UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSTGRADO

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LA MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN FINANCIERA DE LAS UNIDADES DE GESTIÓN EDUCATIVA LOCAL DE LAMBAYEQUE

TESIS PARA OPTAR EL GRADO ACADÉMICO DE

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR

LUIS RAUL TABOADA CORNETERO

ASESOR

MONICA YOLANDA VILLAVICENCIO MONTOYA DE PALOMINO

https://orcid.org/0000-0002-9568-7786

Chiclayo, 2021

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LA MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN FINANCIERA DE LAS UNIDADES DE GESTIÓN EDUCATIVA LOCAL DE LAMBAYEQUE

PRESENTADA POR:

LUIS RAUL TABOADA CORNETERO

A la Escuela de Posgrado de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el grado académico de

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADA POR:

Gregorio Manuel León Tenorio
PRESIDENTE

Ricardo David Iman Espinoza
SECRETARIO

Monica Yolanda Villavicencio Montoya de Palomino
VOCAL

DEDICATORIA

A mis padres Luis e Isabel, a mi hermana Cecilia quienes siempre creyeron en mí y me han apoyado en todo momento para poder desarrollar este nuevo reto en mi vida profesional, ya que han estado presentes para darme fuerza moral y psicológica para cumplir con mi objetivo.

EPÍGRAFE

"Nunca consideres el estudio como un deber, sino como una oportunidad para penetrar en el maravilloso mundo del saber."

Albert Einstein.

AGRADECIMIENTOS

A Dios, por guiar mi vida, permitido seguir por el camino correcto y ayudarme a salir de momentos difíciles. A mis padres por su apoyo incondicional, consejos y ánimos de continuar con el logro de mis objetivos. A mi asesora Mónica Villavicencia Montoya por todos sus conocimientos y dedicación que me ha servido para desarrollar esta investigación.

ÍNDICE

ÍNDICE DE FIGURAS

LISTA DE TABLAS

RESUMEN

La investigación se centra en contribuir en la protección de información financiera de las Unidades de Gestión Educativa Local en la región Lambayeque, por no contar con un modelo de seguridad de la información para sus activos de información financiera, analizando cómo se encuentran actualmente estas unidades, se pudo comprobar que requieren establecer controles que ayuden a proteger dicha información, así minimizar las consecuencias de las amenazas a las que están expuestas.

El objetivo general planteado fue contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de la región Lambayeque, de tal manera que se propuso un modelo de seguridad de la información, analizando marcos de trabajo y estándares internacionales relacionados con este estudio, para adaptarlos al contexto de la unidad de gestión educativa local.

El modelo fue validado por tres expertos, logrando medir la confiabilidad mediante el uso de alfa de Cronbach, así también su concordancia con Kendall, esto permitió demostrar que es válido y se puede aplicar como herramienta en la gestión de seguridad de la información para contribuir en la mejora de activos de información financiera en el sector de Unidades de Gestión Educativa Local.

Palabras clave: gestión de seguridad de información, gestión de riesgo, Unidades de Gestión Educativa Local de Lambayeque, control de seguridad.

ABSTRACT

The research focuses on contributing to the protection of financial information of the Local Educational Management Units in the Lambayeque region, by having an information security model for their financial information assets, analyzing how these units are currently located, was able to verify that they require establishing controls that help protect said information, thus minimizing the consequences of the threats to which they are exposed.

The general objective set was to contribute to improving the security of the financial information assets of the Local Educational Management Units of the Lambayeque region, in such a way that an information security model was proposed, analyzing frameworks and standards related to this study, to adapt them to the context of the local educational management unit.

The model was validated by three experts, managing to measure reliability through the use of Cronbach's alpha, as well as its agreement with Kendall, this allowed demonstrating that it is valid and can be applied as a tool for information security management to contribute to improving financial information assets in the Local Educational Management Units sector.

Keywords: information security management, risk management, Lambayeque Local Educational Management Units, security control.

INTRODUCCIÓN

En toda institución, un importante activo es la información, puede quedar registrada de manera digital en servidores, impresa, enviada por medios electrónicos o redes sociales. En el ámbito de los negocios y privacidad de hoy, esa información sensible se encuentra sujeta a múltiples amenazas, las cuales se pueden ver reflejadas de manera interna, externa, no intencionada o intencionada; pueden provocar pérdidas financieras, divulgación de información sensible, desprestigio a la entidad u organización. Con el inminente crecimiento de la tecnología para alojar, enviar y editar de manera colaborativa todo tipo de información, también este activo de información se ve expuesto a un gran número y variedad de riesgos.

Muchas instituciones y organizaciones no cuentan con un Sistema de Seguridad de la Información, primordial para asegurar confidencialidad, integridad y disponibilidad de la información, siendo de suma importancia para los usuarios beneficiados de este activo [1].

De acuerdo con la encuesta de Percepción de Riesgos Globales (GPRS) 2018-2019 [2], los riesgos mundiales más relevantes son el fraude y robo masivo de datos. Ataques con sistemas maliciosos y protocolos de seguridad vulnerables han dado lugar a robo masivo de información de datos personales durante el 2018. Un claro ejemplo tenemos en India, en un repositorio de datos de identificaciones de la nación, Aadhaar, manifiesta haber sido víctima de filtraciones que comprometieron de manera considerable un total de 1,100 millones de registro de ciudadanos. Así también durante el mes de marzo la organización del estado que ofrece servicios al público, se vio afectada al permitir que cualquier usuario pueda obtener datos completos y número de identificaciones de los ciudadanos.

Figura 1. Diez principales riesgos mundiales en probabilidad e impacto

Fuente: [2]

El Informe de Riesgos Mundiales 2019 en su 14a edición [2], manifiesta que la tecnología también desempeñó un papel fundamental en la conformación mundial de riesgos, siendo los ataques cibernéticos y fraudes de datos unos de los más importantes, otras vulnerabilidades tecnológicas se vieron reflejadas en noticias falsas, apropiación ilícita de identidades; así también el robo de privacidad en gobiernos. El informe refiere a que el 2018 se vieron expuestas nuevas debilidades en lo que corresponde al hardware, además manifiesta que al organizar ataques cibernéticos tienen como uso potencial la inteligencia artificial.

Existen empresas en el ámbito internacional que fueron víctimas de estos riesgos. Según el Portal Identity Theft Resource Center informó que en el 2014 en Estados Unidos fueron detectados 1´198,492 registros de información relacionados a incidentes de fuga de Información en el sector Bancario. En este contexto, la fuga de información corresponde uno de los riesgos más devastadores para un Banco, involucra pérdida de dinero y sobre todo reputación. Es por ello que los controles de Seguridad deben estar enfocados no solo en los sistemas, sino también en el recurso humano que son la pieza más frágil de la seguridad y en los Procesos. Por ejemplo “Card Systems Solutions Inc.”, una empresa de tarjetas de crédito; durante el año 2005 reporta que personas no autorizadas accedieron a transacciones de 40

millones de reportó que personas no autorizadas accedieron a las transacciones de 40 millones de usuarios, trayendo como consecuencia que las organizaciones Visa y Mastercard, cancelaran todo tipo de negociación con la empresa afectada [3].

En el ámbito nacional, [4] en el año 2019 en un estudio sobre Ciber Riesgos y Seguridad de la Información en América Latina y el Caribe; fueron encuestadas organizaciones de sector financiero, manufactura, tecnología, servicios, minería, sector público y otros; obteniendo como resultados que, empresas peruanas en un 32% tuvieron ciberataques en los últimos 24 meses. En el mismo periodo, un 33% de empresas peruanas manifestó que fue víctima de uno, un 22% de dos y un porcentaje similar de tres a más ciberataques respectivamente.

Figura 2. Incidentes de Seguridad en organizaciones

Fuente: [4]

Además, el 36% de las organizaciones consultadas por Deloitte considera que están medianamente protegidas en ciberseguridad y un 14% están poco protegidas. Esto tiene mayor importancia si vemos que en el criterio de Importancia de la Ciber Seguridad para las Organizaciones, en Perú un 71% de las corporaciones encuestadas consideran extremadamente importante la ciberseguridad y para un 25% muy importante y solo un 4% medianamente importante. Esto hace tomar conciencia que actualmente el 46% de empresas peruanas tienen roles y responsabilidades definidas, frente al 37% a nivel de

Latinoamérica; sin embargo, solo un 4% de empresas tienen tareas de detección, prevención y proactividad [4].

Figura 3. Importancia de la Seguridad para las Organizaciones

Fuente: [4]

Así mismo el informe mundial de Tecnología de la Información en el año 2013 ubica a Perú en la posición 103 de 144 países, encontrándose rezagado en el beneficio del uso de la tecnología para modernizar su economía. Aún con el impulso del Gobierno para aumentar los servicios en el acceso a Internet de banda ancha que lo ubicó en el puesto 107, no se han evidenciados suficientes avances en lo correspondiente a la infraestructura Tecnológica de Información y Comunicaciones ubicándola en el lugar 86, en lo concerniente a usuarios con acceso a internet Perú se ubica en el puesto 77, así mismo en hogares con equipos de cómputo están ubicados en el lugar 82 y las mismas con acceso a internet en el puesto 83 [5], podemos ver reflejada que la mayoría de empresas privadas y entidades públicas peruanas no aprovechan el beneficio de la tecnología de información, además existe poca inversión o interés para modernizar la plataforma tecnológica; puesto que la tecnología obsoleta genera más vulnerabilidades para la información de los activos financieros, tan importantes hoy en día y que requiere ser atendida de manera oportuna por la alta demanda.

En el ámbito local, en el año 2017, debido a un error involuntario realizado en la base de datos del el Sistema Único de Planillas, se abonó una cifra exorbitante a un docente de UGEL Chiclayo, el monto pagado ascendió a S/.

307,079.30, el mismo que había sido abonado a su cuenta de banco, por un error involuntario de carácter digital en la oficina antes mencionada según expediente del Sistema de Gestión Documentario 3.0 SISGEDO número 2634496-0. En el caso de las Unidades de Gestión Educativa Local, no tienen planes de continuidad que permitan responder ante las múltiples amenazas que podrían afectar a los bienes lógicos y físicos de las dependencias, donde se puede destacar el evento del fenómeno del niño costero, ocurrido en el año 2017 o las huelgas de docentes organizadas por el Sindicato Único de trabajadores de la Educación del Perú SUTEP, huelga por parte de los servidores públicos del Sindicato de trabajadores de la Educación Lambayeque SITAEL, ocasionando pérdida de clases en la región como también descuentos, retrasos en la remuneración de los trabajadores.

De esta manera se puede evidenciar que los riesgos en la seguridad de información tales como datos erróneos, usuarios con accesos no autorizados, modificaciones no autorizadas a los sistemas, generan consecuencias significativas para las Unidades de Gestión Educativas, dañando la imagen institucional y conllevando a futuras huelgas de trabajadores y docentes, además denuncias o reclamos por parte de los proveedores, es por estos motivos que para las UGEL's, es de suma importancia proteger los activos de información financiera.

Es así como esta investigación realiza la formulación del problema, ¿Cómo contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque?, para lo cual propone que, un modelo de Seguridad de la Información permitirá mejorar la Seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque.

Teniendo como una propuesta general, contribuir en la mejora de la seguridad de los activos de información financiera desarrollando un modelo basado en marcos de trabajo y estándares internacionales de seguridad de la información para las Unidades de Gestión Educativa Local de Lambayeque.

Para el alcance de la propuesta general se planteó:
- Analizar comparativamente estándares y marcos de trabajo internacionales de seguridad de la información, con la finalidad de seleccionar los criterios que más se adecúen a las unidades del sector en estudio.
- Proponer un modelo basado en estándares y marcos de trabajo de seguridad de la información adaptado para contribuir en la mejora de la seguridad de los activos de información financiera en las Unidades de Gestión Educativa Local de Lambayeque.
- Validar el modelo de seguridad de la información propuesto mediante juicio de expertos.

La investigación se justifica desde un ámbito legal, debido a que la Resolución Ministerial N° 004-2016-PCM, dispone la implementación de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 en todas las entidades integrantes del Sistema Nacional de Informática, Sistema que está integrado por los Órganos de Informática de los Gobiernos Regionales. Los Gobiernos Regionales cuentan con 23 dependencias, aprobadas con la R.E.R. No. 240-2010-GR.LAMB/PR [6] bajo la directiva No. 006–2010-GR.LAMB. Una de estas dependencias están conformadas por las Unidades de Gestión Educativa Local de la región Lambayeque, motivo por el que la Unidad Ejecutora se encuentra inmersa en la implementación de la Resolución Ministerial N° 004.2016-PCM.

Viendo la perspectiva social, el trabajo de investigación mejora la seguridad de la información financiera, impactando beneficiosamente a docentes y personal administrativo en la comunidad Lambayecana, puesto que con el modelo propuesto, los docentes pueden ver de forma transparentada, correcta e íntegra la información de pagos de manera oportuna, reduciendo las quejas o reclamos que puedan realizar, reduciendo de esta manera la ausencia de docente en aulas de clase por realizar trámites en UGEL.

En lo económico, el modelo propuesto persevera la confidencialidad e integridad de los activos de información sensible, por ejemplo cálculo de presupuesto, reportes contables, se accedida solo por el personal autorizado en las respectivas áreas de UGEL, así como de los diversos egresos como pagos a proveedores, transportistas y locadores de servicios, evitando errores en las cifras numéricas que puedan atenuar pérdidas económicas a la institución, que puedan conllevar a futuras sanciones administrativas por parte de algún órgano de control o del Ministerio de Justicia.

Relacionado al aspecto tecnológico, el modelo proporciona a las unidades de gestión educativa mecanismos que soportan controles de seguridad, protegiendo sistemas de registro y conciliación financiera como SIAF, registro gestión administrativa en SIGA MEF, información de contratos de docentes en Instituciones Educativas almacenadas en Nexus, así como también información de legajos escalafonarios de trabajadores en el sistema Legix, que se alojan en bases de datos de los servidores instalados en la sede.

CAPÍTULO I MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes

Fundamentando esta investigación, analizo estudios realizados en el ámbito internacional, según [7] el problema identificado era otorgar información oportuna que mejore la calidad de la educación de una organización Colombiana, esta organización está especializada en ofrecer evaluaciones de educación en todas las modalidades de estudio al Ministerio de Educación Nacional, realizando exámenes para el Estado enfocado en temas que infieran la educación de calidad. Motivo por el cual desarrolló un proyecto con el propósito de "Diseñar un sistema de gestión de seguridad de la información utilizando la Norma ISO/IEC 27001:2013". El investigador rescata emplear la norma para aquellas instituciones que necesiten enfocar objetivos de seguridad que aseguren la continuidad de la institución. Identifica una lista de controles de la norma ISO/IEC 27002 para la entidad Colombiana cuyo porcentaje de cumplimiento es del 41,23%. Esta investigación apoya al presente estudio, en medida que se aplica a una unidad educativa y pudimos analizar los distintos controles de seguridad implementación a empresas que ofrecen un similar servicio.

Así mismo [8], identifica que el trabajo y estudio que realizan muchos fiscales en su sector de investigación, son almacenados en documentos físicos, un gran número de documentos son impresos, existiendo la necesidad de implementar un Sistema de Gestión de Seguridad de la Información, centralizado en el área de gestión de la Fiscalía General de Ecuador. Comparando el estándar ISO/IEC 27001, ISO/IEC 20000, AC SI33, ISO/IEC 13335, método OCTAVE y COSO. Se cree conveniente considerar el antecedente, porque explica de una manera clara las normas OCTAVE mencionada permitiendo observar su adaptabilidad a las necesidades según cada organización, proponiendo indicadores a utilizar de manera cotidiana en el área de gestión de información.

Según [9] fue posible determinar que existe necesidad en implantar controles de seguridad, que protejan la integridad de la información o asegurarse que no sea manipulada por usuarios no autorizados. Con la información recopilada, pudo aplicar estándares documentados y difundidos. Proponiendo como objetivo general en análisis de procesos críticos de "Credigestión", de esta manera asegurar la integridad, disponibilidad y confidencialidad de la información, proponiendo controles que se detallan en la Norma ISO/IEC 27001, concluyendo que los activos de información de áreas consideradas críticas, reflejan altos riesgos, quedando la información propensa a robo o modificaciones. Se considera importante esta investigación, puesto que resalta de manera eficiente la importancia proteger los activos de información de catástrofes, además de los controles que evitan el acceso no autorizado.

A nivel nacional, se revisó la investigación [10], donde el autor identifica las razones por las cuales se ve restringido el implantar un Sistema de gestión de seguridad de la información (SGSI) en las entidades públicas a nivel nacional, recoge información de forma estructurada y organizada, lo que le permite proponer soporte en mejora de la implementación de políticas de seguridad en entidades integrantes del Sistema Nacional de Informática, llegando a la conclusión que existe un equilibrio entre alineamiento de Tecnologías de la Información con estrategias de negocio, además de controlar los riesgos de seguridad, facilitando evaluar la dificultad de ejecutar los controles propuestos por la NTP-ISO/IEC 27001. Esta investigación aporta al estudio en la manera que está orientada a entender las causas de implementar SGSI en Entidades Públicas, permitiendo conocer las normas establecidas para este contexto ya que las UGEL en Lambayeque pertenecen al mismo entorno estatal,

El estudio [11] analiza la problemática, aspectos relevantes de los modelos de seguridad de información, luego del estudio realizado identifica ocho elementos (organización, niveles, métricas, fases, indicadores, documentos, funciones y controles), los cuales fueron empleados para la propuesta de un

modelo de SGSI en beneficio del Gobierno Electrónico. Esta propuesta orientada a procesos, lo estructura organizacionalmente en funciones, implementando y gestionando la seguridad de información, según fases y niveles de madurez propuestos; de tal manera que posteriormente se pueda monitorear la seguridad y revisarlas de manera continua a través de las métricas e indicadores establecidos. Este antecedente se rescata la comparación de los elementos identificados de diferentes modelos de seguridad de la Información para el presente estudio de investigación.

Además [12] propuso la investigación "Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) siguiendo las normas internacionales ISO/IEC 27001 para mejorar la seguridad de información en la empresa HM CONTRATISTAS S.A. ubicada en Huaraz", para el desarrollo utilizó la metodología de la ISO 27001 especificando el ciclo de Deming Mejora Continua, donde tiene 4 etapas la primera etapa, se identifica y valoriza los activos de información según su accesibilidad, seguidamente procedió con el análisis, identificación y evaluación de riesgos de los cuales están expuesto los activos de información, seguidamente se elabora la documentación requerida por la norma ISO/IEC 27001 y por último el modelo de procesos del negocio para delimitar el alcance del SGSI. Las demás etapas no se llegaron a considerar porque la tesis solo consiste en la etapa del diseño. Llegando a la conclusión que la empresa no tiene conformada una comisión en seguridad de información, el cual deba estructurar un plan estratégico priorizando los activos de información, de esta manera establecer políticas y controles que respondan a las amenazas. Se cree conveniente citar el estudio puesto que profundiza el ciclo Deming de Mejora Continua, que apoya el modelo propuesto.

En el ámbito local, según [13] propuso un modelo de gestión de riesgos al integrar técnicas cuantitativas y cualitativas que están relacionadas con las tecnologías de información tomando en cuenta la ISO/IEC 27001, ISO/IEC 27002, siendo el SBS una organización que supervisa entidades financieras.

Se implementa un modelo de gestión de riesgos, identificando y evaluando claramente los activos TI y sus categorías como: Disponibilidad, integridad y confidencialidad de la información, lo exigido por la SBS se pudo demostrar mediante una matriz de riesgos que es el producto visible de la metodología de gestión de riesgos. El antecedente es importante en medida que estudia los peligros de las empresas con activos de información financiera, activos que se propone proteger para las Unidades de Gestión Educativas Local.

En la investigación [14], identifica las deficiencias que presentan los sistemas informáticos de las comisarías, por lo que el autor propone la implementación de la norma ISO/IEC 27001, ya que esta identifica las deficiencias, anomalías y da plan de mejora al tratamiento de riesgos disminuyendo amenazas en activos de información. Proponiendo un plan de capacitación y concientizando a los usuarios se puede incrementar el índice del conocimiento en las estrategias de seguridad y obtener un personal más comprometido con la empresa. La importancia del antecedente está orientado a tratar detectar las deficiencias de los sistemas de la entidad y cómo logró orientar políticas para el mayor compromiso del personal con su institución.

En [15] presenta un proyecto para dar solución los inconvenientes que presentan en la actualidad las microfinancieras, quienes no gestionan o presentan deficiencias en gestionar riesgos de TI, lo que trae a consecuencia la interrupción en continuidad del negocio, que conlleva a grandes pérdidas económicas y desconfianza en el cliente, quienes optan por el cambio de entidad financiera. El propósito de este estudio se enmarca en analizar cómo actualmente le rubro microfinanciero viene gestionando sus riesgos, incluyendo una revisión documentada y estudiar normativas a cumplir, aplica métodos y gestión de riesgos de TI, proponiendo un modelo que se adapte al contexto del estudio, aplicándolos a tres microfinancieras que se ubican en el departamento de Lambayeque, luego por medio de evaluación de expertos y al aplicar el caso de estudio, se puede contrastar lo que se había planteado como hipótesis. Esta investigación pretende mostrar que implementando el modelo de gestión de riesgos de TI se apoya la continuidad del negocio

microfinanciero en el departamento Lambayecano. Se cree conveniente citar este antecedente para afianzar más el conocimiento respecto a la protección de activos de información financiera.

1.2 Base Teórico Conceptual

En esta sección se describirán conceptos que se han analizado para dar soporte teórico del método propuesto de esta tesis.

1.2.1 Seguridad de la Información:

Al desarrollar el modelo propuesto fue importante entender conceptos de seguridad tales como, según [16] la seguridad es un estado de bienestar ya que te permite poner la confianza en algo o en alguien sin embargo si la seguridad se mira en un ámbito disciplinario se define como una ciencia en la que se puede evaluar y gestionar los riesgos en los que se encuentra algún bien.

[17] Se define como información al conjunto de datos organizados que posean valor para la empresa independientemente como se guarden o cuando se elaboren.

Según [18] la seguridad de información se define como un sistema de información seguro que diseña normas, planea técnicas, métodos y procesos con el fin de que la información esté disponible y sea confiable.

Para [19] La información es un activo esencial para las entidades así como otros activos sin embargo es mucho más importante en un ambiente comercial por lo tanto necesita ser protegido adecuadamente ya que se ve expuesto a un gran número de amenazas y vulnerabilidades. Es importante la seguridad de

la información ya que sirve como facilitador para las organizaciones públicas y privadas ya que ambos sectores protegen las infraestructuras críticas.

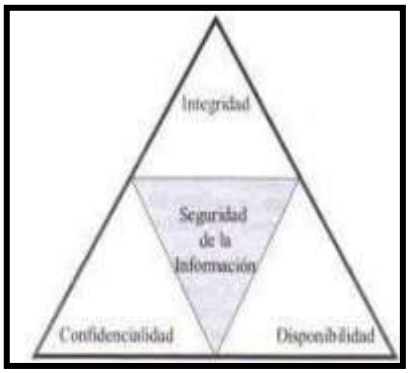
Para la ISO 27001 [20], seguridad de la información trata sobre la preservación de una organización respecto a sus activos de confidencialidad, integridad y disponibilidad.

Así mismo su estructura guarda relación con otros sistemas de gestión tal como la ISO 9001 referida a la Gestión de la calidad, además en lo concerniente a tecnología y proveedores, la seguridad es neutral, demostrando así que la protección de información aplica para toda la organización y no solo para áreas de Tecnología de Información.

1.2.2 Servicios de Seguridad de la Información

Según [21], la triada o los pilares de la seguridad de información, tenemos la confidencialidad que es la que garantiza que cada mensaje transmitido solo lo podrá ver el destinatario a quien fue remitido. Así también la disponibilidad garantiza un correcto funcionamiento y un sistema fuerte que responda adecuadamente frente a cualquier ataque. Además, la integridad garantiza que ningún mensaje sea modificado al momento de ser creado o transmitido a su destinatario.

Figura 4: Seguridad de información - norma ISO/IEC 17799



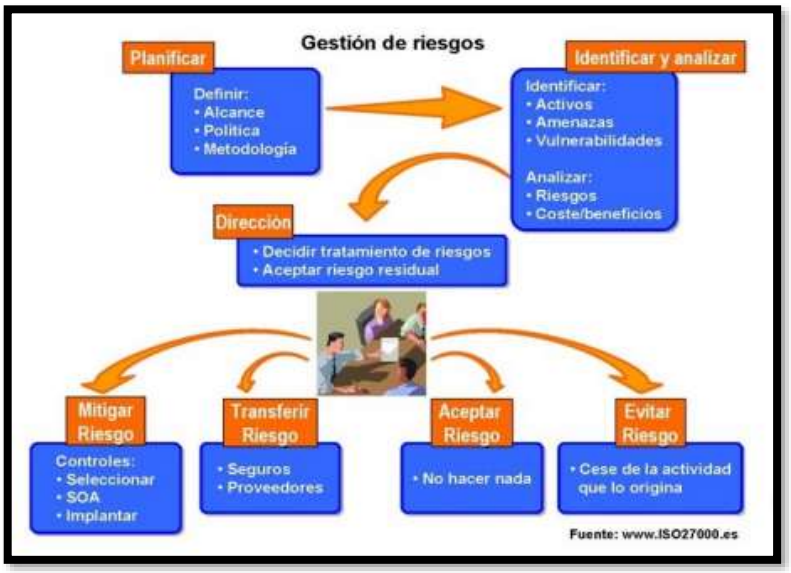
Fuente: *[21]*

1.2.3 Gestión de Riesgos

Así mismo cabe mencionar la importancia de definir el termino Gestión de Riesgos, en el cual "riesgo" se refiere la probabilidad de pérdidas y daños futuros relacionados con los (individuos, familias, comunidades, ciudades, etc.) es una condición latente que capta la posibilidad de perdidas futuras físicas, sicosociales, culturales que están sujetas al análisis y medición de términos cualitativos y cuantitativos [22].

La existencia de riesgo es la presencia de amenazas y factores de vulnerabilidad. [20] Las amenazas son situaciones de riesgo la cual tiene pérdidas materiales e inmateriales en activos de información. El SGSI se basa en la ISO 27001 para apoyar en el control de amenazas; siendo así que el riesgo al materializarse, se convierte en una clara amenaza para el activo de información.

Figura 5. Gestión de riesgos.



Fuente: *[23]*

Riesgo de Tecnología de la Información: La gestión de riesgos utiliza los resultados de analizar el riesgo para controlar los riesgos identificados [24]. El análisis de riesgo identifica las necesidades de seguridad, determina la vulnerabilidad de la misma ante las amenazas y estima el impacto.

Dentro de la evaluación de riesgos, tenemos que según [25] la evaluación **Cuantitativa** es la determinación de una perdida potencial y la asignación de valores monetarios de dicha perdida.

De manera general, resulta más complicado llevar a cabo esta evaluación a comparación de la evaluación cualitativa. Ya que se debe asignar un dato numérico para tener un resultado más preciso en relación a la situación real de los riesgos y otros activos de la empresa.

La evaluación **cualitativa**, [25] es la que valora las características del escenario de las amenazas sobre los activos y los clasifica como alto, bajo y medio. Esta evaluación se convierte en elemento subjetivo, motivo por el cual para la seguridad de la información, resulta necesario establecer criterios resulta muy básico definir criterios precisos de lo que representa cada categoría, el objetivo es tener resultados conscientes.

1.2.4 Controles en la seguridad de la información

[26] Son métodos, procedimientos que minimizan los ataques y permiten proteger activos importantes para una entidad, la exactitud y confiabilidad de sus registros. Los controles de Seguridad soportan los activos de seguridad (Disponibilidad, Integridad y Confidencialidad) y abarcan las terminologías básicas (Vulnerabilidad, Riesgo, Amenaza y Control). Los controles tienen los siguientes niveles: Administrativo, Técnico y Físico.

Administrativo: controles al administrar sistemas, documentos de confidencialidad, personal de seguridad y entrenamiento a personal.

Técnico: Controles a nivel lógico en hardware y software, se considera también la configuración a nivel firewall, políticas de autenticación.

Físico: Especifican el lugar donde el activo está siendo protegido, para ejemplificación guardias de seguridad, cerraduras, circuitos cerrados.

Los controles son configurados en modo "defense-in-Depth", lo que significa estar a muchas capas de seguridad, para que pueda reducir la posibilidad de penetración y el nivel de afectación que pueda ocasionar un atacante.

Al escoger el control a utilizar, en primer lugar se debe conocer la funcionalidad de cada una que propone la norma. Principalmente están por categorías tales como: Disuasorio, Preventivo, Correctivo, Recuperativo, Detectivo, Compensatorio.
[26] Los tipos de controles en los sistemas de información son:

1.2.4.1 Controles Preventivos: controles que disminuyen la probabilidad de materialización del riesgo, proponiendo un margen de violaciones de seguridad, son más rentables y deben incorporarse en los sistemas, de esta manera evitar costos de corrección o reproceso.

1.2.4.2 Controles Detectivos: Definidos como controles que si bien no evitan las causas del riesgo pero si ayudan a detectarlas antes de que ellos ocurran. Son de gran utilidad cuando se evalúan la eficacia de controles preventivos. Son más costosos que los preventivos, se encargan de medir la efectividad de los controles preventivos, aunque algunas amenazas no puedan evitarse durante una etapa preventiva, otra bondad es que incluyen revisiones y comparaciones. También incluye conciliaciones, conteo de inventario físico, analizar procesos de cambio, técnicas automáticas. Además propone validaciones para transacciones, clave, manipulaciones de reportes y auditoría interna.

1.2.4.3 Controles Correctivos: apoya de manera eficiente la investigación de las causas de los riesgos y de esta manera estudiarlas para encontrar la corrección más adecuada. Puede que no resulte ser la más eficiente por lo que es necesario la intervención de controles detectivos para los correctivos, ya que al corregir fallos en cierta actividad queda expuesta a muchos fallos. También ayuda a tomar decisiones en procedimientos para una corrección (la recurrencia). Generan reportes que son elevados a la gerencia, vigilando todo tipo de actividad hasta hallar con la solución.

1.2.4.4 Controles Disuasivos: son aquellos que reducen la probabilidad intentando desalentar un potencial ataque y de esta manera desviar la intención del individuo perpetrador.

1.2.4.5 Controles Recuperativos: toman un lugar posterior al ataque con la finalidad de intentar proveer una restauración de un sistema y volver a la operación regular.

1.2.4.6 Controles Compensatorios: entrega otra medida de control cuando las empresas no pueden financiar o se vean limitadas en algún aspecto institucional, que no les permita implementar el control respecto a los riesgos identificados.

Se puede establecer una propuesta de modelo de Sistema de Gestión de la Seguridad de la Información se basa en ISO 27001 tomando en cuenta la siguiente estructura piramidal:

Figura 6. Modelo de Sistema de Gestión de la Seguridad de la Información

Fuente: [27]

[27] **Manual de seguridad:** El documento dirige y determina el sistema de seguridad, el cual se basa en objetivos, responsables con responsabilidades, políticas, delimitación en el alcance del SGSI.

Procedimientos: Nivel operativo que propone planificar, operar y controlar los procesos de seguridad de una manera eficientes.

Instrucciones, checklists y formularios: Son un tipo de test que verifica si algunas tareas o actividades descritas son cumplidas o no.

Registros: Son documentos que recoge evidenciar el nivel en el que se cumple el requisito del sistema de gestión de seguridad de la información. Este registro se asocia con otros niveles tales como output demostrando que se ha cumplido con los mismos.

1.2.5 La norma ISO/IEC 27001

Comprendiendo el concepto de información, es importante conocer esta norma, [20] lo define con base en el Ciclo Deming el cual permite Planificar-Hacer-Verificar-Actuar, también conocido por sus siglas en inglés PDCA (Plan-Do-Check-Act).

Desarrolla un SGSI que permite evaluar todo tipo de riesgos o amenazas que pueden poner en peligro la información de la entidad o de terceros. Además facilita el formular estrategias para minimizar los peligros.

El Sistema de Gestión de La Seguridad de la Información propuesto por Norma ISO 27001 se resume:

Figura 7. Resumen de las fases que propone Norma ISO 27001.

Fuente: [28]

Al momento de implantar el SGSI según la norma ISO 27001 se centra en evaluar riesgos permitiendo a las empresas integrar este sistema de mejora continua y tengan la visión necesaria para determinar el alcance, el implante y la aplicación de esta norma.

.

1.2.5.1 Metodología sugerida Norma ISO/IEC 27001

[20] Existen muchas metodologías de Evaluación de Riesgos y se debe elegir la apropiada para el requerimiento de cada negocio. Fases de la metodología sugerida en la Norma.

Figura 8. Métodos de evaluación y tratamiento del riesgo.

Fuente: [28]

1. Identificar Activos: Se entiende como activo lo que es de suma importancia para una empresa; incluye los soportes físicos e intelectuales o informáticos así también la manera en que pueda verse afectada una reputación en la organización, etc.

2. **Vulnerabilidad:** Son activos susceptibles o que presentan debilidades para un determinado proceso, llegan a la posibilidad de permitir que un atacante comprometa, la integridad, disponibilidad o confidencialidad.

3. **Amenazas**: Situaciones o fenómenos que atacan a los activos de la información.

Ejemplo: Espionaje, Incendios.

4. **Requisitos legales:** Normas o decretos que Empresa debe ejecutar en beneficio a su clientela, socios estratégicos y proveedores.

5. **Identificar riesgos:** Resultado de evaluar la vulnerabilidad y amenaza de activos que al materializarse puedan afectar total o parcialmente la disponibilidad, confidencialidad e integridad.

6. **Calcular riesgo:** Sirve para poder determinar el riesgo que tiene mayor prioridad, aplicando Riesgo = impacto de una amenaza x probabilidad que esta suceda.

7.- **Plan para tratamiento del riesgo:** Al definir este plan, ya se está preparado para identificar los controles que más se adecúen al riesgo estudiado según las definiciones mencionadas anteriormente, de esta manera se pueda cumplir con: Asumir, Reducir, Eliminar y Transferir los riesgos.

.

1.2.6 Metodología OCTAVE

[29] Ayuda a las organizaciones a identificar y evaluar riesgos de seguridad de la información.

- Se desarrolla evaluando riesgos de manera cualitativa que incluyan un riesgo operacional y apoya a determinar la tolerancia.
- Identifica los activos al desarrollar una revisión de las funciones principales en la organización.
- Identifica amenazas y vulnerabilidades sobre los activos.
- Evalúa estas amenazas y la consecuencia que estas puedan causarle a la entidad.

Son tres las metodologías que están a disposición del público como: OCTAVE, OCTAVE-S y OCTAVE Allegro.

OCTAVE se adecuará en base al foco de las necesidades de evaluar los riesgos. No obstante el método OCTAVE Allegro, es una propuesta que brinda a la organización el proceso de una forma simple y centrada exclusivamente a los activos de información.

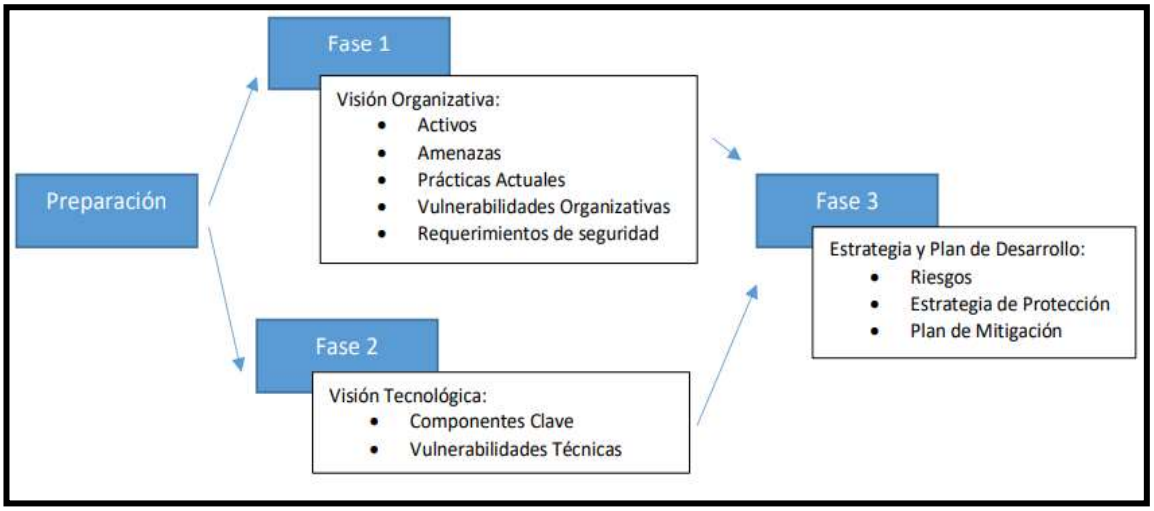
Octave se proponía como guía la cual incorporaba elementos relacionados a procedimientos, catálogo en la información y una serie de capacitaciones, desarrollándolas en base a talleres con un equipo de análisis interdisciplinario entre ellos: responsables de operar el sistema de gestión, el socio de negocio y un grupo de trabajadores del área de TI [29].

- **OCTAVE** se enfoca a organizaciones medianas y grandes, aproximadamente con un número de trabajadores mayores a 300, basado en:
- Organigrama de muchos niveles
- Cuenta con infraestructura TI propia
- Capacidad en la evaluación de vulnerabilidades.
- Interpretación de resultados obtenidos luego de evaluar vulnerabilidades.

El método OCTAVE se describe en 3 fases. En la fase 1, se identifican activos importantes a los cuales se les realizará un tratamiento proponiendo una estrategia de protección actual respecto a los activos identificados. Luego se identifica cuáles de todos los activos pueden resultar muy críticos para la institución, es ahí donde se definen requisitos para la seguridad y selecciona las amenazas que interfieran en los procesos. La fase 2, el equipo evalúa la infraestructura que permita terminar el análisis de las amenazas identificadas durante la fase 1, para posteriormente informar las mitigaciones descritas en la fase 3.

Por último durante la 3 fase, se encarga de identificar los riesgos desarrollando un proceso o procesos de mitigación de riesgos de los activos más importantes para la organización.

Figura 9. Métodos de evaluación y tratamiento del riesgo.



Fuente: [29]

- **Octave-S** desarrollado por SEI (Software Engineering Institute) para ser adecuado a organizaciones de tamaño pequeños. En su versión 1.0 el método se enfoca a empresas con un máximo de 100 trabajadores o menos.

Tomando en cuenta las características de OCTAVE, también el método OCTAVE-S tiene 3 fases, no obstante, OCTAVE-S se trabaja con miembros en el equipo que tengan conocimientos de los procesos de la entidad, sin basarse en una serie de talleres formales para obtener dicha información. Se enfoca más en analizar que el equipo integrado por cinco personas, cuenten con conocimientos prácticos sobre los activos identificados, estos se deben vincular los requisitos en seguridad, amenazas y proponer estrategias en seguridad.

Una divergencia reveladora en OCTAVE-S está más sintetizado y ordenado que el método OCTAVE.

Sus conceptos vinculados a la seguridad incluyen fichas de trabajo y una seria de guías propuestas por OCTAVE-S, permitiendo que los involucrados en el equipo no sean muy profesionales en riesgos.

OCTAVE-S analiza de manera más extensa la estructura de información dentro de la empresa, puesto que instituciones pequeñas no tienen recursos para implementar herramientas de vulnerabilidades, además incluye una

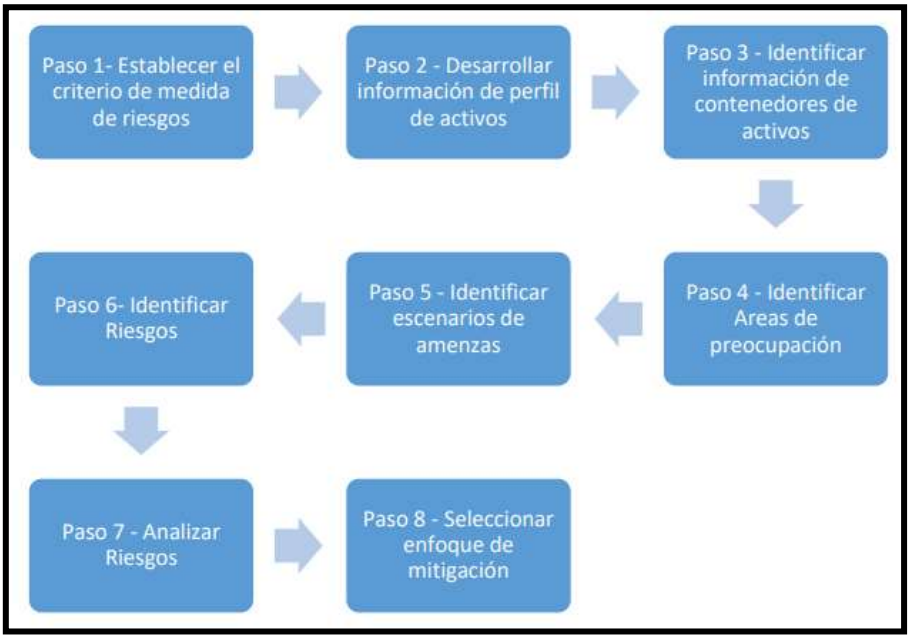
evaluación acotada a los riesgos de forma estructurada, eliminando restricciones que adoptan las empresas.

La base de OCTAVE faculta evaluar el ambiente de riesgos operacionales en una empresa, con la finalidad de tener resultados sin tener conocimientos amplios de evaluación de riesgos. Este enfoque es un nuevo giro para los anteriores enfoques OCTAVE, pues sólo se concentra en los activos de información, verificando la manera en que se utiliza, almacena, procesa, para conocer si está o no expuesto a las amenazas, vulnerabilidades.
Similar a las metodologías antes mencionadas, OCTAVE Allegro puede ejecutarse bajo un entorno colaborativo para contemplar los elementos. Ejemplo: guías, hojas de trabajo y cuestionarios.

- OCTAVE Allegro se adecua al desarrollar análisis de riesgos en empresas que tengan experiencia mínima en relación a la gestión, información de riesgos.

Allegro de OCTAVE cuenta con 8 procesos, como muestra la Figura 10. En la primera fase, desarrollan mediciones de riesgo que guarden relación con los conductores organizativos de la entidad. Durante la fase 2, los activos o criterios se perfilan. En este procedimiento se proponen límites claros para el activo, identificando requisitos de seguridad, para luego trasladarlos donde se ubica, traslada o procesa el activo. En tercera fase, se identifican la ubicación de las amenazas, cómo transporta y almacena el activo. En la última fase, se proponen planes de mitigación.

Figura 10. Fases OCTAVE desde el enfoque Allegro.



Fuente: [29]

1.2.7 Método Mehari

Propuesto por CUSIF (Club De La Sécurité De L'information Français), MEHARI metodología que permite analizar de forma sencilla el evaluar riesgos y seleccionar estrategias de cómo reducirlos [30]. La metodología consta de planes de trabajo que ayuden a clasificar y cuantificar el nivel del riesgo.

El documento de CLUSIF [31], indica que lo importante para MEHARI es facilitar una metodología para evaluar y gestionar riesgos, con considerable dominio de seguridad de la información, respetando lo dicho en la norma ISO/IEC 27005:2008, suministrando herramientas necesarias para su ejecución. Otros objetivos que se adicionan:

- Consiente en analizar directa e individualmente eventos de riesgos que se describan en diferentes situaciones o escenarios,

- Brinda herramientas complejas especialmente adaptadas para la gestión de la seguridad en un tiempo pequeño, mediano y largo plazo, además se adaptan en diversos niveles de madurez.

[32] La metodología sirve de apoyo a las personas responsables introducidas en la gestión de riesgos, dentro de sus actividades. En un ámbito primero se relaciona en la forma de analizar o evaluar un riesgo, proponiendo el enfoque estructurado que se compone en factores tales como:

- Factor estructural u organizacional, aquellos que dependen del activo primordial de la empresa, considerando su contexto.
- Factor para reducir riesgo, se basa directamente en las medidas de seguridad que serán implementadas.

Analizar la seguridad necesaria para identificar que tan grave es la consecuencia de situar el riesgo. Comúnmente se da como factor estructural, en cambio evaluar la seguridad favorece la reducción de u riesgo identificado.

MEHARI incorpora evaluar cualitativa y cuantitativamente factores que colaboren en identificar niveles de riesgo como respuesta a ello. MEHARI también incorpora instrumentos y bases de datos para conocer lo que se está diagnosticando, así también las medidas de seguridad, que complementan fundamentalmente el marco descrito en la ISOEC 27005.

Como ámbito segundo, concerniente en evaluar la seguridad, permitiendo estimar el nivel de seguridad, las propuestas de soluciones para reducir el riesgo, en los siguientes aspectos:

- Revisión de vulnerabilidades, es un elemento que tiene como resultado la evaluación de la vulnerabilidad que sirve como entrada para analizar el riesgo, teniendo como finalidad la garantía que los servicios de seguridad cumplan efectivamente con su comedido.

- Plan de seguridad, se basa en revisar la vulnerabilidad. Obtenido como un resultado propio de evaluar los servicios de seguridad, enfocados en la ejecución del mejoramiento de servicios que no cuenten con un alto nivel de calidad.

- La base de datos en el método MEHARI se utilizan para formar marcos de referencia, que contienen instrucciones que la institución debe tomar en cuenta.

- Dominios que soportan el evaluar las vulnerabilidades. Cuando se analiza los riesgos tomados como base de identificar cualquier situación de riesgo y con el propósito de soportar todo riesgo no tolerable, **MEHARI** no se centra solamente al campo de Tecnología.
- Describir la propuesta de evaluación. Es quien proporciona un enfoque extenso y coherente en seguridad.

En el tercer ámbito se analizan las amenazas, comprende los riesgos y amenazas de los negocios ya que es fundamental por lo que requiere un estricto método de evaluación. Para realizar esta evaluación se toma en cuenta lo siguiente:

- Módulo para examinar las amenazas, son la clave para analizar. Sin embargo con los diferentes fallos o averías no permiten tener un propio juicio sobre el estado actual de nivel de riesgo identificado.

- Analizar amenazas de seguridad: Pone en marcha cualquier plan de seguridad. Sin importar el enfoque determinará implantar de los planes de tratamiento que justificaran el costo en inversión necesario.

- Clasificación: fundamental en políticas de seguridad. Siendo las organizaciones quienes por medios de reglas gestionan seguridad, se ven

exigidas en definir reglas propias de manera interna y acciones que se efectúen relación de la densidad de información procesada.

- Acciones respecto a amenazas de seguridad: Consiste en procesar un análisis de amenazas de seguridad que necesitan del aporte de los encargados de operar siendo parte fundamental planificar la seguridad.

De una manera general se puede apreciar las fases como lo describe la figura:

Figura 11. Perspectiva MEHARI

Fuente: [32]

1.2.8 Metodología Magerit

[33] Creada en el Consejo Superior de Administración Electrónica, con una orientación hacia los riesgos primordiales con relación a los sistemas de información. En su segunda publicación del año 2005 con propósitos de efectuar una exploración constructiva concerniente a los peligros que corren las organizaciones, implicando asuntos profundos respecto a gestión de riesgos. Luego busca una adaptación, no solo basándose en experiencias, adicionalmente busca actualizaciones que presenten las normas internacionales de ISO.

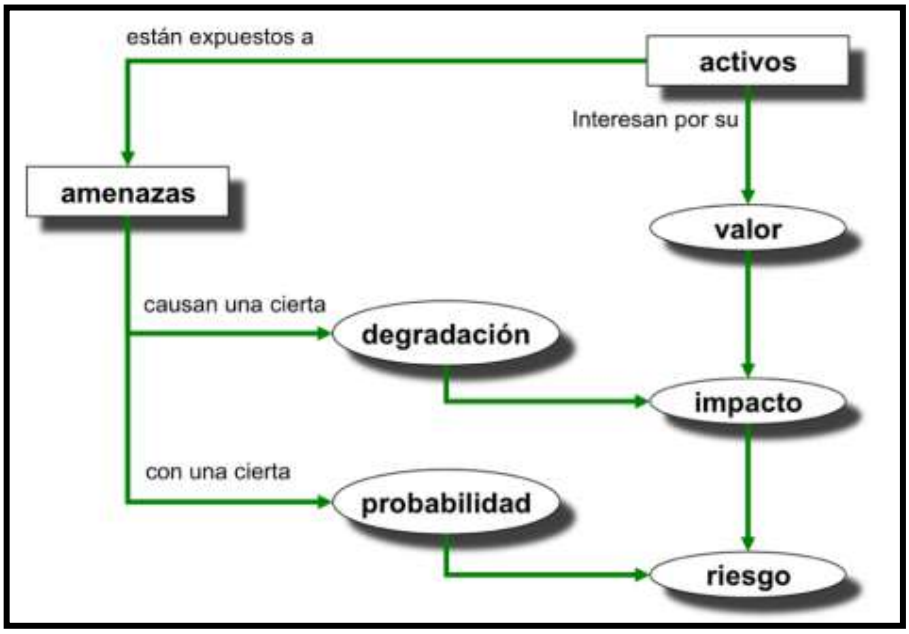
[32] Analizar riesgos es un acercamiento metódico para comprobar los mismos, teniendo en cuenta:

a. Establecer importantes activos para la empresa, buscando la relación y valor, sabiendo que su afectación supone la degradación.
b. Precisar amenazas que se encuentran arriesgados aquellos activos.

c. Determinar salvaguardas existen y son realmente eficientes para contrarrestar el riesgo.

d. Proponer una estimación para el impacto y riesgo que tiene el activo cuya amenaza fue materializada, evalúa la manera en que la ponderación del impacto afecta a que una amenaza ocurra.

Figura 12. Magerit – Componente para analizar riesgos potenciales.



Fuente: [33]

Para analizar riesgos, tiene varios pasos que guardan relación con activo, vulnerabilidad, amenaza, salvaguarda, riesgo residual que se sintetiza de esta manera.

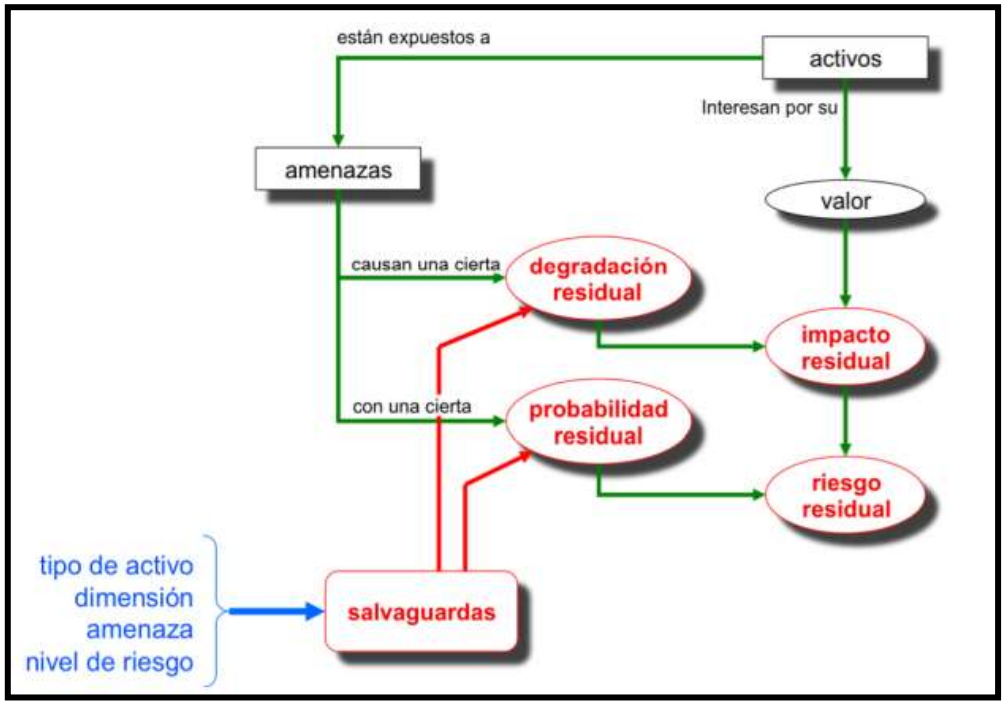
Como primer paso, concerniente a activos como componentes importantes en sistema de seguridad, propenso a ataques de manera deliberada o accidental, esto trae resultados terribles para la institución. Incluye: información, datos, servicios, aplicaciones, equipo de comunicación, recurso físico y humano.

La fase valora el activo para la institución. Teniendo en consideración los servicios que se prestan activos nombrados principales operan procesos críticos del negocio. Tiene dimensiones que miden la confidencialidad,

integridad, disponibilidad, autenticidad y trazabilidad. A demás otra apreciación es que debe considerarse la disponibilidad, posiblemente tenga un impacto severo de mitigar en relación al corte o suspensión del servicio.

El segundo paso, consiste en delimitar las amenazas que afecten los activos. Las amenazas ocurren y todo lo que puede ocurrir, es de interés para nuestros activos y puede ocasionar un daño.

Figura 13. Elementos de análisis del riesgo residual.



Fuente: [33]

Se considera que la identificación de las amenazas y valorar el impacto; la probabilidad y el impacto se verifica en esta fase. Se miden los impactos y riesgos por los cuales los activos se pondrían ver expuestos. Es muy fácil identificar sistemas que no se encuentran protegidos: Las consecuencias posibles de ocurrir no toman en consideración salvaguardas.

Establecen salvaguardas para medir mecanismos tecnológicos que conlleven a reducir el riesgo. Existen amenazas puede ser minimizadas simplemente con

organizarlas de manera adecuada, otras en cambio necesitan un equipo técnico, que brinde seguridad física y políticas al trabajador.

Así también en el tercer paso, se determina las salvaguardas y eficiencia de proteger los activos.

Como cuarto paso, se proponen salvaguardas que ayudan a medir la madurez de un sistema de gestión, queda un escenario con la posibilidad de un impacto que se nombra residual. Se rectifica el impacto, calculando un valor potencial reducido a valor residual. Para calcular el impacto residual, tomando en cuenta que los activos ni su dependencia han sido modificados, se calcula el impacto con un nivel de degradación. La dimensión al degradarse toma como premisa la eficiencia de salvaguardas, el cual se define como la diferencia de eficacia perfecta y real. El cálculo del impacto residual, se acumula en activos de menor escala y pueden repercutir en los activos considerados superiores.

Como quinto paso, las salvaguardas definidas en un proceso de gestión, deja al sistema en una situación vulnerable a riesgos, denominado riesgo residual. Un riesgo se considera transformado cuando el valor potencial produce un valor residual.

La degradación calcula el impacto residual. En la probabilidad residual, siempre se considera la eficiencia de la salvaguarda contra la amenaza y ellos debe ser la proporcionalidad entre la diferencia de eficacia real y perfecta.

1.2.9 NIST SP 800:30

SP 800:30 (Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información) [34]. Se ha elaborado por el Instituto Nacional de Estándares y Tecnología (NIST), de esta manera evalúa riesgos de seguridad de la información que se enfoca a temas relacionados con Tecnología de

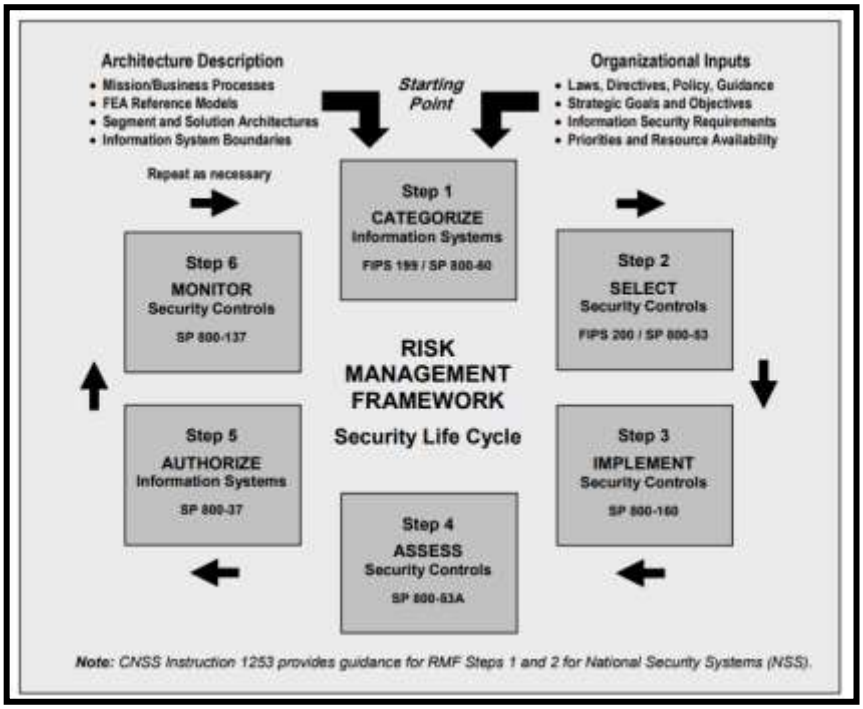
Información, brinda controles de seguridad además de guías que puedan aplicarse desde un enfoque netamente técnico [35].

Esta guía provee pautas fundamentales para administrar el riesgo, así como evaluación y mitigación de riesgos identificados dentro de la Tecnología de Información apoyando a las empresas a proteger todo lo que tenga que ver con su tecnología.

El método NIST SP 800:30 consta de 9 fases, reconocidas principalmente, tales como:

- Caracterización del sistema, establece alcance y límites en las operaciones cuando e evalúa los riesgos de la institución.
- Identificar amenazas, se determina cuál es el origen y como se promueven las mismas dentro de la institución.
- Identificar vulnerabilidades: Identifica las debilidades que se suelen presentar en un sistema, materializadas por la amenaza.
- Analizar controles.
- Estimar una probabilidad
- Analizar el impacto de la amenaza.
- Determinación del riesgo: evalúa dentro de un sistema de información el riesgo ocurrido.
- Control recomendado: Listan controles para de esta manera reducir el riesgo previamente identificado, hasta que se pueda aceptar, luego de ellos se redactan informes de resultados describiendo amenazas y vulnerabilidades, el cálculo de riesgo y proponer ciertas sugerencias al implementar estos controles.

Figura 14. Risk Management Framework SP 800:53



Fuente: [36]

Este método una base efectiva para gestionar riesgos, definiendo guías que al implementar puedan para aliviar los riesgos identificados dentro de un sistema de tecnología. Este propósito apoya a empresas a mejorar el manejo de los riesgos con 3 procedimientos: evaluar, mitigar, analizar el riesgo evaluado [37].

1.2.10 ISO/IEC 27005:2011 Gestión del riesgo de S.I.

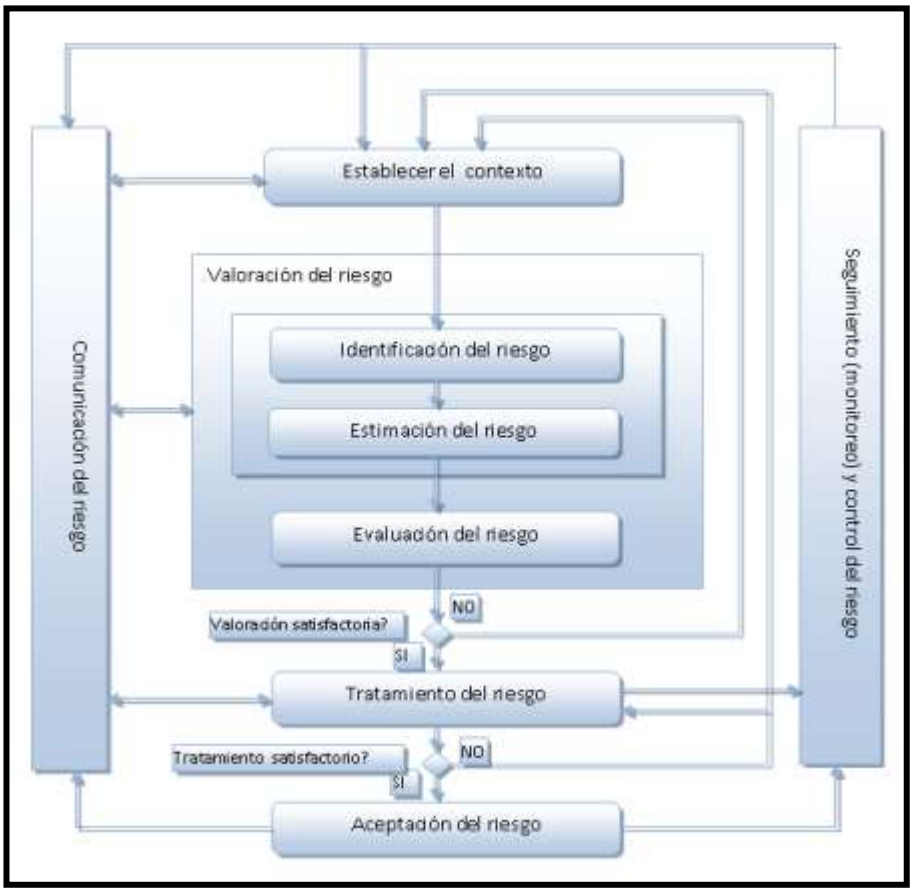
La norma ISO/IEC 27005:2011, [ISO/IEC 11], se integra a la familia de ISO 27000 orientada a la seguridad de la información, de tal manera que se complementa las normas ISO 27001 y 27002, que precisan que las entidades deben analizar riesgos [38].

El enfoque que proporciona la norma, detalla procesos que ayudan a la gestión de riesgos de la seguridad de la información, apoyándose en las definiciones sustentadas de la ISO/IEC 27001:2005. Aporta enfoque genérico

y se apoya en métodos que sirvan para analizar y gestionar riesgos; aplicable a cualquier entidad que quieran controlar o gestionar riesgos en seguridad.

[38] La norma tiene doce cláusulas y 6 anexos que soportan la implementación de cada cláusula. Ellas son: Objetivo de la aplicación, Normativas, definiciones y términos, estructura, información general, visión, establecer el contexto, valorar riesgo, tratar el riesgo, para poder luego considerarlo en un nivel aceptable, comunicándolo y establecer monitorear y revisar dicho riesgo.

Figura 15. Pasos para gestionar riesgos en ISO 27005.



Fuente: [38]

En el desarrollo de la gestión de riesgos se refleja desde la cláusula tal como se detalla.

Cláusula 7, Establecer el contexto, describe los objetivos establecidos para el resto del proceso.

Cláusula 8. Valorar riesgo, se recopila la necesaria información que se requiera para la valorización y priorización de riesgos. Dividido en 3 apartados: Identificar riesgo, estimarlos y luego evaluarlos

Cláusula 9. Tratar el riesgo, establece los procesos para tratar con cada riesgo valorado, logrando con este reducirlo, aceptarlo, evitarlo o transferirlo.

Cláusula 10. Aceptar el riesgo, son riesgos que la organización opta por aceptar, y se justifica en cada riesgo aceptado. Posterior a ello se debe realizar un tratamiento para el riesgo residual.

Cláusula 11. Comunicar el riesgo, se comunica a los interesados de manera que transfieran información respecto a los riesgos, contantemente en el proceso.

Cláusula 12. Monitorear y Revisar el riesgo, al analizar los riesgos, ellos deben ser actualizados en todas sus modificaciones internas o externas que comprometan el valorar riesgos, luego se implementan monitoreo y evaluación continua.

1.2.11 NTP ISO/IEC 27001:2014

La Norma Técnica Peruana ISO/IEC 27001:2014 [39] tiene una conexión con la norma internacional ISO 27001:2013 y contiene modificaciones expresas por ISO después de su publicación. Esta Norma ha sido formulada para facilitar los requisitos sabiendo que se debe: establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

En una empresa, adoptar un sistema de gestión de seguridad de la información es sumamente importante crear una estrategia.

La empresa pone en marcha un sistema de gestión de seguridad de la información que satisfagan necesidades, objetivos, requisitos de seguridad, procesos organizados, tamaño y estructura. Estos factores cambian con el tiempo.

El SGSI maneja procedimientos para gestionar riesgos y brindando seguridad a personas con interés en relación a los riesgos se están operando apropiadamente; resguardando así la confidencialidad, integridad y disponibilidad.

Es fundamental que el SGSI esté incorporando procesos, estructuras, gestión general y la seguridad de la información de la empresa sea considerada en el sistema los controles y diseño de procesos; donde se tiene como expectativa incorporar un sistema de gestión de seguridad de la información haciendo que aumente el nivel conforme a la necesidad de la entidad.

La empresa es evaluada interna y externamente a través de la norma técnica peruana donde ella determinará la capacidad que tiene la entidad en el cumplimiento de los requisitos de SI de la misma.

1.2.12 Resolución Ministerial N° 004-2016-PCM

[40] La PCM admite el uso indispensable de la NTP ISO/IEC 27001:2014 Tecnología de la Información, Métodos de Seguridad, Sistemas de Gestión de Seguridad de la Información, aplicado a instituciones que conforman el Sistema Nacional de Informática, que tiene como objetivos:

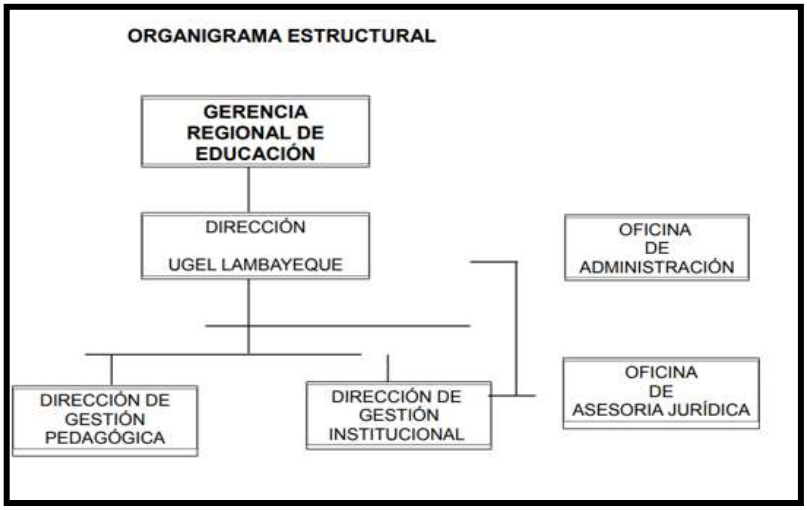
- Fijar normas en las actividades de información oficial.
- La actividad de informática oficial se organiza, incorpora y racionaliza.
- Impulsar la formación, indagación y progreso de las actividades informáticas.

El Consejo Consultivo Nacional de Informática (CCONI), el Comité de Coordinación Interinstitucional de Informática (CCOII), integran este sistema nacional, Las agencias Sectoriales de Informática y demás agencias de Informática de los Ministerios, Entidades Centrales, Establecimientos Públicos en todo el país y Sociedades del Estado, los Gobiernos Regionales, los órganos de Informática de las Municipalidades, Los órganos de Informática de los Poderes Públicos y de los Organismos que son Autónomos.

1.2.13 Unidades de Gestión Educativa Local Región Lambayeque

1.2.13.1 La Unidad de Gestión Educativa Local de Lambayeque, [41] según el Artículo 73° de la Ley General de Educación 28044, es una unidad ejecutora dependiente del Gobierno Regional Lambayeque, teniendo total control respecto a las gestiones de educación, estando ubicado provincia de Lambayeque. Tiene como propósito, fortificar propuestas que se aboquen a la gestión pedagógica y administrativa de los establecimientos educativos.

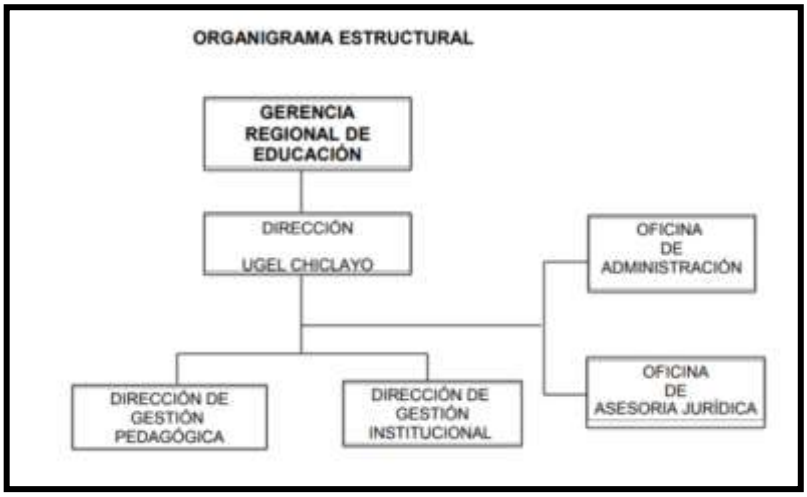
Figura 16. Organigrama Estructural de UGEL Lambayeque.



Fuente: [41]

1.2.13.2 La Unidad de Gestión Educativa Local de Chiclayo, [42] Se describe como órgano descentralizado de la Gerencia Regional de Educación Lambayeque, implicada en procedimiento que orienten al alcance de objetivos diseñados que se encuentren alineados con el Plan Educativo Nacional al 2021, así también el Plan de Desarrollo Regional Concertado 2011-2021, tiene como jurisdicción a todas las Instituciones Educativas de la provincia de Chiclayo.

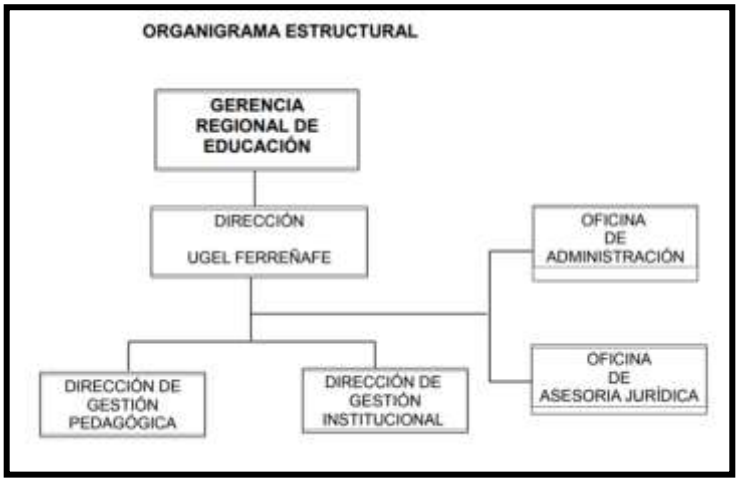
Figura 17. Organigrama Estructural de UGEL Chiclayo.



Fuente: [42]

1.2.13.3 La Unidad de Gestión Educativa Local de Ferreñafe, [43] Es una unidad ejecutora del pliego del Gobierno Regional Lambayeque, que se preocupa por fortalecer la educación en Ferreñafe, teniendo como misión ser una institución que suscita y que vela por los procedimientos normativos de la educación en Instituciones Educativas de Ferreñafe, certificando la asistencia de calidad e imparcialidad en atención con las necesidades educativas de la comunidad Ferreñafana, apoyando al refuerzo del sistema democrático y desarrollo sostenible de la región.

Figura 18. Organigrama Estructural de UGEL Ferreñafe.



Fuente: [43]

CAPÍTULO II MATERIALES Y MÉTODOS

2.1. Diseño de la investigación

El diseño de contrastación de hipótesis es del tipo cuasi experimental debido a que se [44, p. 184] manipulan deliberadamente, mínimo una de las variables consideradas independientes observando su efecto respecto a la dependiente, teniendo el grado de seguridad sobre la equivalencia inicial del grupo.

Se busca evaluar el efecto de ejecutar un modelo de seguridad de la información en las unidades de gestión educativa local de Lambayeque, usando un modelo preprueba/posprueba con un solo grupo:

$$G\ O_1\ X\ O_2$$

Dónde:

G = Caso de estudio seleccionado.

O_1 = Identificar los estándares relacionados a la seguridad de la información financiera de las unidades de gestión educativa local de Lambayeque, antes de aplicar el modelo de gestión de seguridad de la información.

X = Modelo de Gestión de Seguridad de la Información.

O_2 = Resultado de juicio experto del modelo de seguridad de la información financiera de las unidades de gestión educativa local de Lambayeque, después de aplicar el modelo de gestión de seguridad de la información.

2.2. Población, Muestra y Muestreo

En base a diagnosticar inicialmente la presente tesis, se tomaron en cuenta las entidades públicas de unidades de gestión educativa local dentro de Lambayeque, que lo conforman: Unidad de Gestión Educativa Local Lambayeque, Chiclayo y Ferreñafe.

En el Anexo 1, se muestra un cuadro más detallado de la comparación de estas unidades de gestión educativa local.

2.3. Métodos, Técnicas e Instrumentos de Recolección de Datos

Se ha empleado instrumentos que sirvieron para recolectar y analizar la información desde la perspectiva metodológica cuantitativa. Apoyado con las técnicas de recolección de datos:

- Encuesta, al aplicarla, se pudo conocer la situación actual la seguridad de la información, considerando el nivel de controles de seguridad que tenían establecidos en unidades para protección de información y el tipo de respuesta que tienen ante cualquier tipo de amenaza.

- Revisión de documentos, se revisó los documentos legales de las unidades de gestión educativa, tales como el Manual de Organización y Funciones, además de analizar los controles que propone la norma ISO 27002 de Seguridad de la Información en su Anexo A.

2.4. Técnicas de Procesamiento de Datos

La encuesta se realizó a encargados de la oficina del Centro de Sistemas de Información, tuvo como fin diagnosticar si las Unidades de Gestión Educativa Local actualmente tienen controles implementados concernientes a la Seguridad de la Información, así mismo determinar el perfil de seguridad de los activos de información de las unidades educativas. Además de revisar la documentación enmarcada en la R.M. Nº 004-2016-PCM, norma que regula la implementación de la NTP 27001 en todas las entidades que conforman el Sistema Nacional de Informática.

Además se analizó e interpretó datos mostrando gráficos, apoyado en la herramienta ofimática Microsoft Excel. Para tener una base sólida que permita proponer un modelo de Seguridad de la Información.

CAPÍTULO III RESULTADOS Y DISCUSIÓN

3.1. Diagnóstico del Sector

Se aplicó una encuesta basadas en la Norma ISO/IEC 27001:2013 de controles de seguridad de la información, al encargado del Centro de Sistemas de Información de cada Unidad, detalladas en el Anexo 9.
La encuesta tiene la finalidad de diagnosticar si las Unidades de Gestión Educativa Local actualmente tienen controles implementados respecto a la Seguridad de la Información desde el punto de vista del trabajador del Centro de Sistemas de Información, todo esto enmarcado bajo la resolución ministerial Nº 004-2016-PCM, norma que regula su implementación en todas las entidades que conforman del Sistema Nacional de Informática.

Al validar estadísticamente el instrumento, el coeficiente α propuesto por Cronbach con el fin de estimar la confiabilidad de una prueba, a partir de sumar muchas mediciones. Con el fin de la evaluación de confiabilidad u homogeneidad de los ítems, se emplea el coeficiente Alfa de Cronbach cuando existen categorías de respuestas propuestas en varias alternativas; motivo por el cual los valores asumidos serán entre 0 y 1, la confiabilidad nula es 0 y la representación de total confiabilidad equivale a 1.

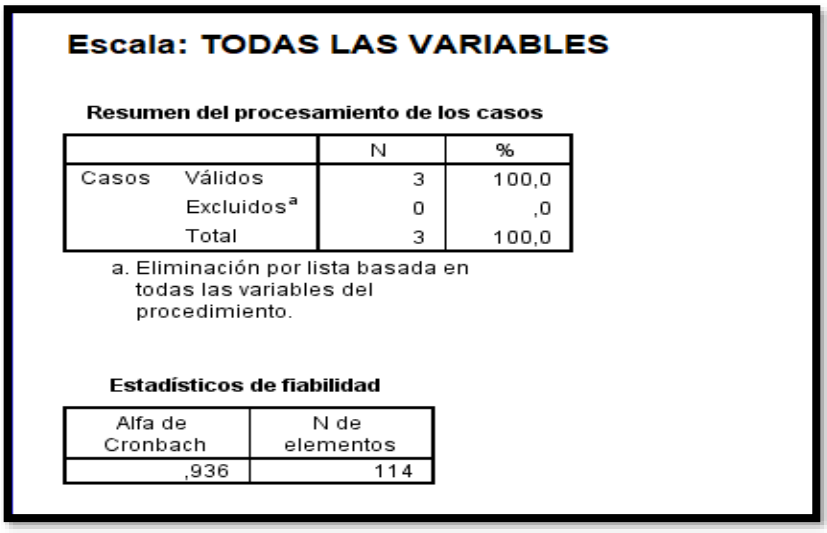
Tabla 1. Criterios que estiman nivel de confiabilidad.

CRITERIO	CONCLUSIÓN
0,53 a menos	Confiabilidad nula
0,54 a 0,59	Confiabilidad baja
0,60 a 0,65	Confiable
0,66 a 0,71	Muy Confiable
0,72 a 0,99	Excelente confiabilidad
1	Confiabilidad perfecta

Fuente: [45]

Aplicando el Alfa de Cronbach en las encuestas que se aplicaron a las Unidades de Gestión Educativa Local de Lambayeque se obtuvo esta confiabilidad.

Figura 19. Resultado de Alfa de Cronbach en SPSS.



Escala: TODAS LAS VARIABLES

Resumen del procesamiento de los casos

		N	%
Casos	Válidos	3	100,0
	Excluidos[a]	0	,0
	Total	3	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

Estadísticos de fiabilidad

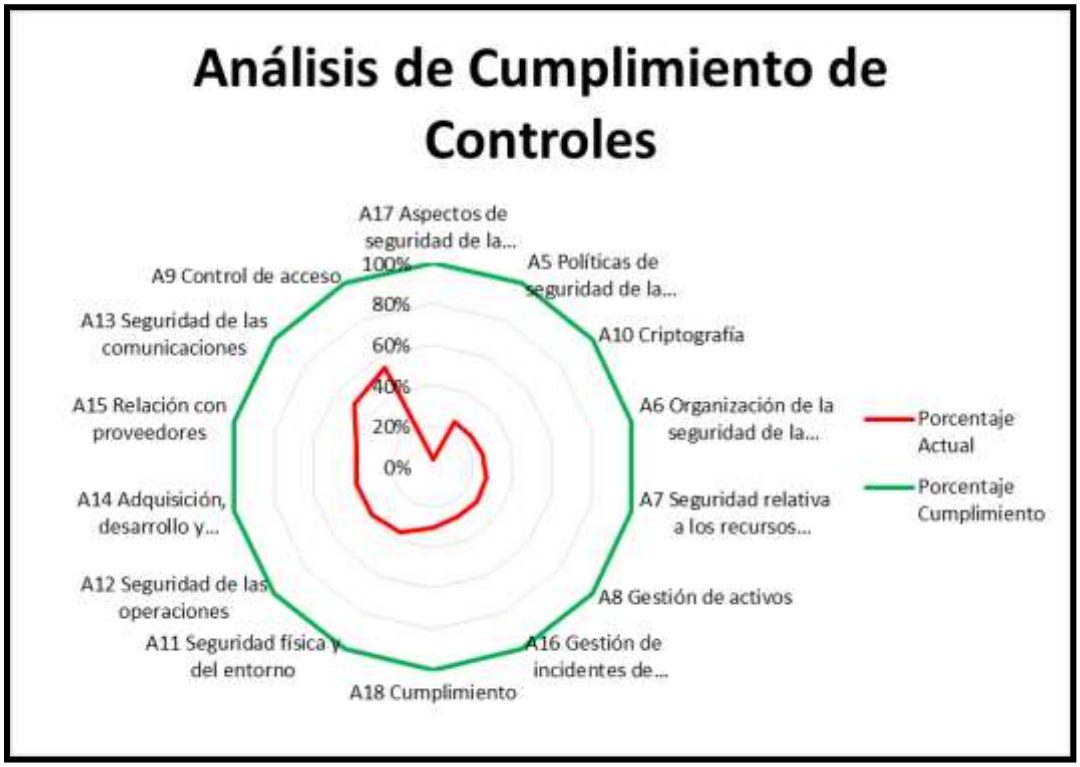
Alfa de Cronbach	N de elementos
,936	114

Fuente: Elaboración propia.

El resultado del análisis de la encuesta, a través de SPSS, indica que el nivel de coeficiente de confiabilidad obtenido es **EXCELENTE CONFIABILIDAD**.

Se aplicó una encuesta basada en la norma ISO 27002, para diagnosticar el estado actual de seguridad de información de las Unidades de Gestión Educativa Local de Lambayeque, Chiclayo y Ferreñafe. Una vez obtenido los porcentajes de cumplimiento en cada sección, se hizo un promedio de cumplimiento entre los resultados evaluados de las tres UGELES, donde el Porcentaje máximo de Cumplimiento es el 100% de la efectividad de todos los controles descritos en la ISO 27002.

Figura 20. Situación actual de Seguridad en las UGEL en Lambayeque.



Fuente: Elaboración propia

Como observamos en el Porcentaje actual de seguridad de la información, obtenido en promedio de las tres UGELES, para la gestión de la continuidad de negocio cumple al 4%, en Políticas de seguridad de la información un 24%, Criptografía un 24%, en Organización de la seguridad de la información al 25%, en Seguridad relativa a los recursos humanos al 27%, en Gestión de activos al 28%, Gestión de incidentes de seguridad de la información un 28%, en el análisis de cumplimiento un 30%, Seguridad física y del entorno un 36%, Seguridad de las operaciones un 38%, Adquisición, desarrollo y mantenimiento de los sistemas de información un 39%, Relación con proveedores 39%, Seguridad de las comunicaciones un 49% y en Control de acceso con 54%.

3.2. Análisis de estándares, marcos de trabajo y metodologías

El modelo propuesto se ha elaborado a partir del análisis de los estándares relacionados al Sistema de Gestión de Seguridad de la Información, como se puede apreciar en Anexo 3, los estándares son:

ISO 27005:2011, Gestión del riesgo de seguridad de la información.
NTP ISO 27001:2014, Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.
OCTAVE - S, Metodología para el análisis de riesgos de TI.
NIST SP 800-30, Método de análisis de riesgos.

Después de haber obtenido resultados producto de un profundo análisis, se describe los conceptos de la estructura del modelo de seguridad propuesto:

FASE I CONTEXTO DE LA ORGANIZACIÓN

Su objetivo es conocer la realidad actual de cada Unidad de gestión educativa, de esta manera comprender su organización. La fase está compuesta por las siguientes actividades:

I.1. Comprender la organización y su contexto, tomado de la ISO 27001, el propósito de esta actividad es identificar la estructura externa e interna de la institución, los factores que lo componen; además de determinar sus recursos y conocimientos reflejados en su misión y visión.

I.1.1. Contexto Externo, aspectos identificados en los factores legales, financieros, políticos y sociales.

- Factor Legal, son normas, directivas, resoluciones o lineamientos bajo los cuales trabajan las Unidades de Gestión Educativa Local, en el cual no cumplirlas puede llevar a futuras sanciones administrativas.

- Factor Financiero, instituciones que influyan económicamente en el rendimiento de las unidades educativas locales.
- Factor Político, instituciones que regulen el funcionamiento y bases de la institución.
- Factor Social, aspectos que tengan referencia con grupos de interés social relacionados con las unidades de gestión educativas.

I.1.2. Contexto Interno, aspecto identificado en el ámbito estructura de la organización, recursos, conocimientos, la visión y misión.

- Estructura de Organización, identificar la organización y jerarquía de la institución.
- Recursos y conocimientos, plataformas que son base para brindar soporte y rendimiento en las diversas operaciones de las unidades educativas para brindar la atención al usuario.
- La visión y misión, conocer la visión y misión definida por la misma institución.

I.2. Definir el alcance y los límites, para esta actividad basada en la NTP ISO 27005:2011 se recopilará información de la institución para ubicar los procesos asociados a los activos, identificar las partes interesadas y determinar la tecnología que interviene al procesar información, para ello se ha considerado:

- Ubicación, los procesos dónde se desenvuelven los activos a proteger.
- Partes interesadas, que contribuyen al desarrollo y propósito de la institución.
- Tecnología, dispositivos y aplicaciones que interactúan con el proceso de la información.
- Exclusiones, describir los controles que no serán considerados para el modelo de seguridad de la información, justificando el motivo de exclusión.

I.3. Análisis de brechas, en esta actividad se identificará el control, los requisitos que implica el control, para analizar la situación actual de los controles en la que se encuentra las Unidades de Gestión Educativa Local, respecto a la situación deseada según los requisitos que exigen los estándares ISO 27001 y NIST 800-53, además de asignar un responsable.

Para evaluar la situación actual y la esperada se hará uso de la escala de madurez.

0 No existe, la política de control no existe dentro de la institución.

1 Inicial, la institución reconoce que existen carencias de control y requieren ser resueltos.

2 Gestionado, existen actividades comunes pero no tienen procesos estandarizados.

3 Definido, existen procesos estandarizados y documentados en la institución.

4 Medible, los procesos estandarizados son monitoreados y medidos.

5 Optimizado, los procesos han alcanzado un nivel de mejor práctica y se enfocan en la mejora continua.

FASE II LIDERAZGO

Las jefaturas deben liderar la propuesta del SGSI, asumiendo el compromiso, proponiendo objetivos de seguridad que guarden relación con los activos de información financiera de las unidades educativas. La fase se compone de las actividades:

II.1. Liderazgo y compromiso, propuesta por la ISO 27001:2014, asegura que los altos ejecutivos deben expresar su compromiso y liderazgo frente a sistema de gestión de seguridad, de tal manera que asegure que las políticas y los objetivos de seguridad son compatibles con la dirección estratégica de la institución.

II.2. Lista de políticas y controles planificados, tiene como propósito la elaboración de un informe de políticas planificadas como resultado de la

situación deseada definido en el análisis de brechas. Se definen los objetivos para cada control asociados a los descritos en la ISO 27001 y NIST 800-53 Revisión 4, dichas políticas de seguridad de información deben ser aprobadas por la alta dirección y comunicados a todas las áreas de la Unidad de Gestión Educativa Local.

FASE III EVALUACIÓN DE RIESGOS

Esta fase tiene como propósito realizar la evaluación de riesgos que afecten a los activos de información financiera más relevantes para la institución, identificando las amenazas y vulnerabilidades por cada activo basándose en la ISO 27005. Además para en análisis de riesgos y plan de tratamiento se hará uso de la metodología OCTAVE – S.

III.1. Identificar los activos, la ISO 27005:2011 define al activo como el valor más importante dentro de una institución, por tal motivo requiere ser protegido. Para su identificación se recurre a una visión más allá del software y hardware. El fin para la actividad es la identificación de los activos más importantes para la institución que guarden relación con la información financiera.

III.2. Valoración de los activos, ISO 27005:2011, significa establecer una escalabilidad a utilizar, en base a criterios relacionados dentro de una ubicación en particular para cada uno de los activos de información financiera identificados. Para las unidades educativas, la valoración tiene base en el costo por pérdidas de:

- Confidencialidad (C), la información no está a disposición de cualquier individuo, entidades externas o procesos no autorizados.
- Integridad (I), el activo se mantiene con exactitud y completitud, además sus procesos no pueden ser alterados.

- Disponibilidad (D), acceder a los activos cuando sean necesitados por individuos, entidades o procesos autorizados.

Además tiene como criterios cualitativos Muy alto, Alto, Medio y Bajo.

III.3. Identificar las amenazas y las vulnerabilidades, Esta actividad se basa en la norma ISO 27005:2011. Toda amenaza puede provocar daños a los activos de información, de proceso o sistemas, siendo estas de origen natural o humano, accidental o provocado. Por lo que se recomienda determinar el origen de la amenaza, además de identificar las vulnerabilidades a fin de estimar la probabilidad de ocurrencia. De esta manera clasificarlas por ciertas características. [46]. Existen tipos de amenazas como D (deliberadas), A (accidentales) y E (ambientales). Las amenazas son valoradas según su probabilidad e impacto que ejerzan sobre los activos de información financiera de las unidades educativas.

III.4. Analizar los riesgos, propuesto por la fase 3 de la metodología OCTAVE-S, para el desarrollo de esta actividad se ha evaluado el impacto tomando en cuenta cuatro áreas:

- Reputación – confianza del cliente, tomando como variable la imagen de las unidades de gestión educativa local.
- Financiero, enfocando en la reducción de presupuesto no planificado.
- Productividad, basado en las interrupciones de los activos para realizar operaciones consideradas críticas.
- Fraude, se toma en consideración el cumplimiento de las normas, leyes, decretos o directivas dentro de UGEL.

Así mismo se evalúa la probabilidad de las amenazas sobre los activos de información medido en el transcurso de 4 años, considerando criterios como alto en el caso que ocurra más de una vez al año, medio si ocurre una vez cada 2 años y bajo si ha ocurrido una vez cada 4 años. Posteriormente se evalúa la matriz de impacto de probabilidad así también establecer criterios de evaluación de probabilidad.

El riesgo será obtenido del resultado de la probabilidad por el impacto, para posteriormente ubicarlos dentro de un mapa de riesgos. Según el resultado del valor del riesgo se identificará la tolerancia del mismo en un nivel "Aceptable" al recibir el riesgo sin oposición, "Tolera" permite el riesgo sin aprobarlo expresamente y "No Tolera" al no permitir el riesgo en la institución.

III.5. Desarrollar la estrategia de protección y plan de tratamiento, También descrito en la fase 3 de OCTAVE-S, en el desarrollo de esta actividad se ha definido una estrategia para proteger y tratar los riesgos. Además los procesos necesarios para poner práctica resultados de la evaluación. Así mismo para el tratamiento se ha considerado la tres tomas de decisiones: **Aceptar**, en el análisis de riesgo no se tomará a cabo ninguna acción para hacer frente al riesgo. **Mitigar**, en el análisis de riesgo se tomarán medidas para hacer frente al riesgo, implementando actividades para que la institución afronte la amenaza. **Aplazar**, en el análisis de riesgo no se acepta ni tampoco se mitiga para afrontar el riesgo, serán observados y evaluados en un futuro por la institución.

FASE IV IMPLEMENTACIÓN

La fase debe contar con un documento formal denominado Declaración de Aplicabilidad y debe estar aprobado por la alta dirección, estableciendo la siguiente actividad:

IV.1. Diseño de controles y procedimientos, tomando como referencia el numeral 8.1 de la ISO 27001:2014 nos indica que la institución debe:
Implementar acciones para el logro de los objetivos de seguridad de información, así también documentar cada procedimiento para corroborar que se han desarrollado como se había planificado. Para desarrollar estos procedimientos de controles se tomará en cuenta:

Quién debe realizar el control, qué es lo que debe implementar, cuándo debería realizarlo, dónde se implementará el control, por qué debería desarrollarse el control y cómo se corrobora el cumplimiento.

IV.2. Aplicar controles y procedimientos, luego de diseñar los procedimientos de los controles, estos deben ponerse en práctica dentro de la institución en un plazo establecido por responsable del procedimiento y las áreas involucradas.

FASE V COMUNICACIÓN Y EVALUACIÓN DEL DESEMPEÑO

Según la NTP ISO 27001:2014 esta fase de da por cumplida cuando la organización evalúa el cumplimiento del sistema de gestión de riesgo de seguridad de la información, comprobando el grado de cumplimiento de los objetivos propuestos. Para esta fase se desarrollará la siguiente actividad:

V.1. Comunicación, Tomada de la ISO 27001:2014, la constante participación de todas las áreas de las unidades educativas, es indispensable para informar respecto a cualquier incidente de riesgo ocurrido en la que pueda verse afectada a la institución, para ello el personal de las áreas interesadas deben entablar la constante comunicación y determinar qué desea comunicar, cuándo comunicar, a quién comunicar y quien debe comunicar.

V.2. Auditoría interna, La norma ISO 27001:2014 indica que la institución identifica, planifica y mantiene uno o muchos planes de auditoría, en los cuales debe considerar la inclusión de responsabilidades, determinar cuáles serán los requisitos, así como también el informe de planificación.

FASE VI MEJORAS

Basada en la fase 10 de la NTP ISO 27001:2014, para su desarrollo se empleará la siguiente actividad:

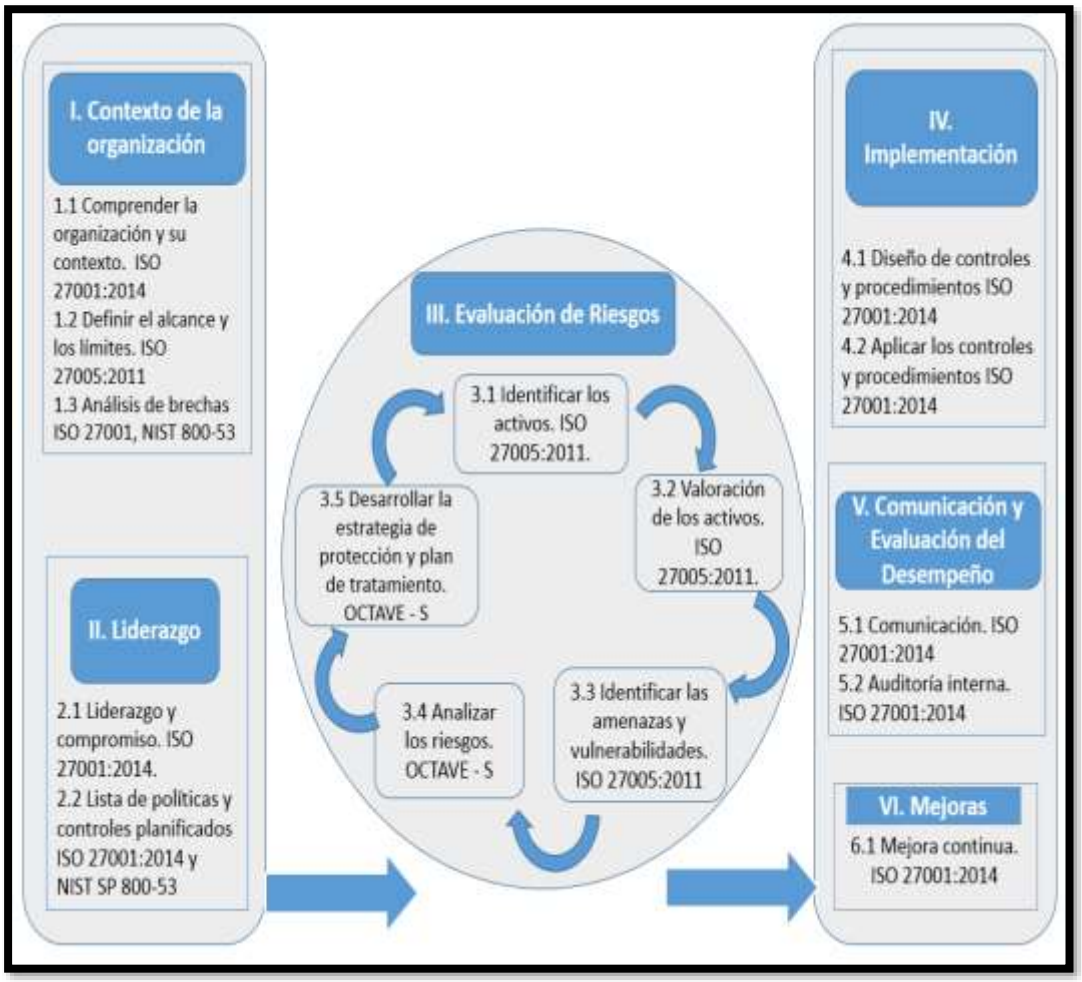
VI.1. Mejora continua, La norma ISO 27001:2014, propone que toda institución debe proponer mejoras en convivir, adecuar la efectividad del sistema de gestión de seguridad de la información.

3.3. Desarrollo del modelo propuesto

Tal como menciona la R.M. Nº 004-2016-PCM, la base tomada en cuenta para las fases que se han detallado es la ISO 27001:20014, complementadas con otros métodos con el fin de proponer plantillas adecuadas a las Unidades de gestión educativa local de la región Lambayeque.

En la figura 21, se muestra el modelo de seguridad propuesto, con las actividades detalladas que conforman cada fase.

Figura 21. Modelo propuesto para la seguridad de la información.



Fuente: Elaboración propia

FASE I CONTEXTO DE LA ORGANIZACIÓN

Esta fase identifica aspectos externos e internos relacionados con el rendimiento de las unidades de gestión educativa, además de conocer los límites y restricciones a nivel organizacional.

I.1. Comprender la organización y su contexto,

Su objetivo es identificar aspectos externos e internos relevantes que afecten la seguridad de la información en las unidades educativas. Cláusula 5.3 de ISO 31000:2009. Los aspectos se proponen en las siguientes tablas:

Tabla 2. Plantilla para identificar contexto externo.

FASE I - CONTEXTO DE LA ORGANIZACION **Formato Nº 01:** Comprender la organización y su contexto externo		
N°	**Ámbito**	**Aspectos identificados**
01	Factor legal	Normas legales o sanciones que al incumplirlas estén supeditadas a multas o sanciones administrativas.
.02	Factor Financiero	Indicar las organizaciones o dependencias que influyen en el presupuesto de las Unidades Educativas.
03	Factor Político	Especificar las instituciones que norman o regulan las gestiones de desempeño de las unidades educativas en la región Lambayeque.
04	Factor Social	Organizaciones de interés social con influencia a supervisar y monitorear el sector educación.

Fuente: Adaptado de [45]

Tabla 3. Plantilla para identificar contexto interno.

FASE I - CONTEXTO DE LA ORGANIZACION **Formato Nº 02:** Comprender la organización y su contexto interno		
N°	**Ámbito**	**Aspectos identificados**
01	Estructura de la organización	Actividades o tareas que la institución realiza, donde estructuren sus áreas para el logro del desempeño de funciones.
02	Recursos y conocimiento	Procedimientos de la administración pública y plataformas digitales que dan soporte a las operaciones de las unidades educativas de la región Lambayeque.
03	La visión y misión	La misión y visión institucional que permita alcanzar sus objetivos estratégicos.

Fuente: Adaptado de [45]

I.2. Definir el alcance y los límites

Su propósito es determinar la ubicación, elementos y tecnología que interactúan con los activos de información dentro de la unidad educativa. Para el desarrollo de esta actividad se toma en cuenta los factores externos e internos, complementados en la siguiente tabla:

Tabla 4. Plantilla para definir alcance y límites

FASE I - CONTEXTO DE LA ORGANIZACION **Formato Nº 03:** Definir el alcance y los límites	
Ubicación	Identificar las funciones donde se procesan los activos de información a proteger.
Partes interesadas	Indicar los interesados en el tratamiento de la información.
Tecnología	Dispositivos y plataformas que interactúan en la operatividad de la información.
Exclusiones	Identificar los controles de la ISO 27001 que no serán considerados por la naturaleza de la institución

Fuente: Adaptado de [45]

I.3. Análisis de brechas

Se comparará la situación actual de los controles con la situación deseada por parte de la institución, medidos por el nivel de madurez: no existe, inicial, gestionado, definido, medible y optimizado.

Tabla 5. Plantilla para Análisis de brechas

FASE I - CONTEXTO DE LA ORGANIZACION **Formato Nº 04:** Análisis de brechas					
Control	**Objetivo**	**Requisitos**	**Nivel Actual**	**Nivel deseado**	**Responsable y comentario**
Criptografía	Objetivo del control Criptográfico	Se debe implantar el uso seguro y efectivo de criptografía, para salvaguardar la autenticidad de los usuarios así como la integridad de información.	**1**	**3**	El coordinador de informática reconoce la problemática de la debilidad de contraseñas en los usuarios pero no cuenta con políticas de criptografía.
Control N	Objetivo del control N	Requisitos N	0	2	Responsable de control N

Fuente: Adaptado de [45]

FASE II LIDERAZGO

II.1. Liderazgo y compromiso, Se deben considerar las funciones de seguridad de información mínima establecidas en la ISO 27001:2014 durante el desarrollo de esta actividad.

Tabla 6. Plantilla para identificar liderazgo y compromiso.

FASE II - LIDERAZGO **Formato Nº 05:** Liderazgo y compromiso				
N°	**Funciones**	**SI**	**NO**	**PARCIAL**
01	¿Se asegura que la política y los objetivos de seguridad de la información sean establecidos y compatibles con la dirección estratégica de la organización?			
02	¿Se asegura la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización?			
03	¿Se asegura que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles?			
04	¿Se comunica la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información?			
05	¿Se asegura que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s)?			
06	¿Se dirige y apoya a las personas para que contribuyan con la efectividad del sistema de gestión de seguridad de la información?			
07	¿Se promueve la mejora continua?			
08	¿Se apoya otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad?			

Fuente: Adaptado de [45]

II.2. Lista de Políticas y controles planificados, tiene como propósito la elaboración de un informe de políticas planificadas como resultado de la situación deseada definido en el análisis de brechas, se propone la siguiente plantilla:

Tabla 7. Plantilla para informar políticas.

FASE II - LIDERAZGO **Formato Nº 06:** Establecer políticas y control de seguridad de información			
Nº	**Política**	**Objetivo**	**Aprobada por**
01	Seguridad de la Información	Debe brindar un direccionamiento y apoyar en la seguridad de la información tomando en cuenta las normativas que ejercen sobre las unidades de gestión educativas de Lambayeque.	Dirección de UGEL.
02	Seguridad de Recursos Humanos	Se debe asegurar que las personas contratadas comprendan sus funciones, acaten la responsabilidad de seguridad de información y la unidad de gestión educativa proteja los activos cuando culmine el contrato con el empleado.	Área de Recursos Humanos Dirección de UGEL.
03	Gestión de Activos	Se deben de identificar los activos de las Unidades de gestión educativas, con la finalidad de aplicar las protecciones apropiadas.	Dirección de UGEL.
04	Control de Acceso	Se debe delimitar todo tipo de accesibilidad a la información, procesos de suma importancia en las unidades de gestión educativa.	Dirección de UGEL.
05	Criptografía	Se debe implantar el uso seguro y efectivo de criptografía, para salvaguardar la autenticidad de	Dirección de UGEL.

		los usuarios así como la integridad de información.	
06	Seguridad de las operaciones	Se debe cuidar que los procesos de información sean correctos, así mismo proponer un respaldo respecto a la pérdida de la información	Dirección de UGEL.
07	Seguridad de las comunicaciones	Se debe mantener la seguridad respecto a la información cuando esta sea transferida internamente en la entidad, o compartida con otras instituciones.	Dirección de UGEL.
08	Relaciones con proveedores	Se debe proteger toda información de la Unidad de gestión educativa si requiere ser compartida con proveedores para el propósito del contrato.	Dirección de UGEL.
09	Seguridad de la información en la gestión de continuidad del negocio	Se debe priorizar la continuidad del proceso de la información con la finalidad que los compromisos que asume las unidades de gestión educativa se vean afectados.	Dirección de UGEL.
10	Política N	Objetivo de política N	Responsable de aprobar Política N

Fuente: Adaptado de [45]

FASE III EVALUACIÓN DE RIESGOS

En el desarrollo de esta fase se tomará en cuenta las consideraciones especificadas en el contexto externo e interno de la institución, con el fin de identificar los activos de información en las plantillas elaboradas, con el fin

de valorarlos e identificar los riesgos que puedan existir sobre ellos. Para esta actividad se realizarán las siguientes actividades:

III.1 Identificar los activos, Detallar la lista resumida de activos que se relacionen con información financiera, considerados relevantes para la Unidad de Gestión Educativa Local y que requieran ser protegidos. Para desarrollar la actividad tendremos en cuenta: descripción o nombre del activo, ubicación del activo, quien custodia el activo y el propietario del activo, según las plantillas mostradas:

Tabla 8. Plantilla para identificar activos hardware UGEL

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 07:** Identificar los Activos – Hardware de UGEL			
Descripción	**Ubicación**	**Custodio**	**Propietario**
Nombre del activo 1.	Ubicación activo 1	Custodio activo 1	Propietario activo 1
Nombre del activo 2.	Ubicación activo 2	Custodio activo 2	Propietario activo 2
Nombre del activo 3.	Ubicación activo 3	Custodio activo 3	Propietario activo 3
Nombre del activo N	Ubicación activo N	Custodio activo N	Propietario activo N
TOTAL			

Fuente: Elaboración propia

Tabla 9. Plantilla para identificar activos información financiera - Hardware

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 08:** Identificar los Activos – Hardware información financiera			
Descripción	**Ubicación**	**Custodio**	**Propietario**
Nombre del activo 1.	Ubicación activo 1	Custodio activo 1	Propietario activo 1
Nombre del activo 2.	Ubicación activo 2	Custodio activo 2	Propietario activo 2
Nombre del activo 3.	Ubicación activo 3	Custodio activo 3	Propietario activo 3
Nombre del activo N	Ubicación activo N	Custodio activo N	Propietario activo N
TOTAL			

Fuente: Elaboración propia

Tabla 10. Plantilla para identificar activo software instalado.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 09:** Identificar los Activos – Software instalado			
Tipo y nombre de Software	**Ubicación**	**Custodio**	**Propietario**
Sistemas Operativos	Ubicación activo 1	Custodio activo 1	Propietario activo 1
Ofimático	Ubicación activo 2	Custodio activo 2	Propietario activo 2
Herramientas Case	Ubicación activo 3	Custodio activo 3	Propietario activo 3
Software financiero	Ubicación activo 4	Custodio activo 4	Propietario activo 4
Repositorio de Datos	Ubicación activo 5	Custodio activo 5	Propietario activo 5
Otros a considerar por la UGEL	Ubicación activo N	Custodio activo N	Propietario activo N

Fuente: Elaboración propia

Tabla 11. Plantilla para identificar activos plataformas de trabajo.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 10:** Identificar los Activos – Plataformas de trabajo				
Descripción	**Funciones**	**Ubicación**	**Custodio**	**Propietario**
Nombre del activo 1.	Funciones de activo	Ubicación activo 1	Custodio activo 1	Propietario activo 1
Nombre del activo 2.	Funciones de activo	Ubicación activo 2	Custodio activo 2	Propietario activo 2
Nombre del activo 3.	Funciones de activo	Ubicación activo 3	Custodio activo 3	Propietario activo 3
Nombre del activo N	Funciones de activo	Ubicación activo N	Custodio activo N	Propietario activo N

Fuente: Adaptado de [45]

Tabla 12. Plantilla para identificar activos servicios financieros.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 11:** Identificar los Activos – servicios financieros			
Servicios	**Proceso**	**Custodio**	**Propietario**
Servicio 1	Detallar los procesos del servicio	Custodio activo 1	Propietario activo 1
Servicio 2	Detallar los procesos del servicio	Custodio activo 2	Propietario activo 2
Servicio 3	Detallar los procesos del servicio	Custodio activo 3	Propietario activo 3
Servicio N	Detallar los procesos del servicio	Custodio activo N	Propietario activo N

Fuente: Elaboración propia.

Tabla 13. Plantilla para identificar activos de información.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 12:** Identificar los Activos – activos de información de archivos físicos y lógicos			
Archivos Físicos			
Descripción	**Ubicación**	**Custodio**	**Propietario**
Activo 1	Ubicación del activo 1	Custodio activo 1	Propietario activo 1
Activo N	Ubicación del activo N	Custodio activo N	Propietario activo N
Archivos Lógicos			
Activo 1	Ubicación del activo 1	Custodio activo 1	Propietario activo 1
Activo N	Ubicación del activo N	Custodio activo N	Propietario activo N

Fuente: Elaboración propia.

III.2. Valoración de los activos, la institución asignará el valor a los activos más relevantes de su información financiera que puedan verse seriamente afectados teniendo en cuenta las dimensiones detalladas:

Tabla 14. Criterios para valorar activos.

Valor	Disponibilidad (D)	Integridad (I)	Confidencialidad (C)
4	La información, proceso, siempre debe estar disponible las 24 horas al día, la pérdida de ella supone la suspensión total de labores en UGEL.	Toda información debe mantenerse y garantizarse intacta, la pérdida de forma accidental o intencionada supone una catástrofe para la UGEL.	La información clasificada como privado, debe ser usada con una explícita autorización de la alta dirección de UGEL.
3	Información, proceso, en el cual su disponibilidad pueda verse afectada en un tiempo de 8 horas.	La información, proceso en el cual mantener la integridad supone una importancia y garantía para la UGEL.	El acceso a la información, proceso, considerado como confidencial es restringido, permitiendo ser utilizado solo a personal autorizado.
2	La información, proceso, que no pueda estar disponible en un máximo de 24 horas.	La integridad de la información, proceso, supone una importancia mediana para la UGEL.	La información, proceso, clasificado como interno, solo puede ser accedido por trabajadores del área correspondiente.
1	La información, proceso, cuya disponibilidad pueda no encontrarse accesible en un máximo de 48 horas.	Durante este nivel la información, proceso, no resulta tan importante para UGEL, sin embargo debe garantizarse.	En este nivel se refleja toda información, proceso, que puede ser accedido y utilizado solo por colaboradores internos de la UGEL.

Fuente: Elaboración propia.

Además la suma de dimensiones determinará el nivel de criticidad como Muy alto, Alto, Bajo, Muy Bajo:

Tabla 15. Valorar nivel de criticidad de activos.

Valor	Nivel
1 – 3	Muy Bajo
4 – 6	Bajo
7 – 9	Alto
10 – 12	Muy Alto

Fuente: Adaptado de [45]

Con los activos más relevantes identificados para las unidades educativas, determinamos el valor del activo según la Disponibilidad, Integridad y Confidencialidad.

Tabla 16. Plantilla para valorar activos de información financiera.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 13:** Valoración de activos						
Nº	Descripción del activo	Valor propio			Valor	Nivel
		D	I	C		
01	Pago movilidad y viático.	1	3	2	6	Bajo
02	Cierre mensual de estado financiero	4	2	1	7	Alto
03	Activo N	N	N	N	N	N

Fuente: Adaptado de [45]

III.3. Identificar las amenazas y vulnerabilidades, Esta actividad se presenta una relación de amenazas comunes propuestas por la ISO 27005, las cuales puede ser deliberadas (D), accidentales (A) y ambientales (E), Ellos deben seleccionarse según el activo relacionado.

Revisada la lista de amenazas, se identifica aquellas que incurran en los activos de información financiera más importantes para las unidades educativas.

Tabla 17. Plantilla para identificar amenazas de activos de información financiera.

FASE III – EVALUACIÓN DE RIESGOS **Formato 14:** Amenazas para activos financieros.			
Nº	**Activo**	**Amenazas**	**Vulnerabilidades**
01	Pago movilidad y viático.	Adulteración de archivo.	Vulnerabilidad 1
02	Cierre mensual de estado financiero	Falla del equipo de procesamiento.	Vulnerabilidad 2
03	Activo N	Amenaza N	Vulnerabilidad N

Fuente: Adaptado de [15]

III.4. Analizar los riesgos:

Evaluación de impacto, Para establecer criterios y evaluar el impacto de las amenazas sobre diferentes áreas de la institución, se han considerado las áreas que propone OCTAVE-S tales como:

a) **Reputación – Confianza del cliente,** nivel de afectación en la reputación de las unidades de gestión educativa local, los cuales al verse afectada puede no ser relevante para la institución (Bajo); recuperar la reputación requiere un poco de esfuerzo y gastos económicos (Medio); la reputación de la institución es irrevocablemente destruida (Alto).
b) **Financiero,** el nivel de impacto se ve reflejado en la pérdida financiera o reducción de presupuesto que afecte a la institución, cuando es menos del 10% (Bajo), si la afectación es del 11 al 50% (Medio) y si supera el 50% (Alto).
c) **Productividad,** se maneja en base a la interrupción de operatividad de los activos considerados críticos, si se ha visto interrumpida en 1 hora la jornada laboral (Bajo), si es hasta 3 horas (Medio), si supera la cantidad de 4 horas (Alto).
d) **Fraude,** se trabaja en base al cumplimiento regulatorio de las normas o decretos que se exija a UGEL; si el incumplimiento amerita una MEMO

de llamada de atención (Bajo): si es meritorio de una suspensión temporal o económica (Medio); si el incumplimiento merece la denuncia y separación definitiva de involucrados (Alto).

Tabla 18. Criterios de evaluación de impacto

Tipo de Impacto	**Bajo**	**Medio**	**Alto**
Reputación	1	2	3
Financiero	1	2	3
Productividad	1	2	3
Fraude	1	2	3

Fuente: Elaboración propia

Tabla 19. Plantilla para identificar el Impacto potencial de amenazas y vulnerabilidades.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 15:** Impacto potencial de amenazas y vulnerabilidades								
Nº	**Activo**	**Amenaza**	**Vulnerabilidad**	**Reputación**	**Financiero**	**Productividad**	**Fraude**	**Total**
01	Pago movilidad y viático	Adulteración de archivo.	Falta de protección física	1	2	3	1	7
02	Cierre EE.FF. mensual	Falla del equipo de procesamiento	No cuenta con planes de continuidad.	1	1	2	1	5
03	Activo N	Amenaza N	Vulnerabilidad N	N	N	N	N	N

Fuente: Adaptado de [47]

Evaluación de probabilidad, se han establecido medidas en probabilidad, tomando en cuenta la frecuencia con la que pueden ocurrir las amenazas sobre un activo de información financiera, tomando los siguientes valores de ocurrencia:

Tabla 20. Criterios de evaluación de probabilidad.

Probabilidad	Valor	Ocurrencia (días)
Bajo (B)	1	Una cada 4 años
Medio (M)	2	Una cada 2 años
Alto (A)	3	Ocurre mínimo una vez al año

Fuente: Elaboración propia.

Tabla 21. Probabilidad de Amenazas y vulnerabilidades.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 16:** Probabilidad de amenazas y vulnerabilidades					
Nº	**Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Total**
01	Pago movilidad y viático	Adulteración de archivo.	Falta de protección física	B	1
02	Cierre EE.FF. mensual	Falla del equipo de procesamiento	No cuenta con planes de continuidad.	M	2
03	Activo N	Amenaza N	N	N	N

Fuente: Adaptado de [47]

Matriz para el análisis del riesgo, para realizar el respectivo análisis del riesgo debemos hallar la magnitud del mismo, de esta manera calculamos:

Riesgo (R) = Total Impacto (I) * Total Probabilidad (P)

El mínimo valor que se obtiene del total del impacto multiplicado por la probabilidad es 4 y en máximo valor obtenido es 36, asignando los niveles de riesgo:

Tabla 22. Nivel de Riesgo.

Valor	Nivel de Riesgo
4 – 8	**Bajo**
9 – 18	**Medio**
19 – 36	**Alto**

Fuente: Adaptado de [15].

De esta manera podemos estimar el riesgo al cual conlleva que una amenaza se llegue a materializar bajo la siguiente plantilla:

Tabla 23. Plantilla para realizar el Análisis de Riesgo.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 17:** Análisis de Riesgo								
Nº	**Descripción del activo**	**Amenaza**	**Vulnerabilidad**	**I**	**P**	**R**	**Código Riesgo**	**Nivel Riesgo**
01	Pago movilidad y viático	Adulteración de archivo.	Falta de protección física	7	1	7	R1	Bajo
02	Cierre EE.FF. mensual	Falla del equipo de procesamiento	No cuenta con planes de continuidad.	5	2	10	R2	Medio
03	Activo N	Amenaza N		N	N	N	R (N)	N

Fuente: Adaptado de [45]

Se priorizará enfocar los riesgos identificados según sea su ubicación, obtenidas a partir del total de impacto identificado en la tabla 22 y total de probabilidad identificados en la tabla 24 en la siguiente matriz:

Tabla 24. Mapa de riesgos.

		TOTAL PROBABILIDAD		
		1	2	3
TOTAL IMPACTO	12	12	24	36
	11	11	22	33
	10	10	20	30
	9	9	18	27
	8	8	16	24
	7	7	14	21
	6	6	12	18
	5	5	10	15
	4	4	8	12

Fuente: Adaptado de [15].

Luego de priorizar los riesgos se determinarán la tolerancia respecto al riesgo de tal manera que:

Tabla 25. Nivel de Tolerancia al riesgo.

Valor	**Nivel de tolerancia**	**Motivo**
1 – 8	Aceptable	Se recibe el riesgo sin oposición o se transfiere.
9 – 18	Tolera	Se trata el riesgo mitigándolo.
19 – 36	No Tolera	El riesgo no se permite en la UGEL.

Fuente: Adaptado de [15].

Para asociar el nivel de tolerancia al riesgo, se hará uso de la siguiente plantilla:

Tabla 26. Plantilla para la evaluación del riesgo.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 18:** Evaluación de Riesgo						
Código Riesgo	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor I*P**	**Nivel Riesgo**	**Nivel Tolerancia**
R1	Pago movilidad y viático	Adulteración de archivo.	Falta de protección física	7	Bajo	Aceptable
R2	Cierre EE.FF. mensual	Falla del equipo de procesamiento	No cuenta con planes de continuidad.	10	Medio	Tolera
03	Activo N	Amenaza N	Vulnerabilidad N	N	N	N

Fuente: Adaptado de [15].

III.5. Desarrollar la estrategia de protección y plan de tratamiento

Para el desarrollo de esta actividad, la institución atenderá el nivel que considere primordial “Aceptable”, “Tolera” o “No Tolera”, para lo cual se determinará:

Tabla 27. Decisión para la estrategia de protección.

Decisión	Definición
Aceptar	No se tomará ninguna acción y la institución asumirá el riesgo.
Mitigar	Se tomarán medidas para hacer frente al riesgo analizado.
Aplazar	El riesgo analizado no se va afrontar ni tampoco aceptar, queda en observación para evaluación a futuro.
Transferir	El riesgo es de bajo impacto por lo tanto se transfiere.

Fuente: Adaptado de [47]

Una vez tomada la decisión se procederá a desarrollar la estrategia de protección mediante la siguiente plantilla:

Tabla 28. Plantilla para la Estrategia del Riesgo.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 19:** Estrategia de protección						
Cod. Riesgo	**Activo**	**Amenaza**	**Nivel Riesgo**	**Nivel Tolerancia**	**Decisión**	**Controles**
R1	Pago movilidad y viático	Adulteración de archivo.	Bajo	Aceptable	Mitigar	Control para la amenaza 1.
R2	Cierre EE.FF. mensual	Falla del equipo de procesamiento.	Medio	Tolera	Mitigar	Control para la amenaza 2.
RN	Activo N	Amenaza N	Nivel Riesgo N	Nivel Tolerancia N	Decisión N	Control para la amenaza identificada N.

Fuente: Adaptado de [45]

Finalmente se desarrolló un plan de mitigación para contrarrestar las amenazas identificadas, Se tomarán en cuenta las prácticas de seguridad propuestas por OCTAVE – S que se adapten al desarrollo del plan de seguridad haciendo uso de la siguiente plantilla:

Tabla 29. Plantilla para el Plan de Mitigación.

FASE III – EVALUACIÓN DE RIESGOS **Formato Nº 20:** Plan de Mitigación		
Área: Práctica de Seguridad.		
Actividades	**Justificación**	**Responsable**
Actividad 1	Razón de Actividad 1.	Responsables desarrollo de la mitigación 1.
Actividad 2	Razón de Actividad 2.	Responsables desarrollo de la mitigación 2.
Actividad N	Razón de Actividad N.	Responsables desarrollo de la mitigación N.

Fuente: Adaptado de [47]

FASE IV IMPLEMENTACIÓN

En esta fase debe implementarse el SGSI definiendo el diseño y aplicación de controles.

IV.1. Diseño de controles y procedimientos, en esta actividad se diseña la implementación de controles basado en la siguiente plantilla:

Tabla 30. Plantilla para Diseño de Procedimientos.

FASE IV – IMPLEMENTACIÓN **Formato Nº 21:** Informe documentado de diseño de procedimientos	
NOMBRE DEL PROCEDIMIENTO	Ejemplo: Procedimientos para creaciones de usuario.
Responsables del procedimiento	Nombre completo y cargo del o los responsables de elaborar el procedimiento.
Responsables de Aprobación	Nombre completo y cargo del o los responsables de aprobar el procedimiento antes propuesto.
Detalle de actividades del procedimiento	Actividades detalladas a realizar para el cumplimiento del procedimiento Actividad 1. Actividad N.
Controles	Listar los controles que soporten la implementación del procedimiento.
Responsables del control	Nombre completo y cargo del o los responsables de ejecutar el control
Frecuencia	Detallar la frecuencia del control.
Fecha de implementación	Fecha de cuándo se implementa el control.
Área de implementación	Dónde se va a implementar el control.
Cumplimiento del procedimiento	Documento o registro que compruebe la ejecución del control

Fuente: Adaptado de [15]

IV.2. Aplicar controles y procedimientos, la alta dirección debe asegurar la implementación los procedimientos y los controles previamente diseñados en la actividad anterior.

Tabla 31. Plantilla para Aplicar controles y procedimientos.

<table>
<tr><td colspan="3">FASE IV – IMPLEMENTACIÓN
Formato Nº 22: Informe de aplicación de controles.</td></tr>
<tr><td>NOMBRE DE PROCEDIMIENTO</td><td colspan="2">Ejemplo: Procedimientos para creaciones de usuario.</td></tr>
<tr><td>Involucrados de implementar procedimientos</td><td colspan="2">Nombres de responsables de implementar el procedimiento.

Áreas involucradas en la implementación del procedimiento.</td></tr>
<tr><td>Nombres del controles</td><td>Responsables del control</td><td>Estado</td></tr>
<tr><td>Control 1</td><td>Nombres del responsable del control 1</td><td>Implementado / No implementado</td></tr>
<tr><td>Control 2</td><td>Nombres del responsable del control 2</td><td>Implementado / No implementado</td></tr>
<tr><td>Control N</td><td>Nombres del responsable del control N</td><td>Implementado / No implementado</td></tr>
</table>

Fuente: Adaptado de [15]

FASE V COMUNICACIÓN Y EVALUACIÓN DEL DESEMPEÑO

En esta fase las unidades educativas evalúan el progreso y cumplimiento del SGSI.

V.1. Comunicación, es de suma importancia que todas las unidades orgánicas de las UGEL, participen con el fin de comunicar informaciones o incidentes que puedan ser relevantes al sistema de gestión de seguridad de la información:

Tabla 32. Plantilla para informe de evaluación.

FASE V – COMUNICACIÓN Y EVALUACIÓN DEL DESEMPEÑO **Formato Nº 23:** Informe de comunicación	
TIPO DE INFORME	Plan de Capacitación
Nombre y cargo	Nombre completo y cargo del responsable quien comunica.
Oficina	Área u oficina a quién comunica.
Fecha	Fecha de cuándo se comunica el Plan.
Detalle	Descripción relevante de lo que va a comunicar en relación a la seguridad dentro de la institución.
Documentos	Adjunta documentos probatorios.

Fuente: Adaptado de [15]

V.2. Auditoría interna, Establecer un predeterminado plan de auditoría interna aplicable dentro de la Institución, entrevistando a la alta gerencia y sus áreas. La actividad se desarrollará cumpliendo con la siguiente plantilla propuesta.

Tabla 33. Plantilla para auditoría interna.

FASE V – COMUNICACIÓN EVALUACIÓN DEL DESEMPEÑO **Formato Nº 24:** Auditoría interna					
Observación	**Causa**	**Recomendación**	**Comentario**	**Responsable**	**Estado**
Observación 1	Descripción de causa 1	Recomendación 1	Comentario 1	Responsable 1	Culminado / Pendiente
Observación 2	Descripción de causa 2	Recomendación 2	Comentario 2	Responsable 2	Culminado / Pendiente
Observación N	Descripción de causa N	Recomendación N	Comentario N	Responsable N	Culminado / Pendiente

Fuente: Adaptado de [45].

FASE VI MEJORAS

La efectividad en un sistema de gestión de seguridad de la información, no solo debe quedar en la implementación. Esta debe mejorar de forma continua, proponiendo la siguiente actividad:

VI.1. Mejora continua, en esta plantilla se tomarán en cuenta los controles de los riesgos que aún están en proceso de cumplir su objetivo, priorizándolos por complejidad o por urgencia.

Tabla 34. Plantilla para mejora continua.

FASE VI – MEJORAS **Formato Nº 25:** Mejora continua					
Nº	**Plan propuesto**	**Riesgo**	**Prioridad**	**Control**	**Inicio**
01	Nombre del plan 1	Riesgos plan 1.	Complejidad / urgencia	Controles propuestos para el riesgo 1.	Inicio: / /
02	Nombre del plan 2	Riesgos plan 2.	Complejidad / urgencia	Controles propuestos para el riesgo 2.	Inicio: / /
03	Nombre del plan N	Riesgos plan N.	Complejidad / urgencia	Controles propuestos para el riesgo N.	Inicio: / /

Fuente: Adaptado de [45].

3.4. Discusión

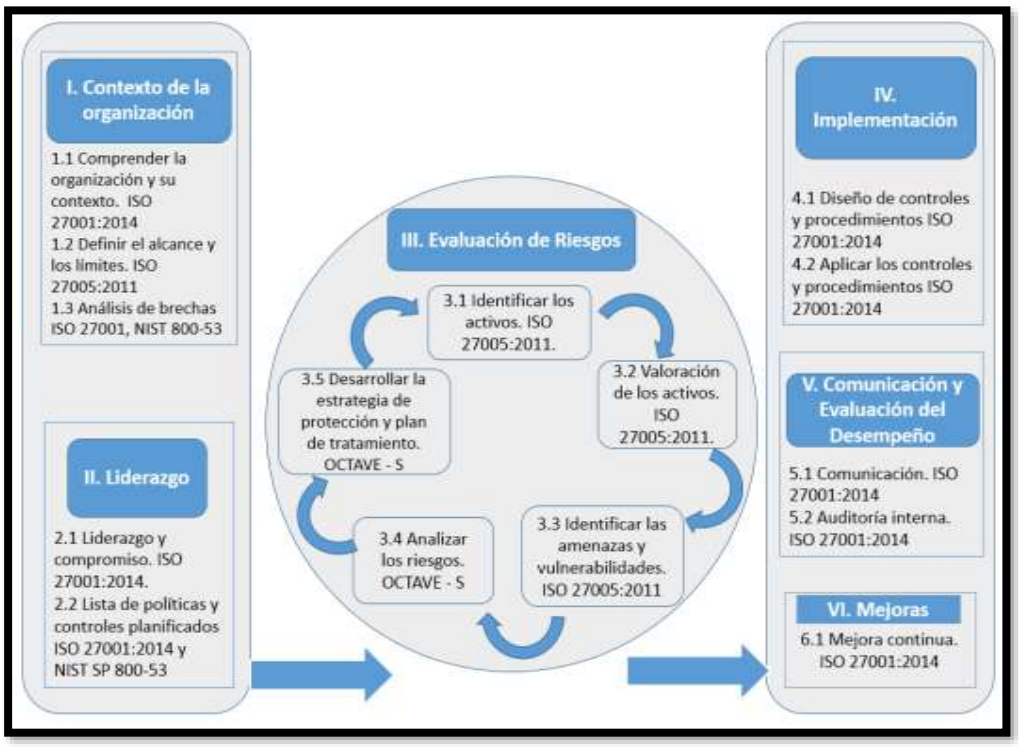
Demostrando la hipótesis planteada en este trabajo de investigación se evaluará:

3.4.1. Armonización de marcos de trabajo

Se consideraron identificar los estándares vinculados con la Seguridad de Información, una vez identificados los marcos tales como:

- NTP ISO/IEC 27001:2014
- ISO 27005:2011
- OCTAVE-S
- NIST SP 800-30

Posteriormente se realizó la comparación entre fases y actividades que propone cada marco de trabajo (Anexo 3), analizando sus similitudes y agrupando de acuerdo a las prioridades exigidas por la Unidades de Gestión Educativas Local en la región Lambayeque. Finalmente se propuso un modelo enfocado a la seguridad de la información, apoyado por los estándares especificados. Teniendo como propuesta:



3.4.2. Actividades enmarcadas en el ciclo PDCA o Deming

En el diagnóstico de la situación actual de las tres Unidades de Gestión Educativa Local de la Región Lambayeque reflejada en el Anexo 2 y Figura 20, se puede apreciar de manera global que las instituciones solo cumplen con un 32 % de los controles propuestos en el Anexo A de la ISO 27001.

El bajo cumplimiento de controles exige la necesidad de implementar un modelo de SGSI. La ISO 27001 utiliza como enfoque el ciclo PDCA (Plan, Do, Check, Act) o ciclo Deming, que consiste en planear, implementar, verificar y mejorar; motivo por el cual el modelo de seguridad propuesto, contiene actividades que abarcan dicho enfoque:

- Actividades para planear: Contenidas en la Fases I, II y III.
- Actividades para implementar: Contenidas en la Fase IV.
- Actividades para verificar: Contenidas en la Fase V.
- Actividades para mejorar: Contenidas en la Fase VI.

3.4.3. Nivel de aceptación de juicio experto

El propósito a nivel general en esta investigación es el de contribuir a la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque. Para alcanzar el objetivo principal, se ha validado el modelo con dos instrumentos:

a) El modelo propuesto fue evaluado por tres expertos en el área de investigación del SGSI, con el propósito de medir su confiablidad. Los resultados (Ver Anexo 7), fueron interpretados aplicando Alfa de Cronbach dando como resultado un 72 % en confiabilidad.

En la investigación de García Samamé S. [45], se han establecido rangos para definir el nivel de aceptación del Alfa de Cronbach que también emplearon para el Diagnóstico del Sector como podemos ver en la Tabla 1.

En consideración al valor obtenido que es de 0.72, se concluye que el instrumento tiene el coeficiente de Excelente confiabilidad.

b) Así mismo para hallar el nivel de concordancia de las evaluaciones se empleó el Coeficiente de concordancia de Kendall (W), usando los parámetros del método, sabiendo que el coeficiente tiende a variar entre 0 a 1, planteamos estas hipótesis:
La evaluación de expertos no tiene concordancia: H0 (W=0).
La evaluación de expertos tiene concordancia: H1 (W>0).

Mediante la herramienta SPSS se pudo constatar la concordancia de las evaluaciones dadas por los expertos, teniendo estos resultados:

Tabla 35. Coeficiente de Kendall

	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA
N	15	15	15	15
W	0.108	0.160	0.067	0.133
X^2	3.250	4.800	2.00	4.00
gl	2	2	2	2
p	0.197	0.091	0.368	0.135

Fuente: Elaboración propia

Tomando en cuenta los resultados de la Tabla 35, en cada criterio el valor de W es mayor que 0, motivo por el cual la hipótesis H0 se rechaza, concluyendo así que la evaluación de los expertos si tiene concordancia en los criterios de suficiencia, claridad, coherencia y relevancia.

CONCLUSIONES

1. Hasta la fecha del presente trabajo de investigación, las Unidades de Gestión Educativas Local de la región Lambayeque, abarcan solo el 32% de controles que propone la ISO 27001, los cuales fueron pre identificados antes de la propuesta del modelo de seguridad.

2. Se cumplió el objetivo trazado de proponer un modelo de seguridad de la información mediante la comparación y análisis de estándares internacionales y nacionales, tomando como referencia la NTP ISO 27001:2014, ISO 27005:2011, el método OCTAVE-S y NIST 800-30; todas ellas alineadas a mejorar la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local en la región Lambayeque.

3. El modelo de seguridad de la información propuesto, contiene etapas que se encuentran enmarcadas en el ciclo Deming, cumpliendo con el enfoque de Planear reflejadas en las Fases de Contexto de la organización, Liderazgo, Evaluación de riesgos; Implementar en la Fase de Implementación; verificar en la Fase de Comunicación y mejorar en la Fase de mejoras.

4. La evaluación del modelo fue realizada por profesionales expertos, teniendo como propósito medir la aplicabilidad en el sector de estudio, obteniendo resultados de su confiabilidad en un 72%, lo cual certifica que es válido para contribuir en la mejora de seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque.

REFERENCIAS BIBLIOGRÁFICAS

[1] INACAL, *Norma Técnica Peruana NTP-ISO/IEC 27002 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.*, 1a ed., Lima, 2017.

[2] World Economic Forum, «Informe de riesgos mundiales 14 edición,» Cologny/Ginebra, 2019.

[3] R. Gómez, D. H. Pérez, Y. Donoso y A. Herrera, «Metodología y gobierno de la gestión de riesgos de tecnologías de la información,» *Revista de ingeniería. Universidad de los Andes Bogotá*, p. 3, 2010.

[4] A. L. Gil, «Ciber Riesgos y Seguridad de la Información en América Latina & Caribe,» *Deloitte*, 2019.

[5] Presidencia del Consejo de Ministros y Oficina Nacional de Gobierno Electrónico, «Una mirada al Gobierno Electrónico en el Perú - La oportunidad de acercar el Estado a los ciudadanos a través de las TIC,» Lima, 2013.

[6] Gobierno Regional Lambayeque, *Resolución Ejecutiva Regional No. 240 - Normas sobre el presupuesto analítico de Personal en las dependencias del Gobierno Regional Lambayeque*, Lambayeque, 2010.

[7] I. Picón Carrascal, Elaboración de un plan de Implementación de la ISO/IEC 27001:2013, Colombia: Instituto colombiano para la evaluación de la educación - ICFES, 2016.

[8] I. Narváez, Aplicación de la norma ISO 27001 para la implementación de un SGSI en la Fiscalía General del Estado, Ecuador: Pontificia Universidad Católica del Ecuador, 2013.

[9] K. G. Bermúdez Molina y E. R. Bailón Sánchez, Análisis de seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información dirigido a una empresa de servicios financieros, Ecuador: Universidad Politécnica SALESIANA, 2015.

[10] J. A. Seclén Arana, Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001, Lima - Perú: Universidad Nacional Mayor de San Marcos, 2016.

[11] J. E. Mercado Rojas, Modelo de Gestión de Seguridad de la Información para el E-Gobierno, Lima - Perú: Universidad Nacional Mayor de San Marcos, 2016.

[12] A. Mory, Aplicación de la norma ISO/IEC 27001 para mejorar la seguridad de la información en la empresa HM Contratistas S.A., Ancash - Perú: Universidad Nacional Santiago Antúnez de Mayolo, 2014.

[13] E. K. Celi Arévalo, «Un modelo para la gestión de riesgos de TI en las empresas microfinancieras: caso Lambayeque, Perú,» Lambayeque - Perú, 2013.

[14] J. C. Alcántara Flores, Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos

de la comisaria del norte P.N.P en la ciudad de Chiclayo, Chiclayo: Universidad Católica Santo Toribio de Mogrovejo, 2015.

[15] F. B. Vásquez Velásquez y J. D. P. Alva Zapata, Modelo de Gestión de riesgos de ti para contribuir en la continuidad del negocio de las Microfinancieras de la región Lambayeque, Chiclayo - Perú: Universidad Católica Santo Toribio de Mogrovejo, 2018.

[16] M. I. Romero Castro y Otros, Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades, Alicante - España: Área de Innovación y Desarrollo, S.L., 2018.

[17] *La norma ISO 27001 Aspectos clave de su diseño e implementación,* ISOTools EXCELLENCE, 2013.

[18] P. Aguilera, Redes seguras (Seguridad Informática), Madrid - España: Editex, 2011.

[19] *Estándar Internacional ISO/IEC 27002:2013*, Organización Internacional de Normalización y Comisión Electrónica Internacional, 2013.

[20] *Norma ISO/IEC 27001:2013,* Organización Internacional de Normalización y Comisión Electrónica Internacional, 2013.

[21] Á. Gómez Vieites, Enciclopedia de la Seguridad Informática 2da Edición, Madrid - España: RA-MA S.A., 2011.

[22] A. Lavell, «Decison Making and Risk Management,» Facultad Latinoamericana de Ciencias Sociales, Secretaría General, 1998.

[23] «iso27000.es,» ISO 27000.ES, [En línea]. Available: https://www.iso27000.es/sgsi.html. [Último acceso: 14 Diciembre 2019].

[24] K. d. R. Gaona Vásquez, 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 - Ecuador: Universidad Politécnica Salesiana, 2013.

[25] «welivesecurity.com,» ESET, [En línea]. Available: https://www.welivesecurity.com/la-es/2015/03/23/evaluacion-de-riesgos-cualitativa-o-cuantitativa/. [Último acceso: 10 Diciembre 2019].

[26] F. G. Pacheco y H. Jara, Hackers al descubierto, Argentina: Gradi S.A., 2009.

[27] J. Lamprecht, ISO 9000 en la pequeña y mediana empresa, Madrid - España: AENOR, 1996.

[28] «normas-iso.com,» Normas ISO, [En línea]. Available: https://www.normas-iso.com/iso-27001/. [Último acceso: 10 Diciembre 2019].

[29] R. A. Caralli, J. F. Stevens, L. R. Young y W. R. Wilson, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Pensilvania - Estados Unidos: Carnegie Mellon, 2007.

[30] «ENISA,» European Union Agency For Cybersecurity, [En línea]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html. [Último acceso: 06 Abril 2020].

[31] «mehari.info,» CLUSIF, [En línea]. Available: http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-IntroduccionESP.pdf. [Último acceso: 10 Abril 2020].

[32] J. Santonja Lillo y J. V. Berná Martinez, Análisis y correlación entre probabilidad e impacto de los riesgos, Alicante - España: Universidad de Alicante, 2019.

[33] M. Á. Amutio Gómez, J. Candau y J. A. Mañas, MAGERIT - Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Madrid - España: Ministerio de Hacienda y Administraciones Públicas, 2012.

[34] G. Stoneburner y A. Feringa, Risk management guide for information technology systems :: recommendations of the National Institute of Standards and Technology, Gaithersburg - Estados Unidos: National Institute of Standards and Technology, 2002.

[35] A. Abril Estupiñan, J. Pulido y J. J. Bohada, Análisis de riesgos en seguridad de la información. Ciencia, Innovación y Tecnología, Colombia: Fundación Universitaria Juan Castellanos, 2013.

[36] «NIST Special Publication 800-53,» Abril 2013. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. [Último acceso: 12 Abril 2020].

[37] H. Alemán Novoa y C. Rodriguez Barrera, Metodologías para el análisis de riesgos en los sgsi, Colombia: Universidad Nacional Abierta y a Distancia, 2015.

[38] M. d. C. Crespo Rin, El análisis de Riesgos dentro de una Auditoría Informática: Pasos y posibles metodologías, Leganés - España: Universidad Carlos III de Madrid, 2013.

[39] *Norma Técnica Peruana NTP-ISO/IEC 27001:2014*, Lima - Perú: Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI, 2014.

[40] *Uso de la NTP ISO/IEC 27001:2014 en las Entidades Integrantes del Sistema Nacional de Informática*, Lima - Perú: Presidencia del Consejo de Ministros, 2016.

[41] «Unidad de Gestión Educativa Local Lambayeque,» Gobierno Regional de Lambayeque, [En línea]. Available: https://www.regionlambayeque.gob.pe/web/informacion-institucional?m1=3645&m2=3041&m3=19676&pass=MTY=. [Último acceso: 12 Abril 2020].

[42] «Unidad de Gestión Educativa Local Chiclayo,» Gobierno Regional de Lambayeque, [En línea]. Available: https://www.regionlambayeque.gob.pe/web/informacion-institucional?pass=MTU=. [Último acceso: 12 Abril 2020].

[43] «Unidad de Gestión Educativa Local Ferreñafe,» Gobierno Regional de Lambayeque, [En línea]. Available: https://www.regionlambayeque.gob.pe/web/informacion-institucional?m1=14508&pass=MTg=. [Último acceso: 12 Abril 2020].

[44] R. Hernández Sampieri, C. Fernández Collado y P. Baptista Lucio, Metodología de la Investigación 6a Edición, México D.F.: Mc Graw Hill Education, 2014.

[45] S. C. García Samamé, Modelo de Seguridad de la Información para contribuir en la gestión de las unidades ambientales de la región Lambayeque, Chiclayo: Universidad Católica Santo Toribio de Mogrovejo, 2018.

[46] *Norma Técnica Colombiana NTC-ISO 27005*, Colombia: Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC, 2011.

[47] S. Amador Donado, Gestión de riesgo con base en ISO 27005 adaptando OCTAVE-S, Popayán, Colombia: Universidad Internacional de la Rioja Máster universitario en Seguridad Informática, 2014.

[48] Instituto Nacional de Estándares y Tecnología, «National Institute of Standards and Technology,» 22 Enero 2015. [En línea]. Available: https://nvd.nist.gov/800-53/Rev4/impact/HIGH. [Último acceso: 10 Mayo 2020].

[49] «Acceso a la Información - Manual Organizaciones y Funciones,» Gobierno Regional de Lambayeque, [En línea]. Available: https://www.regionlambayeque.gob.pe/web/acceso-informacion?tinfo=A&grup_id=970503ADPORTAL&pass=Mg==. [Último acceso: 14 Abril 2020].

ANEXOS

ANEXO 1 DESCRIPCIÓN GENERAL DE LAS UNIDADES DE GESTIÓN EDUCATIVA LOCAL EN REGIÓN LAMBAYEQUE

	UNIDAD DE GESTIÓN EDUCATIVA LOCAL FERREÑAFE	UNIDAD DE GESTIÓN EDUCATIVA LOCAL CHICLAYO	UNIDAD DE GESTIÓN EDUCATIVA LOCAL LAMBAYEQUE
Sector	Educación	Educación	Educación
Razón Social	UGEL FERREÑAFE	UGEL CHICLAYO	UGEL LAMBAYEQUE
Fecha de Creación	02 de Setiembre del 2005	05 de Setiembre del 2005	08 de Setiembre del 2005
Dirección	Avenida Victor Raúl Haya De La Torre Nº200-Ferreñafe	Carretera panamericana norte 775 Chiclayo - Lambayeque	Prolongación 8 de Octubre Nº 230 - Lambayeque
Representante Legal	Mg. Gloria Elizabeth Jiménez Pérez	Mg. Ángel Agustín Salazar Piscoya	Mg. Edith Rossana Soriano Araujo
Teléfonos	074-286298	074 - 204215	283344 / 281320
Misión	Somos una instancia de ejecución descentralizada del Gobierno Regional que promueve y desarrolla los lineamientos de política educativa en las Instituciones Educativas locales, garantizando un servicio de calidad y equidad en atención a las necesidades educativas de la comunidad ferreñafana, contribuyendo al fortalecimiento del sistema democrático y desarrollo sostenible de la región.	La Unidad de Gestión Educativa Local de Chiclayo, es un sistema que forma personas capaces de alcanzar su realización ética, intelectual, artística, cultural, afectiva, física, espiritual y religiosa, para su desempeño en la vida, priorizando el trabajo y el libre ejercicio de su ciudadanía en armonía con su entorno y actitudes que le permitan afrontar con éxito los cambios sociales y del conocimiento.	Somos una Instancia de Gestión Educativa Descentralizada de la Gerencia Regional de Educación de Lambayeque, que promueve la formación de personas competentes para responder a las dinámicas del mundo actual, contribuimos a la construcción y difusión del conocimiento, apoyamos el desarrollo competitivo de la región y del país; impulsando el mejoramiento de la calidad de vida de las comunidades educativas.

	UNIDAD DE GESTIÓN EDUCATIVA LOCAL FERREÑAFE	UNIDAD DE GESTIÓN EDUCATIVA LOCAL CHICLAYO	UNIDAD DE GESTIÓN EDUCATIVA LOCAL LAMBAYEQUE
Visión	La UNIDAD DE GESTIÓN EDUCATIVA LOCAL FERREÑAFE es una Institución Pública eficiente y eficaz, con un sistema administrativo y organizacional moderno, que oferta un servicio de calidad y equidad a las Instituciones Educativas, elevando el desarrollo educativo local y regional, fortaleciendo la identidad e interculturalidad, la participación concertada y democrática insertada a la producción y al turismo, con práctica de valores.	Nuestra visión Educativa al 2019 es una institución con gestión pública, moderna, promotora y articuladora del desarrollo sostenible, principal proveedor de servicios públicos de calidad, para el bienestar de la población Lambayecana	Al año 2020 la Unidad de Gestión Educativa Local de Lambayeque es la Instancia descentralizada líder de la educación impulsa una sociedad educadora con participación y vigilancia de la sociedad civil; garantiza una educación integral, pertinente y de calidad; contribuye al desarrollo pleno de las personas a lo largo de su vida; desarrolla políticas educativas que aseguren en niños, niñas y jóvenes a la igualdad de oportunidades de acceso, permanencia y trato sin ninguna forma de discriminación.
Objetivos Estratégicos	A) Contribuir a la formulación, difusión y asesoramiento en la aplicación de la política y normatividad educativa local, regional y nacional; así como evaluar sus resultados y retroalimentar el sistema educativo. B) Elaborar, ejecutar y evaluar el proyecto educativo local (PEL) de su jurisdicción, articulado con el plan de desarrollo local concertado, con el proyecto educativo regional y nacional, como instrumento orientador de la gestión educativa local.	A) contribuir a la formulación, difusión y asesoramiento en la aplicación de la política y normatividad educativa local, regional y nacional; así como evaluar sus resultados y retroalimentar el sistema educativo. B) Elaborar, ejecutar y evaluar el proyecto educativo local (PEL) de su jurisdicción, articulado con el plan de desarrollo local concertado, con el proyecto educativo regional y nacional, como instrumento orientador de la gestión educativa local. C) Regular y supervisar la gestión pedagógica, administrativa e institucional de las instituciones y programas educativos de	A) Contribuir a la formulación, difusión y asesoramiento en la aplicación de la política y normatividad educativa local, regional y nacional; así como evaluar sus resultados y retroalimentar el sistema educativo. B) Elaborar, ejecutar y evaluar el proyecto educativo local (PEL) de su jurisdicción, articulado con el plan de desarrollo local concertado, con el proyecto educativo regional y nacional, como instrumento orientador de la gestión educativa local.

	UNIDAD DE GESTIÓN EDUCATIVA LOCAL FERREÑAFE	UNIDAD DE GESTIÓN EDUCATIVA LOCAL CHICLAYO	UNIDAD DE GESTIÓN EDUCATIVA LOCAL LAMBAYEQUE
	C) Regular y supervisar la gestión pedagógica, administrativa e institucional de las instituciones y programas educativos de educación básica regular, básica especial, básica alternativa, técnico – productivos y comunitarios bajo su jurisdicción, fortaleciendo su autonomía institucional. D) Prestar apoyo administrativo y logístico a las instituciones públicas de su jurisdicción. E) Asesorar en la formulación, ejecución y evaluación del presupuesto anual de las instituciones educativas.	educación básica regular, básica especial, básica alternativa, técnico – productivos y comunitarios bajo su jurisdicción, fortaleciendo su autonomía institucional. D) Prestar apoyo administrativo y logístico a las instituciones públicas de su jurisdicción. E) Asesorar en la formulación, ejecución y evaluación del presupuesto anual de las instituciones educativas.	C) Regular y supervisar la gestión pedagógica, administrativa e institucional de las instituciones y programas educativos de educación básica regular, básica especial, básica alternativa, técnico – productivos y comunitarios bajo su jurisdicción, fortaleciendo su autonomía institucional. D) Prestar apoyo administrativo y logístico a las instituciones públicas de su jurisdicción. E) Asesorar en la formulación, ejecución y evaluación del presupuesto anual de las instituciones educativas.
Centro de Sistemas de Información	a) Administrar el desarrollo informático y sistémico de la UGEL. b) Ejecutar normas para el uso adecuado de computadoras personales, periféricos, servicios y protección de la información generada por los diferentes sistemas de información en la Red Informática. c) Racionalizar la implementación y distribución de equipos de cómputo mediante criterios técnicos y según la productividad y necesidades de las	a) Administrar el desarrollo informático y sistémico de la UGEL. b) Ejecutar normas para el uso adecuado de computadoras personales, periféricos, servicios y protección de la información generada por los diferentes sistemas de información en la Red Informática. c) Racionalizar la implementación y distribución de equipos de cómputo mediante criterios técnicos y según la productividad y necesidades de las diferentes unidades orgánicas de la UGEL.	a) Administrar el desarrollo informático y sistémico de la UGEL. b) Ejecutar normas para el uso adecuado de computadoras personales, periféricos, servicios y protección de la información generada por los diferentes sistemas de información en la Red Informática. c) Racionalizar la implementación y distribución de equipos de cómputo mediante criterios técnicos y según la productividad y necesidades de las

	UNIDAD DE GESTIÓN EDUCATIVA LOCAL FERREÑAFE	UNIDAD DE GESTIÓN EDUCATIVA LOCAL CHICLAYO	UNIDAD DE GESTIÓN EDUCATIVA LOCAL LAMBAYEQUE
	diferentes unidades orgánicas de la UGEL. d) Asesorar en la adquisición de equipos de cómputo en función a los requerimientos de la Red Informática. e) Proponer la formulación y programación del presupuesto anual correspondiente al sistema de informática que permita su implementación, actualización y mantenimiento. f) Orientar, asesorar y capacitar al personal que hará uso de los sistemas informáticos, software operativo, software aplicativo y otros instalados.	d) Asesorar en la adquisición de equipos de cómputo en función a los requerimientos de la Red Informática. e) Proponer la formulación y programación del presupuesto anual correspondiente al sistema de informática que permita su implementación, actualización y mantenimiento.	diferentes unidades orgánicas de la UGEL. d) Asesorar en la adquisición de equipos de cómputo en función a los requerimientos de la Red Informática. e) Proponer la formulación y programación del presupuesto anual correspondiente al sistema de informática que permita su implementación, actualización y mantenimiento.

ANEXO 2

Análisis de cumplimiento de controles obtenidos de la encuesta basada en ISO 27001 aplicada a las 3 Unidades de Gestión Educativa Local de la región Lambayeque para el Diagnóstico del Sector

Ítem	Análisis de Cumplimiento de Controles	Porcentaje Actual	Porcentaje Ideal UGEL	Porcentaje Cumplimiento
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	4%	70%	100%
A5	Políticas de seguridad de la información	24%	70%	100%
A10	Criptografía	24%	70%	100%
A6	Organización de la seguridad de la información	25%	70%	100%
A7	Seguridad relativa a los recursos humanos	27%	70%	100%
A8	Gestión de activos	28%	70%	100%
A16	Gestión de incidentes de seguridad de la información	28%	70%	100%
A18	Cumplimiento	30%	70%	100%
A11	Seguridad física y del entorno	36%	70%	100%
A12	Seguridad de las operaciones	38%	70%	100%
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	39%	70%	100%
A15	Relación con proveedores	39%	70%	100%
A13	Seguridad de las comunicaciones	49%	70%	100%
A9	Control de acceso	54%	70%	100%
	Porcentaje Global de Cumplimiento de controles	**32%**		

ANEXO 3

Análisis de Estándares, Marcos de Trabajo, Metodología

ISO 27005:2011	NTP ISO IEC 27001:2014	OCTAVE-S	NIST SP 800	Modelo Propuesto
	FASE I - Alcance			
	FASE II – Referencias y normativas			
	FASE III – Términos y definiciones			
PASO I – Establecimiento del contexto	**FASEIV - Contexto de la organización**		**PASO I – Caracterización de los sistemas de información**	**FASE I – Contexto de la Organización**
	4.1 Entender la organización y su contexto.		1.1 Fronteras del sistema	1.1 Comprender la organización y su contexto. ISO 27001:2014
	4.2 Comprender las necesidades y expectativas de las partes interesadas.		1.2 Funciones del sistema	1.2 Definir el alcance y los límites. 27005:2011
1.1 Definir el alcance y los límites.	4.3 Determinación del alcance del sistema de gestión de la seguridad de la información.		1.3 Criticidad de datos y sistemas	1.3 Análisis de brechas. ISO 27001:2014 NIST 800
1.2 Desarrollar criterios de evaluación de riesgo, criterios de impacto, criterios de la aceptación del riesgo.	4.4 Sistema de gestión de seguridad de la información		1.4 Sensibilidad de datos y sistemas	
	FASE V – Liderazgo			**FASE II – Liderazgo**
	5.1 Liderazgo y compromiso.			2.1 Liderazgo y compromiso. ISO 27001:2014
	5.2 Política de seguridad.			2.2 Lista de políticas y controles planificados. ISO 27001:2014 NIST 800

1.3 Establecer y mantener las responsabilidades en la organización.	5.3 Roles, responsabilidades y autoridades organizacionales			
PASO II – Identificación del riesgo	**FASE VI – Planificación**	**FASE I – Construcción de perfiles de amenaza basado en activos**	**PASO II – Identificación de las Amenazas**	**FASE III – Evaluación de riesgos**
2.1 Identificar los activos 2.2 Identificar las amenazas 2.3 Identificar los controles existentes 2.4 Identificar vulnerabilidades y consecuencias		1.1 Establecimiento de Criterios de Evaluación de Impacto. 1.2 Identificación de Activos de información. 1.3 Evaluación de Procedimientos de Seguridad organizacional 1.4 Selección de Activos Críticos 1.5 Identificación de los requisitos de seguridad para los activos críticos 1.6 Identificación de las amenazas a los activos críticos	2.1 Definición de amenazas potenciales	3.1 Identificar los activos. ISO. 27005:2011 3.2 Valoración de los activos. ISO 27005:2011 3.3 Identificar las amenazas y vulnerabilidades. ISO 27005:2011
		FASE II – Identificación de las vulnerabilidades de la infraestructura	**PASO III – Identificación de las vulnerabilidades**	
		2.1 Análisis de vías de acceso. 2.2 Análisis de los procesos tecnológicos relacionados	3.1 Lista de vulnerabilidades potenciales	
PASO III – Estimación del riesgo		**FASE III – Desarrollo de estrategia y planes de seguridad**	**PASO IV – Análisis de controles establecidos**	
3.1 Estimación cualitativa 3.2 Análisis cuantitativo	6.1 Acciones para tratar los riesgos y las oportunidades. 6.2 Objetivos de seguridad de la información y planificación para	3.1 Evaluación de los impactos de las amenazas 3.2 Establecimiento de criterios de evaluación de probabilidad	4.1 Lista de controles actuales y planificados	3.4 Analizar los riesgos. OCTAVE –S 3.5 Desarrollar la estrategia de protección y plan de tratamiento. OCTAVE - S

	conseguirlos.			
PASO IV – Evaluación del riesgo			**PASO V – Determinación de las probabilidades**	
4.1 Comparar niveles de riesgo frente a criterios para evaluación del riesgo 4.2 Criterios de aceptación		3.3 Evaluación de probabilidades de amenazas	5.1 Clasificación de las probabilidades	
	FASE VII – Soporte		**PASO VI – Análisis del impacto**	**FASE IV – Implementación**
	7.1 Recursos.	3.4 Cálculo del valor del riesgo	6.1 Pérdida de integridad	4.1 Diseño de controles y procedimientos. ISO 27001:2014
	7.2 Competencia.		6.2 Pérdida disponibilidad	
	7.3 Concientización			
	7.4 Comunicación		6.3Pérdida de confidencialidad	
	7.5 Información documentada			4.2 Aplicar los controles y procedimientos. ISO 27001:2014
PASO V - Tratamiento del riesgo	**FASE VIII - Operación**		**PASO VII – Determinar riesgo**	
3.1 Reducción del riesgo	8.1 Planificación y control operacional.	3.5 Selección planteamiento de mitigación	7.1 Riesgos y niveles de riesgo	
3.2 Retención del riesgo				
3.3 Evitación del riesgo	8.2 Evaluación de riesgos de seguridad de la información.			
3.4 Transferencia del riesgo	8.3 Tratamiento de riesgos de seguridad de la información.	3.6 Desarrollo de planes de mitigación del riesgo		
PASO VI - Aceptación del riesgo				
PASO VII – Monitoreo del riesgo	**FASE IX - Evaluación del desempeño**		**PASO VIII – Recomendación de**	**FASE V – Comunicación y Evaluación del Desempeño**

			controles adicionales	
5.1 Monitoreo y revisión de los factores de riesgo. 5.2 Monitoreo, revisión y mejora de la gestión del riesgo.	9.1 Monitoreo, medición, análisis y evaluación.		8.1 Controles recomendados	5.1 Comunicación. ISO 27001:2014
			PASO IX – Documentación de los resultados	
	9.2 Auditoría interna 9.3 Revisión por la gerencia.		9.1 Informe de evaluación de riesgo que se presenta a la alta dirección	5.2 Auditoría interna. ISO 27001:2014
	FASE X – Mejoras			**FASE VI – Mejoras**
	10.1 No conformidades y acción correctivas.			6.1 Mejora continua ISO 27001:2014
	10.2 Mejora continua.			

ANEXO 4

Relación de controles propuestos por NIST y Controles de la ISO 27001

Tabla 36. Controles propuestos por NIST 800-53 Rev. 4

No.	**Control**
AC-1	Política y procedimientos de control de acceso
AC-2	Administración de cuentas
AC-3	Aplicación de acceso
AC-4	Cumplimiento de flujo de información
AC-5	Separación de tareas
AC-6	Privilegios mínimos
AC-7	Intentos de inicio de sesión exitosos
AC-8	Notificación de uso del sistema
AC-10	Control de sesiones concurrentes
AC-11	Bloqueo de sesión
AC-12	Terminación de la sesión
AC-14	Acciones permitidas sin identificación o autenticación
AC-17	Acceso remoto
AC-18	Acceso inalámbrico
AC-19	Control de acceso para dispositivos móviles
AC-20	Uso de sistemas de información externa
AC-21	El intercambio de información
AC-22	Contenido públicamente accesible
A LA 1	Política y procedimientos de concientización y formación de seguridad
A LAS 2	Entrenamiento de seguridad
A LAS 3	Entrenamiento de seguridad basado en roles
A LAS 4	Registros de entrenamiento de seguridad
AU-1	Política y procedimientos de auditoría y responsabilidad
AU-2	Eventos de auditoría
AU-3	Contenido de los registros de auditoría
AU-4	Auditoría capacidad de almacenamiento
AU-5	Respuesta a fallas de proceso de auditoría
AU-6	Revisión de auditoría, análisis e informes
AU-7	Reducción de auditoría y generación de informes
AU-8	Sellos de tiempo
AU-9	Protección de información de auditoría
AU-10	No repudiación
AU-11	Retención de registro de auditoría
AU-12	Generación de auditoría
CA-1	Política y procedimientos de evaluación y autorización de seguridad

CA-2	Evaluaciones de seguridad
CA-3	Interconexiones del sistema
CA-5	Plan de acción e hitos
CA-6	Autorización de seguridad
CA-7	Monitoreo continuo
CA-8	Pruebas de penetración
CA-9	Conexiones de sistema interno
CM-1	Política y procedimientos de gestión de configuración
CM-2	Configuración de base
CM-3	Control de cambio de configuración
CM-4	Análisis de impacto de seguridad
CM-5	Restricciones de acceso para el cambio
CM-6	Ajustes de configuración
CM-7	Menos funcionalidad
CM-8	Inventario de componentes del sistema de información
CM-9	Plan de gestión de configuración
CM-10	Restricciones de uso del software
CM-11	Software instalado por el usuario
CP-1	Política y procedimientos de planificación de contingencia
CP-2	Plan de contingencia
CP-3	Formación de contingencia
CP-4	Prueba de plan de contingencia
CP-6	Sitio de almacenamiento alterno
CP-7	Sitio de procesamiento alterno
CP-8	Servicios de telecomunicaciones
CP-9	Respaldo del sistema de información
CP-10	Recuperación y reconstitución del sistema de información
IA-1	Política y procedimientos de identificación y autenticación
IA-2	Identificación y autenticación (usuarios organizativos)
IA-3	Identificación y autenticación del dispositivo
IA-4	Gestión de identificador
IA-5	Gestión de autenticadores
IA-6	Comentarios del autenticador
IA-7	Autenticación del módulo criptográfico
IA-8	Identificación y autenticación (usuarios no organizativos)
IR-1	Política y procedimientos de respuesta a incidentes
IR-2	Entrenamiento de respuesta a incidentes
IR-3	Prueba de respuesta a incidentes
IR-4	Manejo de incidentes
IR-5	Monitoreo de incidentes
IR-6	Informe de incidentes
IR-7	Asistencia de respuesta a incidentes

IR-8	Plan de respuesta a incidentes
MA-1	Política y procedimientos de mantenimiento del sistema
MA-2	Mantenimiento controlado
MA-3	Herramientas de mantenimiento
MA-4	Mantenimiento no local
MA-5	Personal de mantenimiento
MA-6	Mantenimiento a tiempo
MP-1	Política y procedimientos de protección de medios
MP-2	Acceso a medios
MP-3	Marcado de medios
MP-4	Almacén de datos
MP-5	Transporte de medios
MP-6	Saneamiento de medios
MP-7	Uso de medios
PE-1	Política y procedimientos de protección física y ambiental
PE-2	Autorizaciones de acceso físico
PE-3	Control de acceso físico
PE-4	Control de acceso para medio de transmisión
PE-5	Control de acceso para dispositivos de salida
PE-6	Seguimiento del acceso físico
PE-8	Registros de acceso del visitante
PE-9	Equipo de energía y cableado
PE-10	Cierre de emergencia
PE-11	Poder de emergencia
PE-12	Iluminación de emergencia
PE-13	Protección contra incendios
PE-14	Controles de temperatura y humedad
PE-15	Protección contra daños al agua
PE-16	Entrega y retiro
PE-17	Sitio de trabajo alterno
PE-18	Ubicación de los componentes del sistema de información
PL-1	Política y procedimientos de planificación de seguridad
PL-2	Plan de seguridad del sistema
PL-4	Reglas de comportamiento
PL-8	Arquitectura de seguridad de la información
PS-1	Política y procedimientos de seguridad del personal
PS-2	Posición designación de riesgo
PS-3	Examen del personal
PS-4	Terminación de personal
PS-5	Transferencia de personal
PS-6	Acuerdos de acceso
PS-7	Seguridad del personal de terceros

PS-8	Sanciones al personal
RA-1	Política y procedimientos de evaluación de riesgos
RA-2	Categorización de seguridad
RA-3	Evaluación de riesgos
RA-5	Escaneo de vulnerabilidad
SA-1	Política y procedimientos de adquisición de sistemas y servicios
SA-2	Asignación de recursos
SA-3	Ciclo de vida de desarrollo de sistemas
SA-4	Proceso de adquisición
SA-5	Documentación del sistema de información
SA-8	Principios de ingeniería de seguridad
SA-9	Servicios de sistema de información externa
SA-10	Gestión de configuración de desarrollador
SA-11	Evaluación y pruebas de seguridad para desarrolladores
SA-12	Protección de cadena de suministro
SA-15	Proceso de desarrollo, normas y herramientas
SA-16	Entrenamiento proporcionado por el desarrollador
SA-17	Desarrollador seguridad arquitectura y diseño
SC-1	Política y procedimientos de protección de sistemas y comunicaciones
SC-2	Aplicación particionamiento
SC-3	Aislamiento de la función de seguridad
SC-4	Información en recursos compartidos
SC-5	Negación de protección de servicio
SC-7	Protección límite
SC-8	Confidencialidad e integridad de la transmisión
SC-10	Desconexión de red
SC-12	Establecimiento y gestión clave criptográfica
SC-13	Protección criptográfica
SC-15	Dispositivos de computación colaborativos
SC-17	Certificados de infraestructura clave pública
SC-18	Código móvil
SC-19	Voz sobre protocolo de internet
SC-20	Nombre seguro / dirección servicio de resolución (fuente autoritativa)
SC-21	Nombre seguro / dirección servicio de resolución (resolver recursivo o caching)
SC-22	Arquitectura y provisión de nombre / dirección servicio de resolución
SC-23	Autenticidad de la sesión
SC-24	Fallo en estado conocido
SC-28	Protección de información en descanso
SC-39	Aislamiento de proceso
SI-1	Política y procedimientos de integridad del sistema e información
SI-2	Remediación de defectos
SI-3	Protección de código malicioso
SI-4	Seguimiento del sistema de información

SI-5	Alertas, avisos y directivas de seguridad
SI-6	Verificación de funciones de seguridad
SI-7	Software, firmware e integridad de la información
SI-8	Protección contra el spam
SI-10	Validación de entrada de información
SI-11	Manejo de errores
SI-12	Manejo y retención de información
SI-16	Protección de memoria

Fuente: [48]

Tabla 37. Controles propuestos por ISO 27001:2014.

Sección	**Control**
A5	Políticas de seguridad de la información.
A6	Organización de la seguridad de la información.
A7	Seguridad relativa a los recursos humanos.
A8	Gestión de activos.
A9	Control de acceso.
A10	Criptografía.
A11	Seguridad física y del entorno.
A12	Seguridad de las operaciones.
A13	Seguridad de las comunicaciones.
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información.
A15	Relación con proveedores.
A16	Gestión de incidentes de seguridad de la información.
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio.
A18	Cumplimiento.

Fuente: [39]

Relación de amenazas comunes propuestas por ISO 27005

Tabla 38. Ejemplos de amenazas comunes ISO 27005

Tipo	Amenazas	Origen
Daño físico	Fuego	A,D,E
	Daño por agua	A,D,E
	Contaminación	A,D,E
	Accidente importante	A,D,E
	Destrucción del equipo o los medios	A,D,E
	Polvo, corrosión, congelamiento	A,D,E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A,D,E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A,D,E
	Radiación térmica	A,D,E
	Impulsos electromagnéticos	A,D,E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha subrepticia	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D

	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A,D,E

Fuente: [46]

ANEXO 5
FORMATO PARA LA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado ingeniero, por medio del presente documento me dirijo a su digna persona para solicitar su colaboración con respecto a la validación de la propuesta de investigación titulada "Modelo de Seguridad de la Información para contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque". En el cual se tomó como marco de referencias las normas ISO 27001, OCTAVE – S, NIST 800, ISO 27005. Presentando cuestionario de validación y agradeciendo su importante colaboración.

Apellidos y Nombres: _____
Formación Académica: _____
Área experiencia laboral: _____
Tiempo de experiencia: _____
Institución: _____
Cargo actual: _____

Objetivo de la investigación: Contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de la región Lambayeque.

Objetivo del juicio de expertos: Comprobar la validez del modelo propuesto en relación a suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba: Determinar la utilidad de las plantillas propuestas en las Unidades de Gestión Educativa Local de Lambayeque.

De acuerdo a los siguientes criterios, califique cada una de las categorías.

La categoría de calificación se basa de la siguiente manera:

1) CATEGORIA	2) CALIFICACIÓN	3) Criterio
4) 5) SUFICIENCIA	6) Valoración se dará del 1 al 5 7) 1. Total desacuerdo 8) 2. Desacuerdo 9) 3. Regular 10) 4. De acuerdo 11) 5. Totalmente de acuerdo	12) La cantidad y calidad de los elementos presentados en el contenido son suficientes.
13) 14) CLARIDAD	15) Valoración se dará del 1 al 5 16) 1. Total desacuerdo 17) 2. Desacuerdo 18) 3. Regular 19) 4. De acuerdo 20) 5. Totalmente de acuerdo	21) El contenido se presenta utilizando un lenguaje apropiado que facilita su comprensión. 22)
23) 24) COHERENCIA	25) Valoración se dará del 1 al 5 26) 1. Total desacuerdo 27) 2. Desacuerdo 28) 3. Regular 29) 4. De acuerdo 30) 5. Totalmente de acuerdo	31) Existe una correspondencia lógica entre el contenido presentado y la teoría.
32) 33) RELEVANCIA	34) Valoración se dará del 1 al 5 35) 1. Total desacuerdo 36) 2. Desacuerdo 37) 3. Regular 38) 4. De acuerdo 39) 5. Totalmente de acuerdo	40) El contenido presentado es importante y determinante para lograr el entendimiento del tema.

MATRIZ DE CONSISTENCIA PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN FINANCIERA EN LAS UNIDADES DE GESTIÓN EDUCATIVA LOCAL DE FERREÑAFE						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**COMENTARIO**
I. Contexto de la organización	Comprender la organización y su contexto.					
	Definir el alcance y los límites.					
	Análisis de brechas					
II. Liderazgo	Liderazgo y compromiso.					
	Lista de Políticas y controles planificados.					
III. Evaluación de Riesgos	Identificar los activos.					
	Valoración de los activos.					
	Identificar las amenazas y vulnerabilidades					
	Analizar los riesgos					
	Desarrollar la estrategia de protección y plan de tratamiento					

IV. Implementación	Diseño de controles y procedimientos					
	Aplicar controles y procedimientos					
V. Comunicación y Evaluación del desempeño	Comunicación					
	Auditoría interna					
VI. Mejoras	Mejora continua					
TOTAL						

RESULTADOS

Opinión:

	FAVORABLE		**DEBE MEJORAR**		**DESFAVORABLE**

Firma:

_____

ANEXO 6

EVALUACIÓN DEL MODELO POR JUICIO DE EXPERTOS

EXPERTO 1

EVALUACIÓN DE JUICIO EXPERO

INDICADOR DE CALIFICACIÓN DE JUICIO EXPERTO

Estimado ingeniero:

Por medio del presente documento me dirijo a su digna persona para solicitar su colaboración con respecto a la validación de la propuesta de investigación titulada "Modelo de Seguridad de la Información para contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque". En el cual se tomó como marco de referencias las normas ISO 27001, OCTAVE – S, NIST 800, ISO 27005. Presentando cuestionario de validación y agradeciendo su importante colaboración.

Apellidos y Nombres	: Galán Santisteban, Juan Rafael
Formación Académica	: Ing. en Computación e Informática (MBA)
Área experiencia laboral	: Gestión de Tecnologías de la Información
Tiempo de experiencia	: 18 Años
Institución	: Gobierno Regional Lambayeque Contraloría General de la República
Cargo actual	: Analista de Sistemas Informáticos

Objetivo de la investigación	: Contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de la región Lambayeque.
Objetivo del juicio de expertos	: Comprobar la validez del modelo propuesto en relación a suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	: Determinar la utilidad de las plantillas propuestas en las Unidades de Gestión Educativa Local de Lambayeque.

MATRIZ DE CONSISTENCIA PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN FINANCIERA EN LAS UNIDADES DE GESTIÓN EDUCATIVA LOCAL DE FERREÑAFE						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**COMENTARIO**
I. Contexto de la organización	Comprender la organización y su contexto.	4	4	4	5	
	Definir el alcance y los límites.	4	4	4	4	
	Análisis de brechas	4	4	4	5	
II. Liderazgo	Liderazgo y compromiso.	5	4	4	4	
	Lista de Políticas y controles planificados.	5	4	5	4	
III. Evaluación de Riesgos	Identificar los activos.	4	4	4	4	
	Valoración de los activos.	4	5	4	4	
	Identificar las amenazas y vulnerabilidades	4	4	4	4	
	Analizar los riesgos	4	5	4	4	
	Desarrollar la estrategia de protección y plan de tratamiento	4	4	5	4	

IV. Implementación	Diseño de controles y procedimientos	5	4	4	4	
	Aplicar controles y procedimientos	4	4	4	5	
V. Comunicación y Evaluación del desempeño	Comunicación	4	5	4	4	
	Auditoría interna	4	5	4	5	
VI. Mejoras	Mejora continua	4	4	4	4	
TOTAL		63	64	62	64	

RESULTADOS

Opinión:

X	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma:

Ing. Juan Rafael Galán Santisteban (MBA)

EXPERTO 2

EVALUACIÓN DE JUICIO EXPERO

I. INDICADOR DE CALIFICACIÓN DE JUICIO EXPERTO

Estimado ingeniero:

Por medio del presente documento me dirijo a su digna persona para solicitar su colaboración con respecto a la validación de la propuesta de investigación titulada "Modelo de Seguridad de la Información para contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque". En el cual se tomó como marco de referencias las normas ISO 27001, OCTAVE – S, NIST 800, ISO 27005. Presentando cuestionario de validación y agradeciendo su importante colaboración.

Apellidos y Nombres	: Campos Medina Victor Hugo
Formación Académica	: Ingenieria de Computación y Sistemas
Área experiencia laboral	: Tecnología de la Información
Tiempo de experiencia	: 27 años
Institución	: EY Perú
Cargo actual	: Gerente de Consultoria

Objetivo de la investigación	: Contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de la región Lambayeque.
Objetivo del juicio de expertos	: Comprobar la validez del modelo propuesto en relación a suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	: Determinar la utilidad de las plantillas propuestas en las Unidades de Gestión Educativa Local de Lambayeque.

MATRIZ DE CONSISTENCIA PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN FINANCIERA EN LAS UNIDADES DE GESTIÓN EDUCATIVA LOCAL DE FERREÑAFE						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**COMENTARIO**
I. Contexto de la organización	Comprender la organización y su contexto.	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	Definir el alcance y los límites.	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	Análisis de brechas	4	4	4	4	Presenta de forma clara y concreta información y propuesta
II. Liderazgo	Liderazgo y compromiso.	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	Lista de Políticas y controles planificados.	4	4	4	4	Presenta de forma clara y concreta información y propuesta
III. Evaluación de Riesgos	Identificar los activos.	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	Valoración de los activos.	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	Identificar las amenazas y vulnerabilidades	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	Analizar los riesgos	4	4	4	4	Presenta de forma clara y concreta información y propuesta

	Desarrollar la estrategia de protección y plan de tratamiento	4	4	4	4	Presenta de forma clara y concreta información y propuesta
IV. Implementación	Diseño de controles y procedimientos	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	Aplicar controles y procedimientos	4	4	4	4	Presenta de forma clara y concreta información y propuesta
V. Comunicación y Evaluación del desempeño	Comunicación	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	Auditoría interna	4	4	4	4	Presenta de forma clara y concreta información y propuesta
VI. Mejoras	Mejora continua	4	4	4	4	Presenta de forma clara y concreta información y propuesta
	TOTAL	60	60	60	60	

RESULTADOS

Opinión:

X	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma:

Ing. Victor Campos Medina
CIP 73885

EXPERTO 3

EVALUACIÓN DE JUICIO EXPERTO

I. INDICADOR DE CALIFICACIÓN DE JUICIO EXPERTO

Estimado ingeniero:

Por medio del presente documento me dirijo a su digna persona para solicitar su colaboración con respecto a la validación de la propuesta de investigación titulada "Modelo de Seguridad de la Información para contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque". En el cual se tomó como marco de referencias las normas ISO 27001, OCTAVE – S, NIST 800, ISO 27005. Presentando cuestionario de validación y agradeciendo su importante colaboración.

Apellidos y Nombres	: Castro Marquina, Laura Daiana
Formación Académica	: Magíster MBA Centrum, Ingeniera Informática PUCP
Área experiencia laboral	: Consulting
Tiempo de experiencia	: 8 años
Institución	: EY Perú
Cargo actual	: Senior Consulting

Objetivo de la investigación	: Contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de la región Lambayeque.
Objetivo del juicio de expertos	: Comprobar la validez del modelo propuesto en relación a suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	: Determinar la utilidad de las plantillas propuestas en las Unidades de Gestión Educativa Local de Lambayeque.

MATRIZ DE CONSISTENCIA PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN FINANCIERA EN LAS UNIDADES DE GESTIÓN EDUCATIVA LOCAL DE FERREÑAFE						
FASE	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**COMENTARIO**
I. Contexto de la organización	Comprender la organización y su contexto.	4	4	4	4	
	Definir el alcance y los límites.	4	4	4	4	
	Análisis de brechas	4	4	4	4	
II. Liderazgo	Liderazgo y compromiso.	4	4	4	4	
	Lista de Políticas y controles planificados.	4	4	4	4	
III. Evaluación de Riesgos	Identificar los activos.	3	4	4	4	Revisar los comentarios
	Valoración de los activos.	5	5	5	5	
	Identificar las amenazas y vulnerabilidades	5	5	5	5	
	Analizar los riesgos	3	4	4	4	Revisar los comentarios
	Desarrollar la estrategia de protección y plan de tratamiento	4	4	4	4	

IV. Implementación	Diseño de controles y procedimientos	4	4	4	4	
	Aplicar controles y procedimientos	4	4	4	4	
V. Comunicación y Evaluación del desempeño	Comunicación	4	4	4	4	
	Auditoría interna	4	4	4	4	
VI. Mejoras	Mejora continua	3	4	4	4	Revisar los comentarios
	TOTAL	59	62	62	62	

RESULTADOS

Opinión:

X	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma:

_____

ANEXO 7

COMPARACIÓN DE RESULTADOS DE VALIDACIÓN DEL JUICIO DE EXPERTOS

RESULTADOS DE VALIDACIÓN DE JUICIO EXPERTO												
FASE	**ACTIVIDAD**	**Experto 1**				**Experto 2**				**Experto 3**			
		SUFICIENCIA	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**
I. Contexto de la organización	Comprender la organización y su contexto.	4	4	4	5	4	4	4	4	4	4	4	4
	Definir el alcance y los límites.	4	4	4	4	4	4	4	4	4	4	4	4
	Análisis de brechas	4	4	4	5	4	4	4	4	4	4	4	4
II. Liderazgo	Liderazgo y compromiso.	5	4	4	4	4	4	4	4	4	4	4	4
	Lista de Políticas y controles planificados.	5	4	5	4	4	4	4	4	4	4	4	4
III. Evaluación de Riesgos	Identificar los activos.	4	4	4	4	4	4	4	4	3	4	4	4
	Valoración de los activos.	4	5	4	4	4	4	4	4	5	5	5	5

	Identificar las amenazas y vulnerabilidades	4	4	4	4	4	4	4	4	5	5	5	5
	Analizar los riesgos	4	5	4	4	4	4	4	4	3	4	4	4
	Desarrollar la estrategia de protección y plan de tratamiento	4	4	5	4	4	4	4	4	4	4	4	4
IV. Implementación	Diseño de controles y procedimientos	5	4	4	4	4	4	4	4	4	4	4	4
	Aplicar controles y procedimientos	4	4	4	5	4	4	4	4	4	4	4	4
V. Comunicación y Evaluación del desempeño	Comunicación	4	5	4	4	4	4	4	4	4	4	4	4
	Auditoría interna	4	5	4	5	4	4	4	4	4	4	4	4
VI. Mejoras	Mejora continua	4	4	4	4	4	4	4	4	3	4	4	4

ANEXO 8

PERFIL DE EXPERTOS

PERFIL DE EXPERTO	
	**Juan Rafael Galán Santisteban** Profesional de Ingeniería en Computación e Informática, Experto en Finanzas y Gerencia Pública, Planificación Estratégica, Tecnologías de la Información, Simplificación Administrativa, Modernización de Gestión Pública y Control Interno. Con habilidad profesional del Colegio de Ingenieros del Perú. Magíster en Administración de Negocios. Con estudios de Maestría en Gobernabilidad Democrática, Económica y Social. Diplomado en Auditoría de Tecnologías de Información y Seguridad Informática; y experto en Gestión de Centros de Datos. Experiencia de 17 años en el sector público.

Datos Académicos

Grado	Título	Centro de Estudios
MAGÍSTER	MAGÍSTER EN ADMINISTRACIÓN DE NEGOCIOS	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
LICENCIADO / TÍTULO	INGENIERO EN COMPUTACIÓN E INFORMÁTICA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN COMPUTACIÓN E INFORMÁTICA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
	IMPLEMENTADOR LÍDER ISO 27001	NEW HORIZONS LIMA
	CALIDAD DEL SOFTWARE Y CMMI	UNIVERSIDAD SANTO TORIBIO DE MOGROVEJO
	ESPECIALIZACIÓN EN AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN Y SEGURIDAD INFORMÁTICA	UNIVERSIDAD SANTO TORIBIO DE MOGROVEJO
	DISEÑO E IMPLEMENTACIÓN DE CURSOS VIRTUALES	UNIVERSIDAD SANTO TORIBIO DE MOGROVEJO
	FINANZAS Y GERENCIA PÚBLICA	UNIVERSIDAD ESAN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
GOBIERNO REGIONAL LAMBAYEQUE	ANALISTA DE SISTEMAS – COORDINADOR DE PLANEAMIENTO Y GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	2014	ACTUAL
UNIVERSIDAD SEÑOR DE SIPÁN	DOCENTE A TIEMPO PARCIAL	2011	2015
UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO	DOCENTE ADSCRITO AL DPTO. DE INGENIERÍA	2006	2013
GOBIERNO REGIONAL LAMBAYEQUE	JEFE DEL ÁREA DE SOPORTE TÉCNICO	2003	2013
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DOCENTE ADSCRITO AL DPTO. DE ESTADÍSTICA Y COMPUTACIÓN	2000	2002
RED CIENTÍFICA PERUANA – INTERNET PERÚ	JEFE DE ÁREA DE SOPORTE TÉCNICO	1999	2000

PERFIL DE EXPERTO	
	**Víctor Hugo Santiago Campos Medina** Ingeniero de Computación de Sistemas, con maestría en negocios y tecnología, certificado en normas ISO e instructor oficial para la región Centro y Sudamérica. Su experiencia profesional se extiende por más de 26 años (20 años en una Big Four, 3 años en el sector financiero y 3 años en el sector gobierno), habiendo participado en proyectos de asesoría y auditoría de TI, aplicando marcos de trabajo como COBIT, COSO, Ley Sarbanes-Oxley (SOX), ISO/IEC 27001, Normas de Seguridad de Información y Continuidad del Negocio. Además tiene experiencia en Outsourcing de Auditoría Interna basada en Riesgos; Administración de Riesgos en Bancos en el marco del Acuerdo Basilea II.

Datos Académicos

Grado	Título	Centro de Estudios
MAGÍSTER	MAGÍSTER EN DIRECCIÓN ESTRATÉGICA EN TECNOLOGÍAS DE LA INFORMACIÓN	UNIVERSIDAD INTERNACIONAL IBEROAMERICANA
MÁSTER	MÁSTER UNIVERSITARIO EN ADMINISTRACIÓN, DIRECCIÓN Y ORGANIZACIÓN DE EMPRESAS	UNIVERSIDAD CAMILO JOSÉ CELA
LICENCIADO / TÍTULO	INGENIERO DE COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD DE SAN MARTÍN DE PORRES
BACHILLER	BACHILLER EN INGENIERÍA DE COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD DE SAN MARTÍN DE PORRES

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
EY BUILDING A BETTER WORKING WORLD	IT MANAGER - GERENTE RIESGO DE TECNOLOGÍAS	2017	ACTUAL
ORGANISMO DE CERTIFICACIÓN PECB	INSTRUCTOR OFICIAL	2017	ACTUAL
BANBIF BANCO INTERAMERICANO DE FINANZAS	SUB GERENTE DE AUDITORÍA TI	2015	2017
UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS	DOCENTE CURSOS ISO, RIESGOS EN NEGOCIO, SEGURIDAD EN LAS APLICACIONES	2014	2016
NEW HORIZONS COMPUTER LEARNING CENTERS	INSTRUCTOR OFICIAL	2008	2016
KPMG ASESORES S.C. DE R.L.	GERENTE DE CONSULTORÍA EN TI	2011	2015
ISEC INFORMATION SECURITY DEL PERÚ	INSTRUCTOR DEL PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA Y TECNOLOGÍAS DE LA INFORMACIÓN	2013	2013
KPMG ASESORES S.C. DE R.L.	GERENTE DE AUDITORÍA DE SISTEMAS	2005	2011

PERFIL DE EXPERTO	
	**Laura Daiana Castro Marquina** Magister en Administración Estratégica de Negocios e Ingeniera informática titulada, certificada en Lead Implementer ISO 27001 e ISO 22301 y con la certificación de protección de datos CDPSE, con más de 8 años de experiencia en Gestión y evaluación de riesgos, evaluación e implementación de sistemas de gestión de continuidad de negocios y sistemas de gestión de seguridad de la información, privacidad de datos, gobierno de TI y proyectos de reingeniería de procesos de TI) en empresas de sectores de consumo masivo, banca, minería, textil, hidrocarburos, construcción, salud, educación, banca y media; basado en ISO 22301, ISO27001, COBIT e ITIL.

Datos Académicos

Grado	Título	Centro de Estudios
MAGÍSTER	MAGÍSTER EN ADMINISTRACIÓN ESTRATÉGICA DE EMPRESAS	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
LICENCIADO / TÍTULO	INGENIERA INFORMÁTICA	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
BACHILLER	BACHILLER EN CIENCIAS CON MENCIÓN EN INGENIERÍA INFORMÁTICA	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ	DOCENTE TPA.	2013	ACTUAL
EY BUILDING A BETTER WORKING WORLD	SENIOR - INCHARGE ADVISORY SERVICES	2016	ACTUAL
VISANET PERÚ	AUDITORA TI	2014	2014
NETLINE CONSULTING	CONSULTORA CONTINUIDAD DE NEGOCIOS	2014	2016
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ	ANÁLISIS - DESARROLLO	2012	2012
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ	ENCARGADA DE GESTIÓN DE CALIDAD DE DATOS	2011	2011

ANEXO 9

RESULTADO CONSOLIDADO DE ENCUESTAS APLICADAS A LAS UNIDADES DE GESTIÓN EDUCATIVA LOCAL DE LAMBAYEQUE

Dónde: 1 = No, 2 = Parcial, 3 = Si

	ENCUESTA CONTROLES: Preguntas	Uchiclayo	Uferreñafe	Ulambayeque
A5	¿Existe un marco de políticas para la seguridad de la información?	1	3	1
	¿Todas las políticas de seguridad en su unidad educativa tienen un formato y estilo consistentes?	1	2	1
A6	¿Las responsabilidades en seguridad de la información están definidas y asignadas?	1	1	2
	¿Existe una política que cubra la segregación de deberes dentro de su unidad educativa?	1	2	1
	¿Existe una lista de detalles de contacto para las autoridades reguladoras y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias?	1	3	3
	¿Se comparte información sobre amenazas emergentes, nuevas tecnologías de seguridad, buenas prácticas de seguridad, advertencias tempranas de alertas y advertencias dentro de su unidad educativa?	1	2	2
	¿Se identifican y abordan los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos en su dependencia?	1	1	2
	¿Existen política y controles seguridad relacionados con los usuarios móviles?	1	1	1
	¿Existen disposiciones adecuadas para la autenticación del usuario, la seguridad de la red, antivirus, copias de seguridad, parches, encriptación y continuidad del negocio?	1	3	1
A7	¿El proceso de evaluación previa al empleo toma en cuenta las leyes y regulaciones relevantes de privacidad y empleo?	1	3	2
	¿Están claramente definidos los términos y condiciones de empleo?	1	3	2
	¿Se provee información sobre las estrategias y políticas de seguridad de la información en su unidad educativa?	1	1	2
	¿Existe un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los trabajadores?	1	1	1

	ENCUESTA CONTROLES: Preguntas	Uchiclayo	Uferreñafe	Ulambayeque
	¿Existe un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude por parte de los trabajadores?	1	3	1
	¿Existen políticas de revisión, estándares, procedimientos, directrices y registros relacionados con la seguridad de la información para los trabajadores que se mueven lateral o verticalmente dentro de la unidad educativa?	1	2	1
A8	¿Hay un inventario de activos de la información en la unidad educativa?	2	1	3
	¿Los activos cuentan con un responsable técnico?	2	2	3
	¿Existe una política sobre el uso aceptable de los recursos tecnológicos, como el correo electrónico, la mensajería instantánea, el FTP, las responsabilidades de los usuarios?	2	3	2
	¿Existe un procedimiento para recuperar los activos tras una baja o despido?	1	1	2
	¿Conoce los requisitos legales de información clasificada respecto a una divulgación o modificación no autorizada?	1	3	1
	¿Existe un procedimiento de etiquetado para la información tanto en forma física como electrónica?	1	1	3
	¿Están los niveles de clasificación de información adecuadamente asignados a los activos de la unidad educativa?	1	1	2
	¿Existe un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles?	1	1	3
	¿Existen una política específica y documentación de obligaciones contractuales, legales o reglamentarias para la eliminación de los medios de almacenamiento?	1	3	1
	¿Se utiliza un transporte o servicio de mensajería confiable para el traslado de estos medios?	1	1	1
A9	¿Existe una política de control de acceso dentro de su unidad educativa?	3	3	1
	¿Los controles de seguridad de la red son evaluados y probados regularmente (Pentesting)?	1	2	1
	¿Se utiliza un ID de usuario únicos para cada usuario?	3	3	3
	¿El acceso a sistemas y servicios de información se basa en las necesidades de la oficina de la unidad educativa?	3	3	3
	¿Se controlan o supervisan las actividades de los usuarios privilegiados de forma más detallada?	1	1	2

	ENCUESTA CONTROLES: Preguntas	Uchiclayo	Uferreñafe	Ulambayeque
	¿Se implementan controles técnicos, como la longitud mínima de la contraseña, reglas de complejidad, cambio forzado de contraseñas dentro de su unidad educativa?	1	3	3
	¿Se revisan los derechos de acceso para usuarios con privilegios de forma más exhaustiva y frecuente?	1	2	2
	¿Al retirar dererchos de acceso, tiene en cuenta empleados, proveedores y contratistas al finalizar o cambiar su empleo, contrato o acuerdo?	1	1	2
	¿Existe un proceso de cambio de contraseñas en caso de ser comprometida?	2	3	2
	¿Al acceder a un sistema, Se identifican los usuarios de forma individual?	3	3	3
	¿Se registran los inicios de sesión exitosos dentro de los sistemas de su unidad educativa?	1	3	3
	¿Los sistemas requieran una fortaleza de contraseñas establecidos en las políticas y estándares?	1	3	3
	¿Existe un proceso auditable de aprobación, y cada instancia de su uso está registrado para los privilegios de los sistemas?	1	1	2
	¿El código fuente de los sistemas, se almacena en una o más bibliotecas de programas fuente o repositorios?	3	1	1
A10	¿Se cumple con la política y requerimientos de controles cifrados?	1	1	1
	¿Se generan claves diferentes para sistemas y aplicaciones?	3	1	2
A11	¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado?	2	2	2
	¿Existe un registro de todas las entradas y salidas en su entidad educativa?	1	3	1
	¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos?	1	1	1
	¿Existe un procedimiento de recuperación de desastres?	1	1	1
	¿Se realiza una verificación al final del día por las oficinas, las salas de informática y otros lugares de trabajo?	1	1	1
	¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?	3	3	1
	¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas?	3	1	3
	¿El sistema UPS proporciona una potencia adecuada, confiable y de alta calidad?	3	1	3

	ENCUESTA CONTROLES: Preguntas	Uchiclayo	Uferreñafe	Ulambayeque
	¿Se separa el cableado de suministro eléctrico del cableado de comunicaciones para evitar interferencias?	3	1	3
	¿Se asigna personal cualificado para realizar el mantenimiento de los equipos (infraestructura y dispositivos de red, equipos de trabaja, portátiles, equipos de seguridad y servicios tales como detectores de humo, dispositivos de extinción de incendios)?	1	3	3
	¿Existe un control para limitar el traslado de activos de información mediante el uso de unidades de almacenamiento externo?	1	3	1
	¿Existe una política que cubra los requisitos de seguridad, con respecto al uso de dispositivos móviles o portátiles que se utilizan desde casa o en ubicaciones remotas?	1	1	1
	¿Se mantienen registros adecuados de todos los medios que se eliminan?	1	1	3
	¿Se protegen los bloqueos de pantalla con contraseña?	1	3	3
	¿Existen políticas, normas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas dentro de su unidad educativa?	1	1	1
A12	¿Existe un conjunto completo de procedimientos operacionales de seguridad y se revisan continuamente?	2	1	1
	¿Los cambios en responsabilidades operacionales, están debidamente documentados, justificados y autorizados por la administración?	1	3	1
	¿Existe una política de gestión de capacidad?	1	1	1
	¿Se tiene en cuenta el riesgo de la información y los aspectos de seguridad que incluye el cumplimiento de privacidad si los datos personales se mueven a entornos menos seguros?	1	3	3
	¿Existen políticas y procedimientos asociados a controles antimalware?	1	1	3
	¿Existen políticas y procedimientos asociados a las copias de seguridad dentro de su dependencia?	1	3	1
	¿Existen políticas y procedimientos para el registro de eventos?	1	3	1
	¿Los registros de eventos se almacenan en un formato seguro o mecanismo de control no-editable?	1	1	1
	Hay responsables identificados para la administración de acceso privilegiado al análisis de eventos?	1	3	1
	¿El reloj de todos los sistemas dentro de la unidad educativa están sincronizados a una fuente de tiempo de referencia única?	3	3	3

	ENCUESTA CONTROLES: Preguntas	Uchiclayo	Uferreñafe	Ulambayeque
	¿Existe una política acerca de la instalación de software?	2	3	3
	¿Existen procesos adecuados para verificar los inventarios de los sistemas e identificar si las vulnerabilidades divulgadas son relevantes?	1	1	1
	¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados?	3	3	3
	¿Existe una política que requiera auditorias de seguridad de la información?	1	1	1
A13	¿Existen políticas de redes físicas e inalámbricas?	1	3	3
	¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada?	1	2	3
	¿Los grupos de servicio de información, usuarios y sistemas se encuentran clasificados dentro de las redes?	2	1	3
	¿Existen políticas y procedimientos relacionados con la transmisión segura de información?	1	3	1
	¿Existen acuerdos para la transferencia segura de información entre la unidad educativa y partes externas?	3	3	1
	¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)?	1	1	1
	¿Existen acuerdos de confidencialidad para el intercambio de información entre la unidad educativa y partes externas?	2	3	3
A14	¿Existen políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software?	1	3	3
	¿La unidad educativa usa o proporciona aplicaciones web de comercio electrónico?	1	1	1
	¿Las transacciones de sistemas de información, se realizan y almacenan en un entorno interno seguro?	2	1	3
	¿Existe una política de desarrollo seguro que abarque la arquitectura de seguridad?	1	1	1
	¿Los cambios en los sistemas que utiliza la unidad educativa, están debidamente documentados, justificados y autorizados por la administración?	1	3	2
	¿Al cambiar las plataformas operativas, las aplicaciones y sistemas son revisados y probados para asegurar que no exista impacto adverso en las operaciones?	1	3	3
	¿Se hace una comprobación de compatibilidad con otro software en uso?	2	1	3

	ENCUESTA CONTROLES: Preguntas	Uchiclayo	Uferreñafe	Ulambayeque
	¿Se capacita a los desarrolladores para que tengan el conocimiento adecuado acerca de las prácticas seguras de programación?	1	1	1
	¿Se aíslan a un lugar seguro los ambientes de desarrollo e integración de sistemas?	1	1	1
	¿De contratar un tercero para desarrollo de software, éste es supervisado y monitoreado por la unidad educativa?	2	3	2
	¿Tiene en cuenta acuerdos de licencia, propiedad del código y propiedad intelectual al desarrollar un software?	1	3	3
	¿Se efectúan pruebas de seguridad antes de la introducción de nuevos sistemas en la red?	3	3	3
	¿Se utilizan mecanismos para proteger datos de prueba como la seudonimización, enmascaramiento, datos falsos, borrado, etc.?	1	3	1
A15	¿Los proveedores de servicios externos son monitoreados rutinariamente y auditados para cumplir con los requisitos de seguridad?	1	1	2
	¿Se ha establecido requisitos relevantes de seguridad de la información entre la unidad educativa y los proveedores cuando necesite acceder a la información de la dependencia?	1	2	3
	¿Los proveedores incluyen requisitos para abordar la seguridad de la información?	1	2	2
	¿La unidad educativa monitorea y revisa regularmente la entrega de servicios por parte de su proveedor?	1	1	3
	¿Los cambios en los servicios relacionados con la información, servicios adicionales por parte de los proveedores son gestionados tomando en cuenta los riesgos de la unidad educativa?	1	3	3
A16	¿Se han establecido responsabilidades de gestión para asegurar una respuesta rápida a los incidentes de seguridad de la información?	1	1	1
	¿Se crean informes de seguimiento de los incidentes de seguridad de la información?	2	1	1
	¿Existe una obligación contractual por parte de los empleados para reportar cualquier tipo de ocurrencia inusual que involucre la seguridad de la información?	1	2	3
	¿Los eventos de seguridad de la información son evaluados y calificados como incidentes de seguridad?	2	2	1
	¿Se documentan las acciones tomadas para resolver y finalmente cerrar un incidente?	1	1	3
	¿Existe un proceso de evaluación investigación para identificar incidentes de impacto recurrentes de seguridad?	1	1	3

	ENCUESTA CONTROLES: Preguntas	Uchiclayo	Uferreñafe	Ulambayeque
	¿Haya personal capacitado, competente y confiable con herramientas adecuadas y procesos definidos para recopular evidencias de incidentes de seguridad?	1	1	3
A17	¿Existen un diseño adecuado de continuidad para sistemas de TI, redes y procesos críticos?	1	1	1
	¿La unidad educativa establece procesos y controles para asegurar la continuidad de seguridad de la información?	1	2	1
	¿Existe un método de pruebas del plan de continuidad?	1	1	1
	¿Los controles clave de seguridad de la información están implementados y son funcionales en los sitios de recuperación de desastres?	1	1	1
A18	¿Existe una política acerca del cumplimiento de requisitos legales?	2	3	1
	¿Existen políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento?	3	3	3
	¿Los registros de la unidad educativa, están protegidos de cualquier pérdida y divulgación no autorizada?	1	1	1
	¿Hay un responsable de privacidad en la organización?	1	2	1
	¿Existe una política que cubra actividades relacionadas con importación, exportación de material criptográfico?	1	1	1
	¿Están las prioridades de implementación de controles alineadas con los riesgos a activos de información?	1	1	1
	¿Se hace una verificación periódica del cumplimiento de las políticas relacionadas a la seguridad de la información?	2	1	3
	¿Se llevan a cabo escaneos de vulnerabilidades de red y pruebas de Pentesting regulares para verificar el cumplimiento de las políticas de seguridad dentro de su unidad educativa?	2	1	2