**	
76	**Proyecto 06**	433 días	lun 1/01/18	mié 28/08/19	
77	Normatividad de la seguridad de la información	2 mss	lun 1/01/18	vie 23/02/18	
78	***Validación y seguimiento de documentos normativos de seguridad de información***	281 días	mié 1/08/18	mié 28/08/19	
79	Ejecución 01	1 ms	mié 1/08/18	mar 28/08/18	77
80	Ejecución 02	1 ms	vie 1/02/19	jue 28/02/19	79
81	Ejecución 03	1 ms	jue 1/08/19	mié 28/08/19	80
82	**Proyecto 01**	412 días	jue 1/03/18	vie 27/09/19	
83	Aplicar encuestas de niveles	1 ms	jue 1/03/18	mié 28/03/18	77
84	***Aplicar encuestas de niveles***	280 días	lun 3/09/18	vie 27/09/19	
85	Ejecución 01	1 ms	lun 3/09/18	vie 28/09/18	83
86	Ejecución 02	1 ms	vie 1/03/19	jue 28/03/19	85
87	Ejecución 03	1 ms	lun 2/09/19	vie 27/09/19	86

- **RECURSOS Y COSTOS**

Nº	Nombre del Recurso	Costo	Etiqueta	Costo Total
1	Arquitectura de sistemas actuales.	S/.25.00	1 Hora(s)	S/.25.00
2	Binarios de antivirus y antimalware.	S/.12.50	2 Hora(s)	S/.25.00
3	Calendarización de mantenimientos.	S/.12.50	3 Hora(s)	S/.37.50
4	Discos duros externos.	S/.100.00	3 Unidad	S/.300.00
5	Documentación de arquitectura de sistemas informáticos y arquitectura de correo electrónico	S/.125.00	1 Hora(s) - TI interno	S/.125.00
6	Documentación de arquitectura informática.	S/.62.00	1 Hora(s) - TI interno	S/.62.00
7	Documentación de clasificación de soportes de información	S/.60.00	2 Hora(s) - especialista	S/.120.00
8	Documentación de controles.	S/.60.00	2 Hora(s) - especialista	S/.120.00
9	Documentación de despliegue de antivirus y antimalware.	S/.5.35	7 Hora(s) - TI interno	S/.37.45
10	Documentación de encuestas.	S/.9.00	4 Hora(s) - TI interno	S/.36.00
11	Documentación de equipos.	S/.10.50	6 Hora(s) - TI interno	S/.63.00
12	Documentación de infraestructura del local.	S/.37.50	1 Hora(s) - TI interno	S/.37.50
13	Documentación de plan de mantenimientos.	S/.37.50	1 Hora(s) - TI interno	S/.37.50

14	Documentación de políticas de contraseñas robustas.	S/.40.00	5 Hora(s) - especialista	S/.200.00
15	Documentación interna (MOF, ROF, Contratos de trabajo).	S/.6.25	2 Hora(s) - TI interno	S/.12.50
16	Documentación técnica de soluciones.	S/.120.00	2 Hora(s) - TI interno	S/.240.00
17	Documentación de Gestión.	S/.6.25	2 Hora(s) - TI interno	S/.12.50
18	DVDs.	S/.2.00	25 Unidad	S/.50.00
19	Equipos biométricos.	S/.1,000.00	2 Unidad	S/.2,000.00
20	Inventario de impresoras.	S/.31.25	2 Hora(s) - TI interno	S/.62.50
21	Licencias de antivirus y antimalware.	S/.20,000.00	3 Por paquete	S/.60,000.00
22	PC / Laptop	S/.0.00	51 Unidad	S/.0.00
23	Pizarra.	S/.0.00	3 Unidad	S/.0.00
24	Plumones.	S/.10.00	6 Unidad	S/.60.00
25	Proyector.	S/.0.00	3 Interno	S/.0.00
26	Sala de capacitación.	S/.0.00	3 Interno	S/.0.00
27	Servidor de Impresiones.	S/.3,500.00	1 Unidad	S/.3,500.00
28	Coordinador de capacitaciones.	S/.10.00/hora	200 horas	S/.2,000.00
29	Empresa de desarrollo SGI.	S/.25,000.00/ms	960 horas	S/.150,000.00
30	Encargado de sistemas.	S/.0.00/hora	1,000 horas	S/.0.00
31	Encargado de soporte.	S/.0.00/hora	3,426 horas	S/.0.00
32	Especialista en seguridad de información.	S/.1,500.00/ms	880 horas	S/.8,250.00
33	Especialista en seguridad informática.	S/.1,500.00/ms	560 horas	S/.5,250.00
34	Oficial de seguridad de la información.	S/.0.00/hora	2,600 horas	S/.0.00
35	Procesamiento de encuestas.	S/.10.50/hora	480 horas	S/.5,040.00
36	Propuestas de proveedores.	S/.40.00/ms	120 horas	S/.30.00

- **ASIGNACIÓN DE RECURSOS**

Código	Nombre de tarea	Nombres de los recursos
1	**Equipo 01**	
2	**Proyecto 02**	
3	Diseño e Implementación de controles de Acceso y de áreas seguras	Encargado de soporte.[50%];Especialista en seguridad informática.[50%];Documentación de infraestructura del local.[1 Informe];PC / Laptop[2 Unidad];Equipos biométricos.[2 Unidad]
4	***Análisis e identificación de mejoras a controles de acceso y áreas seguras***	
5	Ejecución 1	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
6	Ejecución 2	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
7	Ejecución 3	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
8	Ejecución 4	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]

9	Ejecución 5	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
10	Ejecución 6	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
11	Ejecución 7	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
12	**Proyecto 12**	
13	Revisión y clasificación de soportes de información	Discos duros externos.[1 Unidad];DVDs.[50 Unidad];Encargado de soporte.[25%];PC / Laptop[1 Unidad]
14	***Revisión de clasificación de soportes de información***	
15	Ejecución 01	Encargado de soporte.[50%];Documentación de clasificación de soportes de información[1 Informe];PC / Laptop[1 Unidad]
16	Ejecución 02	Documentación de clasificación de soportes de información[1 Informe];Encargado de soporte.[50%];PC / Laptop[1 Unidad]
17	**Equipo 02**	
18	**Proyecto 03**	
19	Establecer políticas de contraseñas robustas para sistemas informáticos y correos institucionales	Especialista en seguridad de información.[50%];Documentación de arquitectura de sistemas informáticos y arquitectura de correo electrónico[1 Informe];PC / Laptop[1 Unidad]
20	***Validación de políticas de contraseñas robustas***	
21	Ejecución 01	Especialista en seguridad de información.[50%];Documentación de políticas de contraseñas robustas.[1 Informe];PC / Laptop[1 Unidad]
22	Ejecución 02	Documentación de políticas de contraseñas robustas.[1 Informe];Especialista en seguridad de información.[50%];PC / Laptop[1 Unidad]
23	Ejecución 03	Documentación de políticas de contraseñas robustas.[1 Informe];Especialista en seguridad de información.[50%];PC / Laptop[1 Unidad]
24	Ejecución 04	Documentación de políticas de contraseñas robustas.[1 Informe];Especialista en seguridad de información.[50%];PC / Laptop[1 Unidad]
25	Ejecución 05	Documentación de políticas de contraseñas robustas.[1 Informe];Especialista en seguridad de información.[50%];PC / Laptop[1 Unidad]
26	**Proyecto 07**	
27	Plan de Cultura de Seguridad de la Información	Especialista en seguridad informática.[25%];Coordinador de capacitaciones.[25%];Encargado de soporte.[25%];Documentación interna (MOF, ROF, Contratos de trabajo).[1 Informe];PC / Laptop[2 Unidad]
28	***Capacitación en seguridad de información a personal***	
29	Ejecución 01	Encargado de soporte.[20%];Sala de capacitación.[1 Unidad];Proyector.[1 Unidad];Pizarra.[1 Unidad];Plumones.[2 Unidad];PC / Laptop[1 Unidad]
30	Ejecución 02	Sala de capacitación.[1 Unidad];Encargado de soporte.[20%];Proyector.[1 Unidad];Pizarra.[1 Unidad];Plumones.[2 Unidad];PC / Laptop[1 Unidad]
31	Ejecución 03	Pizarra.[1 Unidad];Plumones.[2 Unidad];Proyector.[1 Unidad];Encargado de soporte.[20%];Sala de capacitación.[1 Unidad];PC / Laptop[1 Unidad]

32	**Equipo 03**	
33	**Proyecto 10**	
34	Plan de mantenimientos para el parque informático y plan de renovación de equipos	Coordinador de capacitaciones.[25%];Encargado de soporte.[25%];Propuestas de proveedores.[25%];Calendarización de mantenimientos.[1 Archivo];Documentación técnica de soluciones.[1 Informe];Documentación de Gestión.[1 Informe];Documentación de plan de ma...
35	***Seguimiento de plan de mantenimientos***	
36	Ejecución 01	Encargado de soporte.[25%];Documentación de equipos.[1 Informe];PC / Laptop[1 Unidad]
37	Ejecución 02	Encargado de soporte.[50%];Documentación de equipos.[1 Informe];PC / Laptop[1 Unidad]
38	**Proyecto 11**	
39	Plan para la adquisición de licencias antivirus y antimalware de puesto de trabajo y servidor institucional	Encargado de soporte.[25%];Encargado de sistemas.[25%];Propuestas de proveedores.[25%];Documentación técnica de soluciones.[1 Informe];PC / Laptop[1 Unidad]
40	Adquisición de licencias antivirus y antimalware	Encargado de soporte.[25%];Licenciamiento de antivirus y antimalware; PC / Laptop[1 Unidad]
41	Despliegue de antivirus y antimalware para servidor	Encargado de soporte.[25%];Binarios de antivirus y antimalware.[1 Archivo];Licenciamiento de antivirus y antimalware; Documentación de despliegue de antivirus y antimalware.[1 Informe];Discos duros externos.[1 Unidad]
42	Despliegue de antivirus y antimalware para estaciones de trabajo	Encargado de soporte.[25%];Binarios de antivirus y antimalware.[1 Archivo];Licenciamiento de antivirus y antimalware; Documentación de despliegue de antivirus y antimalware.[1 Informe];Discos duros externos.[1 Unidad]
43	***Validación de antivirus y antimalware para nuevas estaciones de trabajo***	
44	Ejecución 01	Encargado de soporte.[50%];Documentación de despliegue de antivirus y antimalware.[1 Informe]
45	Ejecución 02	Documentación de despliegue de antivirus y antimalware.[1 Informe];Encargado de soporte.[25%]
46	Ejecución 03	Encargado de soporte.[25%];Documentación de despliegue de antivirus y antimalware.[1 Informe]
47	Ejecución 04	Documentación de despliegue de antivirus y antimalware.[1 Informe];Encargado de soporte.[25%]
48	Ejecución 05	Documentación de despliegue de antivirus y antimalware.[1 Informe];Encargado de soporte.[25%]
49	**Proyecto 08**	
50	Plan de mantenimiento preventivo y correctivo de los equipos informáticos	Encargado de soporte.[50%];Calendarización de mantenimientos.[1 Archivo];Documentación de equipos.[1 Informe];PC / Laptop[1 Unidad]
51	Ejecución de plan de mantenimiento preventivo y correctivo de equipos informáticos	Encargado de soporte.[50%];Calendarización de mantenimientos.[1 Archivo];Documentación de equipos.[1 Informe]
52	***Seguimiento de plan de mantenimientos***	
53	Ejecución 01	Encargado de soporte.[25%];Documentación de equipos.[1 Informe]
54	Ejecución 02	Documentación de equipos.[1 Informe];Encargado de soporte.[25%]

55	**Proyecto 04**	
56	Implementar Controles de Impresiones	Encargado de soporte.[25%];Inventario de impresoras.[1 Informe];Servidor de Impresiones.[1 Unidad];Documentación de controles.[1 Informe]
57	Validación de controles de impresiones	Encargado de soporte.[25%];Oficial de seguridad de la información.[25%];Inventario de impresoras.[1 Informe];Documentación de controles.[1 Informe];PC / Laptop[1 Unidad]
58	**Equipo 04**	
59	**Proyecto 05**	
60	Implementación de un Sistema Integrado de Gestión.	Encargado de sistemas.[50%];Oficial de seguridad de la información.[50%];Empresa de desarrollo SGI.[50%];PC / Laptop[2 Unidad]
61	***Validación de funcionamiento correcto de sistema integrado de gestión***	
62	Ejecución 01	Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
63	Ejecución 02	Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
64	Ejecución 03	Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
65	**Equipo 05**	
66	**Proyecto 09**	
67	Elaborar e implementar controles de seguridad para el parque informático.	Encargado de soporte.[50%];Especialista en seguridad informática.[25%];Documentación de arquitectura informática.[1 Informe];PC / Laptop[1 Unidad]
68	***Análisis e identificación de mejoras a controles de seguridad para el parque informático***	
69	Ejecución 01	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
70	Ejecución 02	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
71	Ejecución 03	Oficial de seguridad de la información.[50%];Encargado de soporte.[50%];PC / Laptop[1 Unidad]
72	Ejecución 04	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
73	Ejecución 05	Oficial de seguridad de la información.[50%];Encargado de soporte.[50%];PC / Laptop[1 Unidad]
74	Ejecución 06	Encargado de soporte.[50%];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
75	**Equipo 06**	
76	**Proyecto 06**	
77	Normatividad de la seguridad de la información	Especialista en seguridad de información.[50%];Encargado de soporte.[50%];Documentación de Gestión.[1 Informe];Documentación interna (MOF, ROF, Contratos de trabajo).[1 Informe];PC / Laptop[1 Unidad]
78	***Validación y seguimiento de documentos normativos de seguridad de información***	
79	Ejecución 01	Especialista en seguridad de información.[50%];PC / Laptop[1 Unidad]
80	Ejecución 02	Especialista en seguridad de información.[50%];PC / Laptop[1 Unidad]
81	Ejecución 03	Especialista en seguridad de información.[50%];PC / Laptop[1 Unidad]
82	**Proyecto 01**	

83	Aplicar encuestas de niveles	Oficial de seguridad de la información.[50%];Documentación de encuestas.[1 Informe];PC / Laptop[1 Unidad]
84	***Aplicar encuestas de niveles***	
85	Ejecución 01	Oficial de seguridad de la información.[50%];Documentación de encuestas.[1 Informe];Procesamiento de encuestas; PC / Laptop[1 Unidad]
86	Ejecución 02	Procesamiento de encuestas; Documentación de encuestas.[1 Informe];Oficial de seguridad de la información.[50%];PC / Laptop[1 Unidad]
87	Ejecución 03	Oficial de seguridad de la información.[50%];Documentación de encuestas.[1 Informe];Procesamiento de encuestas ;PC / Laptop[1 Unidad]

- **Tabla Resumen**

Además, una tabla donde se resumen por equipo la cantidad de trabajo, duración y costos que demandara la implementación del SGSI, A continuación:

	Modo de	Nombre de tarea	Duración	Comienzo	Fin	% completado	Costo	Trabajo
1		Equipo 01	520 días	lun 1/01/18	vie 27/12/19	0%	S/.4,557.50	1,840 horas
2		Proyecto 02	520 días	lun 1/01/18	vie 27/12/19	0%	S/.4,287.50	1,600 horas
12		Proyecto 12	434 días	lun 2/04/18	jue 28/11/19	0%	S/.270.00	240 horas
17		Equipo 02	476 días	lun 1/01/18	lun 28/10/19	0%	S/.7,216.25	936 horas
18		Proyecto 03	455 días	lun 1/01/18	vie 27/09/19	0%	S/.4,825.00	480 horas
26		Proyecto 07	453 días	jue 1/02/18	lun 28/10/19	0%	S/.2,391.25	456 horas
32		Equipo 03	520 días	lun 1/01/18	vie 27/12/19	0%	S/.65,184.20	1,410 horas
33		Proyecto 10	520 días	lun 1/01/18	vie 27/12/19	0%	S/.1,042.25	360 horas
38		Proyecto 11	456 días	jue 1/03/18	jue 28/11/19	0%	S/.60,392.45	530 horas
49		Proyecto 08	279 días	lun 2/04/18	jue 25/04/19	0%	S/.67.00	400 horas
55		Proyecto 04	304 días	mar 1/05/18	vie 28/06/19	0%	S/.3,682.50	120 horas
58		Equipo 04	499 días	lun 1/01/18	jue 28/11/19	0%	S/.150,000.00	3,120 horas
59		Proyecto 05	499 días	lun 1/01/18	jue 28/11/19	0%	S/.150,000.00	3,120 horas
65		Equipo 05	499 días	lun 1/01/18	jue 28/11/19	0%	S/.1,937.00	1,560 horas
66		Proyecto 09	499 días	lun 1/01/18	jue 28/11/19	0%	S/.1,937.00	1,560 horas
75		Equipo 06	455 días	lun 1/01/18	vie 27/09/19	0%	S/.8,838.50	1,360 horas
76		Proyecto 06	433 días	lun 1/01/18	mié 28/08/19	0%	S/.3,762.50	560 horas
82		Proyecto 01	412 días	jue 1/03/18	vie 27/09/19	0%	S/.5,076.00	800 horas

Imagen 22: Resumen Implementación de SGSI