DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL - CHICLAYO

DESIGN OF AN INFORMATION SECURITY MANAGEMENT SYSTEM FOR THE LOCAL EDUCATION MANAGEMENT UNIT - CHICLAYO

Victor Miguel Baca Flores[1]

Fecha de recepción: 17 de abril 2016
Fecha de aceptación: 20 de mayo 2016

Resumen

El presente trabajo de investigación tiene por objetivo fundamental el diseño de un Sistema de Gestión de Seguridad de la Información para la Unidad de Gestión Educativa Local de Chiclayo, basado en las normas internacionales ISO/IEC 27001:2013 e ISO/IEC 27002:2013, adoptando COBIT 5 como marco de trabajo, debido a que las medidas actuales de control para satisfacer los requisitos mínimos de seguridad han sido poco efectivos. La importancia del diseño del SGSI permitió determinar los objetivos, procesos y procedimientos para el establecimiento de políticas y controles de seguridad que ayudarán a gestionar los riesgos en la seguridad de la información que maneja la Unidad de Gestión Educativa Local de Chiclayo, mejorando de esta forma la gestión de los incidentes de seguridad que se detecten. El estudio fue descriptivo. La población y muestra estuvo constituida por los empleados de la Unidad de Gestión Educativa Local de Chiclayo. Para la recolección de datos se utilizaron técnicas como el análisis de documentos, encuestas al personal, entrevistas y observación directa; los formatos utilizados fueron cuestionarios. El análisis de datos se realizó utilizando la herramienta de procesamiento Excel, la cual sirvió como software de auditoría para el análisis de riesgos. La metodología empleada para el análisis y evaluación de riesgos, se basó principalmente en MAGERIT v.3.0.

Se concluye que el diseño de un SGSI permite mejorar la situación actual que vive la Unidad de Gestión Educativa Local de Chiclayo en materia de seguridad de la información, ya que la utilización de estándares internacionales y buenas prácticas, repercuten directamente en una efectiva gestión de la información dentro de la institución objeto de estudio, garantizando el cumplimiento de los principios básicos de seguridad: integridad, disponibilidad y confidencialidad.

Palabras claves: *ISO 27001, MAGERIT, Seguridad de la Información, SGSI*.

Abstract

This research work is fundamental objective of the design of a Management System Information Security for Unit Local Educational Management Chiclayo, based on international standards ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013, I adopting COBIT 5 as the framework, because the current control measures to meet the minimum safety requirements have been ineffective. The importance of design ISMS allowed to determine the objectives, processes and procedures for establishing policies and security controls that help manage security risks of the information handled by the Unit Local Educational Management of Chiclayo, thus improving the management of security incidents are detected. The study was descriptive. The population and sample consisted of employees of the Local Education Management Unit of Chiclayo. For data collection techniques were used as analysis of documents, staff surveys, interviews and direct observation; the formats used were questionnaires. Data

[1] *Escuela Profesional de Ingeniería de Sistemas. Facultad de Ingeniería Civil, de Sistemas y de Arquitectura. Ing. Universidad Nacional "Pedro Ruiz Gallo" Lambayeque. Lambayeque. Perú. vmbacaflores@gmail.com.*

analysis was performed using Excel processing tool, which served as audit software for risk analysis. The methodology used for analysis and risk assessment was based mainly on MAGERIT v.3.0.

It is concluded that the design of an ISMS can improve the current situation in the Unit of Local Educational Management Chiclayo security of information, as the use of international standards and best practices directly affect effective management information within the institution under study, ensuring compliance with the basic safety principles: integrity, availability and confidentiality.

Keywords*: ISO 27001, ISMS, Information Security, MAGERIT.*

1. Introducción

En la actualidad, no se puede cuestionar el hecho que la gran mayoría de procesos de negocio están siendo soportados, automatizados y gestionados por sistemas informáticos, así como los sistemas de información apoyan en la actividad gerencial y en la toma de decisiones, inclusive es la propia información y el acceso a la misma, el producto o servicio que se intercambia como principal objeto de negocio. La seguridad de la información ya no puede ser vista como el resultado de un accionar defensivo y reactivo, sino se debe requerir de la incorporación de la misma como elemento estratégico. De esa manera, la organización al gestionar adecuadamente la seguridad de su información, por un lado, está dando cumplimiento a sus obligaciones y regulaciones y a su vez genera la confianza necesaria en sus clientes. Cada día, existe mayor conciencia en la importancia de la seguridad de la información en las empresas y organizaciones, cualquiera sea el sector de la economía o rol en la sociedad que desempeñen, de preferencia empresas medianas y grandes. La seguridad de la información, no es un activo que se compra; la seguridad debe gestionarse, debe existir una meta concreta, tomarse criterios de evaluación y decisión, además debe poder medirse; es un sistema dinámico en constante evolución que debe ser evaluado y monitoreado, con métricas establecidas que permitan comparar de manera consciente y objetiva, diferentes escenarios y tomar decisiones con respecto a los riesgos que se afrontan y los recursos con los que se cuentan. Como parte de la seguridad de la información de las organizaciones, se deben identificar primero los activos de información que tienen un impacto significativo en el negocio; luego, realizar un análisis y evaluación del riesgo, y, por último, decidir cuáles son las opciones de tratamiento del riesgo a implantar a fin de minimizar las posibilidades de que las amenazas puedan causar daño a la organización. Los pasos descritos anteriormente, son las acciones que un Sistema de Gestión de la Seguridad de la Información busca instaurar en una empresa.

Es por ello, que el presente trabajo de investigación tiene por objetivo fundamental el diseño de un Sistema de Gestión de Seguridad de la Información para la Unidad de Gestión Educativa Local de Chiclayo, basado en las normas internacionales ISO/IEC 27001:2013 e ISO/IEC 27002:2013, adoptando COBIT 5 como marco de trabajo.

2. Materiales y Métodos

Dentro de la presente investigación de tipo descriptiva aplicada, se utilizaron variables e indicadores obtenidos de los mismos dominios de la norma, que fueron seleccionados y adecuados a la investigación. Estas dimensiones, junto con el objeto de estudio, conforman las variables de estudio, que por ser un modelo de tipo causal en el que las dimensiones definen y miden el grado de la Seguridad de la Información, y se clasifican:

Tabla 1: *Variables dependientes e independientes*

Clasificación	Dimensiones
Dependiente	Seguridad de la Información
Independientes	Políticas de seguridad. Aspectos Organizativos. Seguridad ligada a los Recursos Humanos. Gestión de Activos. Control de Accesos. Cifrado. Seguridad Física y Ambiental. Seguridad en la Operativa. Seguridad en las Telecomunicaciones.

Fuente: *Elaboración propia.*

Cada variable independiente, tiene uno o más indicadores, los cuales fueron seleccionados de los controles de la norma. Específicamente, se seleccionaron setenta y tres (73), donde cada indicador o control se mide a través de las encuestas realizadas. Se seleccionaron los controles más relevantes para la seguridad actual de la UGEL – Chiclayo que estaba directamente relacionado con los problemas detectados en la investigación preliminar.

a) Población y muestra.

La población de la presente investigación está determinada por el personal, como se muestra:

Tabla 2: *Descripción de la población.*

Oficina	Personal	Nº
UGEL Chiclayo	Director, especialistas, técnicos, analistas.	7
Gestión Pedagógica	Director, Especialistas, Técnicos, Psicológicos.	15
Gestión Institucional	Director, Especialistas, Profesionales	7
Oficina de Administración	Director, Especialistas, Técnicos, Supervisores.	26
Asesoría Jurídica	Director, Abogados.	5
	Total	60

Fuente: *CAP UGEL Chiclayo - 2014.*

Al ser la población pequeña, la muestra estaría conformada por el mismo número de elementos.

b) Estrategias para la demostración de la hipótesis.

La naturaleza del proyecto es una investigación por objetivos, por lo que culminado la ejecución del proyecto se procederá al análisis de los resultados los cuales se contrastarán con la hipótesis y con los objetivos cumplidos. En el transcurso de la investigación se utilizarán diversos métodos que permitan evaluar la hipótesis, entre ellos:

Método inductivo, con el que se utilizará un marco referencial basado en casos exitosos, de otras empresas u organizaciones, lo que permitirá inducir posibles soluciones a la problemática encontrada; y ***Método estadístico***, para el análisis y procesamiento de los datos obtenidos de encuestas u otras técnicas de recolección de datos que permitan obtener a través de la estadística mediciones estimadas.

c) Materiales, herramientas y equipos.

Para la presente investigación, la utilización de equipos informáticos, paquetes de ofimática, acceso a internet fueron necesarios, además de la bibliografía, la misma que fue adquirida durante el transcurso de la investigación a través de libros, documentos electrónicos, manuales y direcciones electrónicas.

d) Técnicas, Formatos y Ensayos para la recolección de datos.

Entre las técnicas de recolección de datos se emplearon: *análisis de documentos*, como bibliografías digitalizadas e impresas, documentos internos y documentación diversa de la institución; *entrevistas* realizadas al personal administrativo, directores de las diferentes áreas beneficiadas por el área de TI, y al Coordinador del Centro de Sistemas de Información de la UGEL Chiclayo, siendo su opinión y experiencia muy importantes, por estar involucrado de manera directa con la gestión de la información; *encuestas escritas*, donde los participantes evaluarán la situación actual de la institución frente a la seguridad de la información; además, se utilizó la técnica de *observación directa* durante varios periodos del día. Se utilizaron cuestionarios como formatos para la recolección de datos, se utilizaron como instrumentos: guías de análisis documental, metodologías de análisis y recolección de datos, modelos de operacionalización de las variables y fichas de recolección de datos y resúmenes.

e) Análisis de datos.

Para el análisis de los datos obtenidos mediante las técnicas e instrumentos de recolección de datos se utiliza la herramienta de procesamiento MS Excel en su actual versión, la cual servirá como software de auditoria durante el análisis de riesgos en la UGEL – Chiclayo.

3. Resultados

El análisis de los resultados obtenidos, tras la aplicación de los diferentes instrumentos metodológicos, permitió identificar, analizar y diagnosticar una serie de factores que condicionan la seguridad de la información en la UGEL – Chiclayo.

A continuación, se presenta la propuesta de Diseño de un Sistema de Gestión de Seguridad de la Información a ser implementado más adelante en la institución, con la finalidad de minimizar los riesgos detectados.

Descripción de la propuesta.

Se adoptaron las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 y COBIT 5 en el diseño del SGSI, como estrategia de mejora. Estas normas internacionales, proporcionan un modelo sólido y aceptado para la implementación de principios y lineamientos que gobiernan desde la evaluación, diseño hasta la implantación de la seguridad en cualquier organización.

Para el establecimiento del SGSI se adoptó MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, en su versión 3.0, por ser compatible con los estándares propuestos. Dicha metodología, ofrece ventajas: es gratuita, es reconocida mundialmente por diferentes organismos de certificación ISO, y define claramente lo que se tiene que hacer paso por paso y proporciona mucha documentación y ejemplos al alcance del usuario.

Desarrollo de la propuesta.

Las normas seleccionadas y la metodología MAGERIT dividen el proyecto SGSI en una serie de etapas que deben llevarse a cabo, siendo estas: (a) Establecimiento del SGSI, (b) Implementación y operación del SGSI, (c) Monitoreo y revisión del SGSI y (d) Mantenimiento y mejora del SGSI.

En la etapa del Establecimiento del SGSI, que es el objetivo de esta propuesta, se contempla una serie de pasos, los cuales se explican a continuación:

a) Definir un Comité de Gestión de SI.

Un Comité de Seguridad de la Información (CSI) está destinado a garantizar el apoyo de las autoridades en las iniciativas de seguridad para lograr un buen trabajo, comprometiendo las áreas involucradas. Se define un CSI como parte de la propuesta, donde se detalla el objetivo e importancia de crear un Comité encargado de tratar concernientes a la seguridad de la información en la UGEL Chiclayo. Se detallan algunas indicaciones, como la selección y número de miembros, quienes deberían conformarlo, la asignación de un Oficial de Seguridad de la Información, el establecimiento de horarios para las reuniones, cada qué tiempo deben llevarse y la posibilidad de modificar el MOF de la institución con el fin de incorporar ciertas funciones de seguridad de la información y gestión de riesgos. En lo que concierne a la composición del Comité, se tomó el criterio de elegir a los representantes de las diferentes áreas, comenzando por el Órgano de Dirección quien sería la persona que asuma el rol de presidente (a), el coordinador del centro de sistemas, quien fue propuesto como Oficial de Seguridad de la Información por sus años de experiencia en el ámbito laboral como Ingeniero de Sistemas, mientras que los demás miembros, estarían conformados por los directores de las diferentes áreas de la institución.

Además, se propuso cambiar la estructura organizacional con el fin de incorporar el Comité y otras entidades de especialistas o consultorías externas. No podían faltar las funciones que el Comité debe asumir como parte de su rol en la seguridad y la documentación concerniente a cada reunión, el registro de los temas que se tratan, y las decisiones que se toman.

b) Definir el alcance del SGSI.

En este documento, se define los límites del SGSI, quien pretende regularizar y controlar todo aspecto concerniente al uso de sistemas de información, prestación de servicios, revisión de procedimientos y almacenamiento de información en servidores a fin de mantener las operaciones lo más seguras posibles sin impactar en el nivel de servicio y en la continuidad de las operaciones, facilitando la gestión administrativa de la institución; siendo cuatro los servicios que brinda: Educación Básica Regular, EB Alternativa, EB Especial y Educación Técnico Productiva.

En lo que concierne a los sistemas de información gestionados por la UGEL se consideraron: Sistema de Gestión Documentaria, Sistema de Información de Apoyo a la Gestión de la Institución Educativa, Sistema de Información Integrado de Gestión Administrativa, Sistema de Racionalización, Sistema Electrónico de Contrataciones del Estado, Sistema Estadística de la Calidad Educativa, Sistema Integrado de Administración Financiera, Sistema NEXUS MINEDU, Sistema SIENEC de Estadística.

Se incluyeron los activos de información identificados como relevantes en los principales procedimientos seleccionados de la UGEL Chiclayo.

c) Definir la Política de Seguridad.

Una política de seguridad debe ser parte de la documentación de la UGEL Chiclayo, debiendo ser aprobada previamente por el Comité de Gestión de Seguridad, y puesto a conocimiento del Órgano de Dirección, buscando su aceptación y compromiso. Esta política debe estar disponible como información documentada, ser comunicada dentro de la institución y puesta a disposición de las partes interesadas.

Esta política contiene una declaración donde la institución reconoce que la información que se genera, procesa o administra en el ejercicio de sus funciones, constituye un recurso muy valioso para la eficacia del desempeño institucional. A esto se suman los objetivos y el alcance que tendrá dicha política, se definen roles y responsabilidades de cada involucrado, entre ellos: el Comité de Seguridad, la Dirección, el Oficial de Seguridad de la Información, el personal que labora en la institución y personal externo: clientes, proveedores de bienes o servicios y otras partes interesadas. Dentro de la Política de Seguridad, se detallan aquellos lineamientos y políticas, que deberán ser adecuados a los cambios que puedan ocurrir en la institución, estos cambios pueden involucrar a la tecnología. Así mismo, se aclara que este tipo de documento debe ser revisado y actualizado regularmente una vez al año, para evitar que

queden en el olvido o reflejen una realidad distinta a la que realmente es. Se toma en cuenta las sanciones respectivas que se aplicarán; en caso no se cumpla con lo indicado.

d) Definir una metodología de evaluación riesgos.

Se define un enfoque o una metodología de evaluación de riesgos, apropiada para el SGSI y las necesidades de la organización, desarrollando criterios de aceptación de riesgos y determinando un nivel de riesgo aceptable. La metodología utilizada resulta de combinar diferentes propuestas existentes, y utiliza un método cualitativo, que permite la agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo. Se toma a MAGERIT en su versión 3.0 como fuente importante de información para la construcción de esta metodología.

En la estructura de la metodología, se detallan: el objetivo, términos y definiciones a considerar, y las personas autorizadas para la ejecución del documento a cargo del Oficial de Seguridad. Previo a esta metodología de evaluación, se considera otra para la identificación, clasificación y valoración de activos, posteriormente se identifican amenazas a los que se encuentran expuestos estos activos de información, para luego determinar los riesgos que pueden amenazar la información de la institución. Se determina la probabilidad de ocurrencia según las preguntas: ¿ha sucedido antes?, ¿sucede muy seguido?, ¿podría suceder?, a esto se agrega el nivel de impacto que tendría si la amenaza se llega a materializar, considerando los controles existentes en la institución. Seguido, se multiplica el valor de la probabilidad con el nivel de impacto, para obtener un nivel de riesgo, que será clasificado en tres niveles: alto, medio y bajo. Una vez determinado el nivel de riesgo, se identifica quien o quienes son los responsables del tratamiento del mismo y se evalúa qué tipo de tratamiento es el más apropiado: *mitigar, aceptar, transferir o evitar el riesgo.* Por último, se seleccionan los objetivos de control y controles, con ayuda de los estándares internacionales, para realizar un mapeo de controles en el que se identifican cuáles de estos controles se han de implementar con el fin de reducir el nivel de impacto o la probabilidad de ocurrencia de los riesgos, hasta llevarlos a un nivel aceptable para la institución.

La metodología permite un trabajo más ordenado y precioso en el análisis y evaluación de riesgos.

e) Análisis y evaluación de riesgos.

El primero paso para mejorar la seguridad en una institución es dar respuesta a estas preguntas: ¿qué proteger?, ¿contra qué?, y ¿qué esfuerzo se está dispuesto a invertir para obtener una protección adecuada?, estas interrogantes conforman lo que se conoce como Análisis del riesgo, es aquí donde se detecta a tiempo las amenazas a las que está expuesto un activo de información, la probabilidad de ocurrencia y sus posibles consecuencias sino se realiza nada al respecto. Luego de identificar qué se va a proteger, contra qué y cuánto esfuerzo se necesita, se procede a gestionar el riesgo, tras una serie de actividades necesarias que no hacen más que controlar aquellas amenazas que pudiesen existir.

A continuación, se detallan las actividades realizadas para el análisis y evaluación de riesgos:

Identificación de activos

La UGEL Chiclayo no cuenta con un inventario de activos de información, así que, por ser una propuesta del trabajo de investigación, y por ser el primer SGSI que se puede implementar, se propuso una manera de identificarlos, ya que éstos necesitan ser clasificados, valorados y protegidos. Se realiza una clasificación de activos, tomando en cuenta varias metodologías, se elaboró una propia, donde agrupa los activos, con el fin de facilitar la identificación de amenazas y posteriormente la evaluación de riesgos.

Tabla 3: *Clasificación de activos de información*

Tipo de activo	Descripción
[D] Información	Activo que será almacenado en equipos o soportes de información, o será transferido de un lugar a otro por los medios de transmisión de datos.
[S] Servicios	Función que satisface una necesidad de los usuarios.
[SW] Software	Sistemas de información, aplicaciones, herramientas de desarrollo y utilidades.
[HW] Hardware	Equipamiento informático destinado a soportar los servicios que presta la institución, siendo depositarios de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesamiento o transmisión de datos.
[COM] Redes de comunicaciones.	Incluyen tanto las instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
[Media] Soportes de información.	Dispositivos físicos que permiten almacenar información de forma permanente, o durante largos períodos de tiempo.
[AUX] Equipamiento auxiliar.	Equipos que sirven de soporte a los sistemas de información, sin estar relacionados con los datos.
[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.
[P] Personal	Personas relacionadas con los sistemas de información.

Fuente: *Libro II MAGERIT v.3 – 2012*

Una vez identificados, clasificados y agrupados, se realiza una valoración, tomando en cuenta su nivel de importancia y la necesidad de ser protegido, pues cuanto más valioso es un activo de información, mayor nivel de protección se requiere. Se utilizó la escala de Likert que se muestra a continuación:

Tabla 4: *Escala Likert para valorar activos*

Valor	Descripción
5	Muy alto
4	Alto
3	Medio
2	Bajo
1	Muy bajo

Fuente: *Elaboración propia*

Dicha escala se elaboró con el criterio de cuál sería impacto en la operatividad, cumplimiento legal o imagen institucional si la pérdida o falla del activo afecta la divulgación o revelamiento no autorizado (confidencialidad), la exactitud o completitud (integridad) y la accesibilidad o disposición (disponibilidad) de la información.

Reciben una valoración de (5) aquellos que impacten irreversiblemente en la institución, un (4) aquellos que lo hagan gravemente, un (3) si su impacto es considerable, un (2) si solo es parcial, y un (1) si no impacta en la operatividad, cumplimiento legal o imagen institucional de la UGEL Chiclayo. Estos valores se establecen de manera subjetiva. Luego, se estima el valor del activo, de promediar los valores del nivel de importancia de la confidencialidad, integridad y disponibilidad, para calcular luego un nivel de tasación, según la tabla:

Tabla 5: *Nivel de tasación de activos.*

Valor del activo	Nivel de tasación
3.334 - 5	Alto
1.668 – 3.333	Medio
1 – 1.667	Bajo

Fuente: *Elaboración propia*

Aquellos activos cuyo nivel de tasación sea BAJO, no serán considerados para el análisis y evaluación de riesgos.

Identificación de amenazas

Una amenaza tiene el potencial de dañar los activos de cualquier organización, indiferente del tamaño que esta tenga, por ello es muy importante identificar las principales a las que los activos están expuestos. En este punto, se debe hacer un listado de aquellas que afectan los activos de información de la UGEL Chiclayo, siendo algunas, producto de desastres naturales, como incendios, terremotos, inundaciones; mientras que otras, serán producto de la actividad humana.

En esta propuesta, por cada activo, se determinaron las posibles amenazas a las que están expuestos, luego, según la experiencia del coordinador de sistemas, se consideran aquellas que pudiesen presentarse en alguna oportunidad.

En la siguiente tabla, se sugiere un listado de posibles amenazas que afectan según el tipo de activo y las dimensiones de seguridad, tomando a MAGERIT como metodología:

Tabla 6: *Listado de amenazas.*

Amenazas
Incendios de causa natural.
Inundaciones de causa natural
Otros desastres naturales (terremotos)
Incendios generados de forma accidente o deliberada
Inundaciones por fuga de agua.
Explosiones
Derrumbes
Sobrecarga eléctrica.
Fluctuación eléctrica.
Polvo y suciedad.

	Averías de origen físico o lógico. Corte del suministro eléctrico. Fallo en el servicio de comunicaciones. Interrupción de otros servicios y suministros esenciales (refrigerante) Degradación de los soportes de almacenamiento de información

Fuente: *Libro II: Catálogo de Elementos de MAGERIT*

Evaluación del riesgo.

Una vez identificadas las amenazas, se podrá identificar fácilmente cuál es el nivel de riesgo existente y así poder tomar las medidas que ayuden a proteger los activos de información de la UGEL. Para ello, primero se debe determinar la probabilidad y el nivel de impacto que puede ocasionar, ambos se detallan:

Probabilidad de ocurrencia, se determina mediante las interrogantes: ¿ya ha sucedido antes?, ¿sucede muy seguido?, y ¿podrá suceder más adelante? La valoración lo determina la siguiente tabla:

Tabla 7: *Criterios para el cálculo de la probabilidad de ocurrencia.*

Nivel	Probabilidad	Frecuencia
5	Muy alta	Una vez a la semana.
4	Alta	Una vez al mes.
3	Moderada	Una vez cada 6 meses
2	Baja	Una vez al año
1	Muy baja	Una vez cada 5 años

Fuente: *Elaboración propia*

La probabilidad de ocurrencia se medirá de acuerdo a la frecuencia con que una amenaza se haya materializado antes en la institución, o que con el tiempo pueda suceder.

Nivel de impacto, se determina cuál es el nivel de impacto que tendría la materialización de la amenaza, considerando los controles existentes. Para esta valoración se recomienda utiliza la siguiente tabla:

Tabla 8: *Criterios para el cálculo del impacto.*

Nivel	Impacto	Criterio
8	Catastrófico	Interrupción de las operaciones de la UGEL Chiclayo por más de 1 semana.
6	Mayor	Interrupción de las operaciones de la UGEL Chiclayo por más de 2 días.
4	Moderado	Interrupción de las operaciones de la UGEL Chiclayo por 1 día.
2	Menor	Interrupción de las operaciones de la UGEL Chiclayo por algunas horas.
1	Insignificante	No hay interrupción de las operaciones.

Fuente: *Elaboración propia*

Para el nivel de impacto, se toma como criterio, en qué medida repercute en las operaciones de la UGEL Chiclayo y por cuánto tiempo lo hace.

Evaluación del riesgo, el valor del riesgo, se obtiene de la multiplicación de la probabilidad y el nivel de impacto previamente definidos, lo cual permite ubicar el riesgo en una de las siguientes celdas, con la ayuda de la matriz de calor:

Tabla 9: *Matriz de calor.*

IMPACTO	8	8	16	24	32	40
	6	6	12	18	24	30
	4	4	8	12	16	20
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		PROBABILIDAD				

Fuente: *Elaboración propia*

La obtención del valor del riesgo, es una cifra que permitirá clasificarla en un nivel, dicho nivel como se muestra en la tabla 10, se divide en: Bajo, Medio y Alto, siguiendo el siguiente criterio:

Tabla 10: *Niveles de riesgo.*

Riesgo	Impacto	Criterio
1 - 8	Bajo	Riesgos inferiores, deben ser tratados con procedimientos de rutina de la institución.
9 - 19	Medio	Riesgos que necesitan ser tratados con ayuda de controles de seguridad.
20 - 40	Alto	Riesgos que deben ser tratados de manera inmediata y con alta prioridad.

Fuente: *Elaboración propia*

Aquellos riesgos cuyo valor oscile entre 1 y 8, serán de nivel BAJO, que deben ser tratados con procedimientos de rutina por la institución; aquellos cuyo valor oscile entre 9 y 19, serán de nivel MEDIO, y ya requieren ser tratados con ayuda de controles de seguridad; para los que adquieran un valor de 20 a 40, serán considerados de nivel ALTO, y deberán ser tratados de manera inmediata por la institución, y considerados de alta prioridad, por causar mayores daños. En la presente investigación, se identifican amenazas por cada activo de información, luego se determina el valor del riesgo, a partir de obtener la probabilidad de ocurrencia y el nivel de impacto, para finalizar con un nivel de riesgo, dejando paso al tratamiento del mismo en el siguiente punto.

Tratamiento del riesgo

Se debe identificar quien o quienes son los responsables del tratamiento de los riesgos y evaluar los tipos de tratamiento más apropiados. Para esta propuesta se dispone de cuatro maneras de tratar el riesgo, dejando a decisión de la institución el tipo de tratamiento que se va a disponer. Se explica mejor los criterios en la siguiente tabla:

Tabla 11: *Tratamiento de riesgos*

Tratamiento	Descripción
Mitigar	Implementar controles de seguridad de la información a fin de reducir el riesgo a niveles aceptables. Se utiliza cuando al implementar controles trae beneficios mayores a la inversión de su implementación.
Aceptar	Aceptar la posibilidad de que pueda ocurrir el riesgo sin tomar medidas de acción concretas. Se utiliza cuando el costo de implementar controles, en términos económicos, superan el impacto del riesgo que se desea reducir, o cuando el impacto del riesgo es mínimo.
Transferir	Transferir el impacto del riesgo a terceros, empresas aseguradoras o proveedoras de servicio. Se utiliza cuando no se puede reducir la probabilidad de ocurrencia del riesgo, pero su impacto es inminente.
Evitar	Eliminar la fuente que genera la amenaza. Se utiliza cuando el nivel de riesgo es Alto, la actividad del proceso o sistema que lo genera no es de gran impacto en términos de negocio para la institución, de modo que puede ser retirada funcionalmente.

Fuente: *Elaboración propia*

Luego de haber definido los niveles de riesgos respecto a las amenazas que puedan afectar la integridad, confidencialidad o disponibilidad de los activos de información en el punto anterior; se definió un criterio de aceptación del riesgo el cual determina si el riesgo es Aceptable o si requiere de algún tratamiento.

Selección de objetivos de control y controles

En este paso se proponen controles o salvaguardas para gestionar los riesgos identificados en el paso anterior y así reducirlos hasta un nivel aceptable por la institución.

Estos controles se toman de la ISO/IEC 27002:2013, sin embargo, este estándar internacional aclara que los controles propuestos no son exclusivos y podrían ser complementados con otros, esto va de la mano con el entorno y la realidad que vive la institución.

En la investigación se detallan los objetivos de control y controles sugeridos, tomando en cuenta nuevos de los catorce dominios del estándar internacional delimitados en el alcance del estudio. Se incluye una Cláusula de seguridad, el Objetivo de control, los controles propuestos adaptados a la UGEL Chiclayo y el riesgo que se reducirá a un nivel aceptable por la institución. Todo esto es una forma resumida y clara de observar los controles que se proponen para gestionar los riesgos detectados en la

UGEL Chiclayo en cada uno de sus activos de información. Se puede apreciar en la siguiente tabla un ejemplo de dichos controles:

Tabla 12: *Selección de controles y objetivos de control*.

Dominio		Objetivo de control		Control propuesto
5	Políticas de Seguridad de la Información	5.1.	Directrices de la Dirección en seguridad de la información.	5.1.1. Conjunto de políticas para la seguridad de la información.
				5.1.2. Revisión de las políticas para la seguridad de la información.
6	Aspectos Organizativos de la Seguridad de la Información	6.1.	Organización interna.	6.1.1. Asignación de responsabilidades para la seguridad de la información.
				6.1.2. Segregación de tareas.
				6.1.3. Contacto con las autoridades.
				6.1.4. Contacto con grupos de interés especial.
				6.1.5. Seguridad de la información en la gestión de proyectos.
		6.2.	Dispositivos para movilidad y teletrabajo.	6.2.1. Política de uso de dispositivos móviles.

Fuente: *Elaboración propia*

Aprobación de la Gerencia para riesgos residuales

En el paso anterior, se seleccionaron los controles y objetivos de control para los niveles de riesgos existentes. La aplicación de estos controles persigue llevar el riesgo a niveles aceptables, permitiendo un margen de error, el Riesgo Residual, el cual debe ser conocido y aprobado por el Órgano de Dirección. La aprobación de los riesgos residuales implica que la gerencia acepte los niveles resultados del tratamiento del riesgo propuesto.

Partiendo de ello, se hace necesario en la presente investigación que el Órgano de Dirección de la UGEL Chiclayo, apruebe el riesgo residual no cubierto. La aprobación se puede conseguir de dos maneras: (a) Con la firma de la Matriz de Riesgos, o (b) con la firma del siguiente documento que constituye un ejemplo de declaración:

GOBIERNO REGIONAL LAMBAYEQUE

APROBACIÓN DEL RIESGO RESIDUAL

DECLARACIÓN

A través del presente documento se aprueba el “Riesgo Residual de Seguridad de la Información” no cubierto en la implantación de los controles y objetivos de control sugeridos como resultado del Análisis y Evaluación de Riesgos para el primer Sistema de Gestión de Seguridad de la Información de la Unidad de Gestión Educativa Local de Chiclayo. A los…… días del mes de……del 2015.

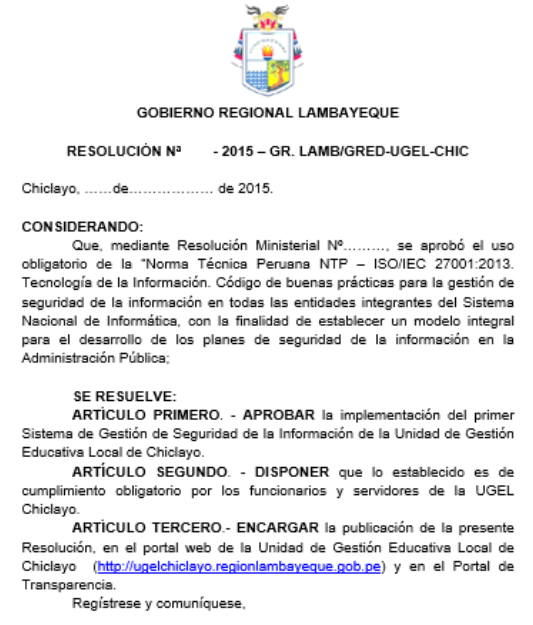
DRA. ZOILA URIARTE GONZÁLES
DIRECTORA DE LA UGEL CHICLAYO

Figura 1: *Aprobación del Riesgo Residual*
Fuente: *Elaboración propia*

Este documento constituye solo un modelo, debiendo estar sujeto a la normativa de la institución y al tipo de documentación interna que se maneje.

Autorización de la Gerencia para futura implementación.

Se persigue garantizar la puesta en marcha del SGSI, con el compromiso del Órgano de Dirección de facilitar los recursos necesarios para la exitosa implementación de los controles propuestos. La propuesta sugiere que la autorización para la futura implementación del SGSI en la institución se podrá lograr si: (a) Se firma el “Enunciado de Aplicabilidad” por parte del Órgano de Dirección o la persona designada por éste. O en su defecto, (b) con la firma de una Resolución o Decreto puesta a disposición de todo el personal, se propone un modelo de Resolución tal como se muestra a continuación:



GOBIERNO REGIONAL LAMBAYEQUE

RESOLUCIÓN Nº - 2015 – GR. LAMB/GRED-UGEL-CHIC

Chiclayo, ……de…… de 2015.

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº……, se aprobó el uso obligatorio de la “Norma Técnica Peruana NTP – ISO/IEC 27001:2013. Tecnología de la Información. Código de buenas prácticas para la gestión de seguridad de la información en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de establecer un modelo integral para el desarrollo de los planes de seguridad de la información en la Administración Pública;

SE RESUELVE:

ARTÍCULO PRIMERO. - APROBAR la implementación del primer Sistema de Gestión de Seguridad de la Información de la Unidad de Gestión Educativa Local de Chiclayo.

ARTÍCULO SEGUNDO. - DISPONER que lo establecido es de cumplimiento obligatorio por los funcionarios y servidores de la UGEL Chiclayo.

ARTÍCULO TERCERO.- ENCARGAR la publicación de la presente Resolución, en el portal web de la Unidad de Gestión Educativa Local de Chiclayo (http://ugelchiclayo.regionlambayeque.gob.pe) y en el Portal de Transparencia.

Regístrese y comuníquese,

DRA. ZOILA URIARTE GONZÁLES
DIRECTORA DE LA UGEL CHICLAYO

Figura 2: *Modelo de resolución.*
Fuente: *Elaboración propia*

Redactar el enunciado de aplicabilidad.

Dentro de la documentación que exige la ISO/IEC 27001:2013 como parte del establecimiento de un SGSI, es la preparación de un enunciado de aplicabilidad.

La declaración de aplicabilidad o SoA, del inglés Statement of Applicability, es un documento que se referencia en el apartado 6.1.3. d) del estándar ISO/IEC 27001:2013, en el cual se describen aquellos objetivos de control y controles relevantes y aplicables al alcance del SGSI de la institución, en función de la política y conclusiones del proceso de análisis, evaluación y tratamiento de riesgos.

4. Discusión y Conclusiones

El diseño de un Sistema de Gestión de Seguridad de la Información permite mejorar la situación actual de la UGEL Chiclayo en materia de seguridad de la información, ya que la utilización de estándares internacionales y las buenas prácticas, repercuten directamente en una efectiva gestión de la información dentro de la institución, garantizando el cumplimiento de los principios básicos de seguridad: integridad, disponibilidad y confidencialidad.

No existe el interés adecuado en materia de seguridad de la información dentro de la UGEL Chiclayo, y se demuestra claramente en la falta de políticas, normas y controles de seguridad.

Se puede asegurar que la solución planteada en este trabajo de investigación, es decir con el diseño de un SGSI, es válida, ya que, a nivel mundial, muchas empresas adoptan estas metodologías, estándares y demás con muy buenos resultados, reiterando que todos ellos han sido elaborados por expertos en el rubro de la seguridad de la información o han sido desarrollados en base a buenas prácticas reconocidas y aprobadas internacionalmente por diversas organizaciones y la UGEL Chiclayo no podría ser la excepción.

Con un SGSI, se puede abordar efectivamente la implementación de un marco de gobierno de seguridad de la información y dar solución a diversos problemas como: (a) brindar un nivel aceptable de seguridad en relación a la información que la institución maneja, evitando posibles incidentes que afecten la operatividad diaria de la misma; y (b) contar con un modelo que se amolde al paso del tiempo y se pueda actualizar siempre, debido a las revisiones periódicas a las que está sujeto el SGSI.

Como en todas las organizaciones, el recurso humano es el activo más importante, al igual que la información, y es el que genera mayores complicaciones para un adecuado control. Por consiguiente, es imperativo que todo el personal, interno o externo, esté debidamente concienciado, capacitado y comprometido con la seguridad de la información, siendo de su conocimiento aquellas sanciones contractuales y legales en el caso de cometer acciones deliberadas que atenten contra la disponibilidad, integridad y confidencialidad de los activos de información.

Para poder identificar adecuadamente los activos con los que cuenta cualquier organización, es importante realizar un modelado de los procedimientos involucrados dentro del alcance del SGSI. Para lo cual, en la presente investigación, se procedió a diagramar los principales procedimientos de la UGEL Chiclayo, utilizando una notación BPMN con la herramienta Bizagi, la cual muestra de manera clara y concisa el flujo de actividades que se realizan en cada procedimiento.

De manera independiente de que la norma internacional ISO/IEC 27001:2013 proponga una serie de documentos estándar para tomar medidas preventivas y reactivas que resguarden y protejan la información, es la propia institución la que decide cómo manejar la seguridad de su información y qué métricas desea implementar, en base a lo que considera que es importante medir o evaluar.

Con el fin de cumplir con los parámetros establecidos por el estándar internacional ISO/IEC 27001:2013, para el análisis y evaluación de riesgos, y el alcance del SGSI de la UGEL Chiclayo, se analizaron diversas metodologías, optándose finalmente por desarrollar una propia que se ajustara de la

mejor manera. Esta metodología de riesgos establecida, así como la utilizada para valoración de activos, incorporan elementos comunes de otras existentes en la industria, tales como MAGERIT.

Un SGSI debe involucrar a todo el personal de la institución, desde el Nivel Gerencial hasta el operativo. Si no se cuenta con el apoyo del Órgano de Dirección, no se contará con el soporte necesario para lograr los objetivos del SGSI. Asimismo, si el personal de la UGEL Chiclayo, no sigue con las políticas y lineamientos propuestos de seguridad, no se obtendrá un nivel adecuado de seguridad de la información en los distintos procesos y procedimientos de la institución.

Para identificar los activos críticos de información de una institución, es necesario clasificarlos de acuerdo al tipo de activo al que pertenece, detallar quien es su propietario y la ubicación física o lógica en la que se encuentre. También es necesario valorizarlos de acuerdo a su nivel de importancia y la función que cumple dentro de la institución. Con ello, se puede definir los diferentes perfiles de amenazas y riesgos, y así proponer las respectivas salvaguardas para su protección, con el fin de minimizar los impactos que las amenazas identificadas pudieran causar.

No todos los controles y procedimientos de seguridad tienen validez para todos los casos, por lo que se deben seleccionar aquellos que permitan mitigar los riesgos y excluirse aquellos que no estén enfocados en el alcance del SGSI. La selección debe ser justificada sobre la base del análisis, evaluación y tratamiento de riesgos, declarándose todo en la redacción del Enunciado de Aplicabilidad, que forma parte de la documentación de ISO/IEC 27001:2013.

Toda la normativa relacionada con políticas, procedimientos, procesos y controles para mantener la confidencialidad, integridad, y disponibilidad de los activos de información de la UGEL Chiclayo, debe estar sujeta a la aprobación y total apoyo del Órgano de Dirección, quien verificará su cumplimiento.

La creación de un Comité de Seguridad de la Información es primordial en la implementación de un SGSI, ya que es el ente regulador de cualquier cambio dentro del sistema de gestión, y el responsable de la toma de decisiones en materia de seguridad. Asimismo, también es necesario la asignación de un Oficial de Seguridad de la Información, cuya función sea velar por el cumplimiento de las Políticas de Seguridad de la Información y mantener informado al Comité sobre la situación y avances actuales del SGSI tras su implementación.

La implementación de un SGSI no es un proceso de corto plazo, ya que se requiere de una serie de procesos y requisitos que debe cumplir la institución. El tiempo necesario para incorporar el SGSI está supeditado a diversos factores relacionados con el tamaño de la empresa, la situación actual con relación a la seguridad de la información, los recursos institucionales que se designan y a la naturaleza de sus funciones.

5. Referencias

Aguirre D. (2014). *Diseño de un Sistema de Gestión de Seguridad de la Información para Servicios Postales del Perú S.A.* (tesis de pregrado). Pontificia Universidad Católica del Perú.

Aguirre J. y C. Aristizabal. (2013). *Diseño del Sistema de Gestión de Seguridad de la Información para el grupo empresarial La Ofrenda*. (tesis de pregrado). Universidad Tecnológica de Pereira, Facultad de Ingenierías, Programa de Ingeniería de Sistemas y Computación Pereira.

Alexander G., Alberto. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información; Óptica ISO/ IEC 27001:2005*. Bogotá: Alfaomega Colombiana S.A.

Aliaga L. (2013). *Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo*. Tesis para optar por el título de Ingeniero Informático, Pontificia Universidad Católica del Perú.

Ampuero Chang, Carlos. (2011). *Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros.* (tesis de pregrado). Pontificia Universidad Católica del Perú.

Barrantes C. y H. Herrera. (2012). *Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos*. Tesis para optar el título de Ingeniero en Computación y Sistemas, Universidad de San Martín de Porres.

Buenaño J. y M. Granda. (2009). *Planeación y diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 270001-27002*. (tesis de pregrado). Universidad Politécnica Salesiana Sede Guayaquil.

COBIT 5.0, *Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Grupo ISACA, 2012.

Espinoza H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo*. (tesis de pregrado). Pontificia Universidad Católica del Perú.

Estándar Internacional ISO/IEC 27001:2013, Tecnología de la Información – Técnicas de Seguridad – Sistemas de la Seguridad de la Información – Requisitos. Segunda edición, versión en inglés, 2013.

Estándar Internacional ISO/IEC 27002:2013, Tecnología de la Información – Técnicas de Seguridad – Código de buenas prácticas para los controles de Seguridad de la Información. Segunda edición, versión en inglés, 2013.

Fernández, E. Moya, R. y M. Piattini (2003). *Seguridad de las tecnologías de la información*. La construcción de la confianza para una sociedad conectada. Madrid: AENOR.

Lara H., Reyes J. y W. Navarrete. (2006). *Diseño de Sistema de Gestión de Seguridad de Información para Ecuacolor*. Diplomado en Auditoría Informática, Escuela Superior Politécnica del Litoral.

Mujica M. (2007). *Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica “Antonio José de Sucre” Sede Rectoral*. (tesis de Maestría). Universidad Centro Occidental “Lisandro Alvarado”, 2007.

Ormella, C. (10 de agosto de 2014). *Gobierno de seguridad de la información*. “Gobierno corporativo” (2014): 1-6. Recuperado de: http://goo.gl/EVSHC5

Pallas G. (2009). *Metodología de implantación de un SGSI en un grupo empresarial jerárquico*. (tesis de Maestría). Instituto de Computación.

Ríos J. (2014). *Diseño de un Sistema de Gestión de Seguridad de la Información para una Central Privada de Información de Riesgos*. (tesis de pregrado). Pontificia Universidad Católica del Perú.

Sánchez A. (2013). *Diseño de un Sistema de Gestión de la Seguridad de la Información para Comercio Electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito*. (tesis de pregrado). Pontificia Universidad Católica del Ecuador.

Soluciones Integrales Itera. *¿Qué es el Gobierno de TI?*. (10 agosto, 2014). Recuperado de: http://goo.gl/O5mmeq

Tersek R. (2008). *Sistema de Gestión de Seguridad de la Información para un sistema de información (Caso de estudio: Sistema Administrativo Integrado SAI en la Red de datos de la UNEXPO – Puerto Ordaz)*. (tesis de Maestría). Universidad Centro Occidental “Lisandro Alvarado”.

Villena M. (2006). *Sistema de Gestión de Seguridad de Información para una Institución Financiera*. (tesis de pregrado). Pontificia Universidad Católica del Perú.