RILCO
Revista de Investigación Latinoamericana en Competitividad Organizacional

Año 2 Número 5
Febrero 2020
ISSN 2659-5494

# PROPUESTA DE UN MODELO DE UN SISTEMA DE GESTIÓN DE CALIDAD EN SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA INSTITUCIONES EDUCATIVAS

Dr. Juan Alberto Ruíz Tapia;
jart2005@gmail.com
Dr. César Enrique Estrada Gutiérrez;
ceeg1971@gmail.com
Dr. Ma. de la Luz Sánchez Paz;
maluspdra@gmail.com
Universidad Autónoma del Estado de México

Para citar este artículo puede utilizar el siguiente formato:

Juan Alberto Ruíz Tapia, César Enrique Estrada Gutiérrez y Ma. de la Luz Sánchez Paz (2020): "Propuesta de un Modelo de un Sistema de Gestión de Calidad en Seguridad de la Información basado en la norma ISO 27001 para Instituciones Educativas", Revista de Investigación Latinoamericana en Competitividad Organizacional RILCO, n. 5 (febrero 2020). En línea:
https://www.eumed.net/rev/rilco/05/gestion-instituciones.html
http://hdl.handle.net/20.500.11763/rilco05gestion-instituciones

**RESUMEN:**

Se pretende desarrollar un modelo de sistema de gestión de calidad en seguridad de la información aplicado a instituciones educativas basado en la norma ISO 27001. El objetivo es proponer un modelo general que facilite la implementación de un Sistema de Gestión de Calidad en Seguridad de la Información (SGCSI), en base a los objetivos de control de la norma ISO 27001 que serán la base para su desarrollo y así disminuir riesgos informáticos en instituciones educativas para prevenir pérdidas de información, financieras, problemas jurídicos, etc. Consiste en realizar un análisis de posibles riesgos identificando activos críticos, analizar la normatividad y los requisitos de la norma NTC ISO/IEC 2700:2005 que permitan proponer un modelo general que facilite la implementación de un SGCSI en este tipo de instituciones educativas.

Se plantea el problema en el cual se muestran los inconvenientes que actualmente tienen algunas instituciones educativas que no cuentan con un SGCSI implementado, se podrán identificar los diferentes riesgos que son causados por diversas prácticas dentro de esta instituciones y su tratamiento con el fin de poder minimizar el impacto negativo dentro de estas. Con esto se pretende aportar un modelo que contenga los objetivos del SGCSI a desarrollar y una propuesta tecnológica dentro del marco de referencia a partir del cual se logre medir las dimensiones del proyecto para poder aplicarlo a cualquier institución educativa con el objetivo de prevenir vulnerabilidades y amenazas sobre el sistema de seguridad.

La seguridad de la información es un aspecto esencial en las actividades y procesos de las instituciones de nivel superior y es de gran importancia implementar medidas de seguridad para mejorar su eficiencia. Se levantará y analizará la información para documentar los resultados correspondientes y finalmente generar propuesta para otras Universidades en situaciones similares.

**INTRODUCCIÓN.**

La seguridad de la información ya no puede ser vista como el resultado de acciones defensivas y reactivas, 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 que 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 la Institución; 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 Organización. Es por ello, que el presente trabajo de investigación tiene por objetivo fundamental proponer un modelo de Sistema de Gestión de Calidad en Seguridad de la Información para la Institución Educativa, basado en la norma internacional ISO/ 27001:2013.

**ANTECEDENTES Y JUSTIFICACIÓN.**

En los últimos años, el gran avance de las tecnologías de la información, así como el desarrollo de los mecanismos empleados para realizar comunicaciones, han logrado hacer que las personas tengan comodidad y rapidez teniendo en sus operaciones diarias un gran impacto en los procesos productivos y de servicios, pero también con estos adelantos tecnológicos han surgido riesgos a la seguridad de la información con la necesidad de proteger los sistemas de información tanto en software como en hardware y que se contrastan con la deficiente preparación con que las organizaciones adoptan la tecnología como elemento primordial para el desarrollo de sus actividades afectando con ello la integridad, confidencialidad y disponibilidad de su información.

Las instituciones educativas han insertado medidas de seguridad para proteger su información, pero en muchas ocasiones son insuficientes con lo que se ve en la necesidad de seguir normas para prevenir, medir, evaluar y corregir los posibles riesgos que puedan provocar daños irreversibles. Debido a esto, el SGCSI es una herramienta que permite proponer un plan para solucionar los problemas de la seguridad de su información mediante técnicas como analizar los riesgos, la mejora y el mantenimiento de su información a que está expuesta para lograr que su información no se pierda. Con la ayuda de estándares internacionales como la ISO 27001 un SGCSI está compuesto por una estructura organizacional de la institución educativa abarcando características como: tamaño, objetivos, tipo, procesos, requerimientos y personal especializado identificando posibles amenazas, impactos y vulnerabilidades

Por otro lado se ve que la implementación de un SGCSI en las instituciones que prestan el servicio educativo tiene asociados los siguientes beneficios:

• Metodología de riesgos que permite identificar y priorizar amenazas y riesgos del contexto educativo.
• Mejora continua.
• Disponibilidad del servicio educativo.
• Reducción de costos de incidentes.

• Cumplimiento de la legislación.
• Incremento de confianza de las partes interesadas.
• Mejora de la imagen institucional.
• Establecimiento e identificación de responsabilidades caracterizando las actividades relacionadas con la seguridad de la información.

**PLANTEAMIENTO DEL PROBLEMA.**

Algunas instituciones educativas no hacen un correcto uso y/o manejo de la información, esto facilita la exposición de la vulnerabilidad a terceros no autorizados, incluso la confidencial, ya que no tienen definida ninguna política de seguridad de la información. Dichas instituciones manejan un gran volumen de información como por ejemplo material de apoyo, datos, estadísticas y calificaciones que resultan vitales para llevar a cabo todos los procesos que se manejan a nivel interno. Por lo anterior se deben definir algunas políticas sobre la seguridad de la información dentro de las cuales es muy importante resaltar una política de riesgo, esta última elaborada en base a la guía de riesgos que implementa la ISO 31000, debido a que la información es almacenada en dispositivos tanto lógicos como físicos los cuales no se encuentran localizados de manera estratégica, permitiendo así que la información sea vulnerable y como consecuencia de ello se genere un alto riesgo sobre la seguridad de la misma.

Las principales causas de fallas presentadas en los sistemas y/o portales educativos son las amenazas y vulnerabilidad a nivel de software, hardware, desastres naturales e incluso el factor humano, ya sea por desconocimiento o por mala intención actuando sin ética y sin profesionalismo, utilizan distintas técnicas para atacar al sistema como por ejemplo denegación de servicio, puertas traseras, errores de programación, suplantación, acceso no autorizado a intrusos sobre la red informática o sobre los equipos de la institución educativa, generando un alto riesgo para la misma. Una de las principales consecuencias es el robo de información sensible y confidencial, lo cual puede ocasionar problemas legales que lleven al cierre de la institución educativa aunque sea sólidamente fuerte. La pérdida o mal uso de información confidencial genera daños y repercusiones relacionados con la confidencialidad, integridad y disponibilidad de los archivos de la institución y a su vez para el titular del documento, incluso pérdida de credibilidad por parte de sus estudiantes y comunidad educativa.

Se desarrollarán las políticas de seguridad con base en los riesgos identificados, tanto lógicos como físicos, que deben implementarse en las instituciones educativas con enfoque en niveles académicos básica y media, con el fin de proteger la red informática y salvaguardar la información, garantizando la confidencialidad, integridad, disponibilidad y autenticidad de la misma, esto le permitirá a la institución educativa llevar un correcto funcionamiento de su información interna y externa. El desarrollo de estas políticas de seguridad estará apoyado de un sistema de gestión de calidad de la seguridad de la información (SGCSI) que facilitará su implementación en cada institución educativa. Este SGCSI se realizará a través del ciclo Deming y en base a la norma ISO 31000 para la gestión del riesgo. Esta norma recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de referencia cuyo propósito sea integrar el proceso para la gestión del riesgo en los procesos globales de gobierno, estrategia y planificación, gestión, procesos de presentación de informes, políticas, valores y cultura de la organización. La gestión del riesgo se puede aplicar a toda la organización, en todas sus diferentes áreas y niveles, en cualquier momento, así como a funciones, proyectos y actividades específicos.

**PREGUNTA DE INVESTIGACIÓN.**

¿Cuál será el Modelo de un Sistema Integrado de Calidad en Seguridad de la Información basado en la norma ISO 27001 para Instituciones Educativas?

Al terminar esta investigación se plasmará una propuesta en un documento que permitirá al personal de las instituciones educativas la implementación de los controles de seguridad que se llevará a cabo al interior de la Institución educativa para proteger la información y su red informática, obteniendo así una mejora integral en la calidad de los productos y servicios de la institución educativa en base a lo establecido en la norma ISO 27001:2005.

**DELIMITACIÓN.**

El modelo de SGCSI se enfocará únicamente en las instituciones educativas de tres países latinoamericanos: Brasil, Ecuador y Nicaragua, además de 4 instituciones educativas del Estado de México, donde se desea mejorar el esquema de seguridad que tienen implementado en cuanto a la información que manejan.

**OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS:**

OBJETIVO GENERAL

Analizar, desarrollar y proponer un modelo de Sistema de Gestión de Calidad en Seguridad de la Información basado en la norma ISO 27001 para Instituciones Educativas (SGCSI) que facilite la identificación de los riesgos en la seguridad de la información en instituciones educativas de Educación Superior.

OBJETIVOS ESPECÍFICOS

- Identificar un marco teórico pertinente para el estudio del ISO 27001 en ambientes universitarios.
- Determinar las principales características que afectan el desempeño de un SGCSI en universidades.
- Analizar las características y medidas de seguridad de la información que actualmente maneja las instituciones educativas.
- Analizar los riesgos que se presentan sobre las medidas de seguridad haciendo uso de la norma ISO 31000.
- Definir políticas y controles de seguridad para las instituciones educativas con la norma ISO/IEC 27001.
- Implementar una guía modelo que permita exponer la propuesta SGCSI desarrollada.
- Realizar un estudio comparativo entre países y universidades latinoamericanas.

- Realizar un diagnóstico estratégico para hallar las fortalezas, debilidades y oportunidades de mejora.
- Diseñar un plan de acción que permita la puesta en marcha del Modelo de un Sistema de Gestión de Calidad en Seguridad de la Información basado en la norma ISO 27001 para Instituciones Educativas con acciones y estrategias que posibiliten un mejoramiento continuo de los procesos.
- Documentar el sistema el cual contendrá el modelo como recurso fundamental para la gestión del mismo.

**ALCANCES Y METAS.**

El alcance de la investigación se basa en el estudio de la identificación de las fortalezas, amenazas, oportunidades y debilidades de algunas Instituciones educativas, así como realizar estudios comparativos en universidades latinoamericanas y a partir de esta información desarrollar un modelo y metodología aplicables para estas universidades.

Las metas se dan en cada una de las etapas e incluyen el levantamiento en tres de los diferentes países con los que cuenta la Red de Investigación Latinoamericana en Competitividad Organizacional (RILCO) así como en cuatro Instituciones educativas en el Estado de México y dentro de estos entornos se generarán levantamientos con instrumentos cuantitativos que faciliten el análisis objetivo de datos y conclusiones que puedan reflejar la situación general de los objetivos de esta investigación.

Adicionalmente se realiza un reporte de investigación exclusivamente de la realidad local para con esto poder generar propuestas que puedan ser transmitidas y presentadas a tomadores de decisiones de las universidades participantes en cada región. De esta manera el modelo propuesto local en coordinación con las regiones latinoamericanas permitirá la relación entre los diferentes miembros de la red al generar la aplicación de este modelo con estudios comparativos entre regiones que sea pertinentes comparar, por la situación socio-demográfica, económica, etc.

**MARCO TEÓRICO.**

La presente investigación toma entre otras referencias de apoyo, la monografía llamada: *"Protocolo de políticas de seguridad informática para las universidades desarrollada en la Universidad Católica de Pereira"*. Esta investigación desarrolla la una temática similar a la de este trabajo y se apoyará en temas como:

- Identificación de las principales debilidades de los sistemas enfocados a la educación.
- Normatividad actual de estandarización según Norma ISO 27000.
- Identificación de debilidades como lo son encuestas y entrevistas.
- Elaboración de procesos normativos para el desempeño del SGCSI.
- Difusión de conceptos de seguridad informática al personal tanto administrativo como académico.

En las instituciones de educación superior se ha encontrado que no se le da la importancia necesaria a la seguridad informática, ya que según estudios realizados mediante pláticas y entrevistas en diferentes universidades, se puede conocer que son muy pocas las que tienen algún indicio de seguridad y aquellas que la tienen se encuentran en proceso de implementación, igualmente se comenta que no se están guiando por metodologías, técnicas o normas de seguridad estandarizadas y con aplicación específica al entorno académico, si no con una mezcla, la cual no asegura un buen proceso final.

De igual manera se puede considerar que probablemente los usuarios tanto administrativos como académicos no tienen un gran conocimiento sobre seguridad informática. También se piensa que en las instituciones donde tienen un mínimo de seguridad en la parte de sistemas no tienen claro el concepto del mismo, ni hay una difusión a los usuarios sobre las políticas de seguridad establecidas.

Por esta razón se realizará un modelo basado en la norma ISO 27000, entendiendo que la seguridad tiene una parte muy importante que es la evaluación y análisis de riesgos y

así se presenta la propuesta de que un modelo de seguridad puede ser aplicado en las instituciones de educación superior, lo cual permite guiar y facilitar su implementación garantizando una disponibilidad, integridad y seguridad de la información en un porcentaje muy alto de aplicación y protección.

Un SGCSI es una parte del sistema de gestión de una organización, basado en una aproximación a los riesgos del negocio, que permite establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización. Algunos componentes esenciales de un sistema son los siguientes:

- Estructura organizativa.
- Políticas.
- Planificación.
- Responsabilidades definidas.
- Buenas prácticas.
- Procedimientos de actuación.
- Procesos de gestión.
- Recursos suficientes.

Hay que darse cuenta de que la creación de un SGCSI es una decisión estratégica de la organización y debe ser apoyada y supervisada por la dirección. Su implementación dependerá de los objetivos establecidos, los requisitos de seguridad, los procesos involucrados y la propia estructura de la organización.

Otras definiciones relacionadas con ISO 27001:2005 son las siguientes:
Un Sistema de Gestión de Seguridad de la Información está basado en el ciclo de Deming que ha adoptado esta norma como otras (ISO 9000 e ISO 14000) y que está basado en cuatro fases denominadas como Plan, Do, Check, Act, (PDCA). Este ciclo permite la mejora continua de la seguridad de la información dentro de la organización apoyándose en el sistema de gestión como soporte para dicha mejora.

Este Sistema de Gestión, como todo, tiene un principio y es en su construcción donde se hace hincapié en la primera auditoría. Esto permite a la organización mejorar su seguridad de la información, consiguiendo que la organización vaya poniendo el término Seguridad de la Información junto al de Sistema de Gestión.

**NORMA ISO 27001.**

El estándar ISO 27001:2005 establece todos los requisitos necesarios a la hora de implementar un Sistema de Gestión de Seguridad de la Información (SGCSI) en cualquier tipo de empresa. La parte más importante de una empresa es la información. La organización debe contar con otro tipo de activos que también tengan una destacada importancia, pero si la organización tiene algún problema en la seguridad de la información, ésta no podrá recuperarla. Esa es la principal razón por la que las organizaciones deben dedicar parte de su esfuerzo en garantizar la seguridad de la información corporativa.

Normalmente, la gestión de la Seguridad de la Información en una organización se encuentra desorganizada, por lo que no cuenta con un criterio común, es decir, cada departamento de la organización cuenta con sus propios procedimientos y políticas, que han sido constituidas sin contar con las necesidades generales de la organización e incluso podemos hablar de que se encuentran alejadas de sus objetivos.

Implementar un Sistema de Gestión en Seguridad de la Información (SGCSI) basado en la norma ISO 27001:2005 es la manera más eficiente de poder conseguir la coordinación y gestión necesaria para alcanzar los objetivos de la organización y además puede conseguir que la organización salga mucho más reforzada.

Un SGCSI según la ISO 27001 genera una garantía con la que sabemos que se puede realizar una adecuada gestión de la seguridad de la información en la organización. Para ello, se debe realizar un tratamiento según los diferentes niveles de riesgos cosechados como consecuencia de considerar los distintos efectos que se pueden producir sobre la información de la organización. El SGCSI según la norma ISO-27001 genera un proceso de mejora continua y de gran flexibilidad frente a los cambios que se pueden

producir en la empresa refiriéndonos a los procesos de negocio y a la tecnología, ya que ésta avanza a una gran velocidad.

El SGCSI se basa en tres pilares fundamentales:

- Confidencialidad: es la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin.
- Integridad: es la preservación de la información completa y exacta.
- Disponibilidad: es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

El Sistema de Gestión de Seguridad de la Información tiene que tener en cuenta estos tres pilares fundamentales para realizar el tratamiento de los riesgos de la organización ya que la implementación de los controles de seguridad son los activos de la organización.

**SEGURIDAD DE INFORMACIÓN EN LA FAMILIA ISO/IEC 27000.**

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie de norma contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGCSI), estas normas incluyen:

1. ISO/IEC 27000- es un vocabulario estándar para el SGCSI. Se encuentra en desarrollo actualmente.
2. ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGCSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
3. ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC

17799. Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.

4. ISO/IEC 27003 - son directrices para la implementación de un SGCSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.

5. ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.

6. ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información con sus anexos;

- Anexo A: Definición del alcance del proceso.
- Anexo B: Valoración de activos y evaluación de impacto.
- Anexo C: Ejemplos de amenazas típicas.
- Anexo D: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad.

7. ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGCSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.

8. ISO/IEC 27007 - Es una guía para auditar al SGCSI. Se encuentra en preparación.

9. ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.

10. ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este estándar hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO

27001, en su segunda cláusula, en términos de “documento indispensable para la aplicación de este documento” y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares. Implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 es la manera más eficiente de poder conseguir la coordinación y gestión necesaria para alcanzar los objetivos de la organización y además puede conseguir que la organización salga mucho más reforzada.

Los anteriores son solo estudios en los que se basa la presente investigación para el desarrollo y el manejo del análisis para obtener los resultados esperados.

**GUÍA DE SEGURIDAD INFORMÁTICA.**

Para el desarrollo de la guía en cuestión, se toman de referencia 5 dominios, los cuales se relacionan directamente con el área informática:

6.- Organización de la seguridad de la información.
7. Gestión de Activos.
8. Seguridad de los recursos humanos
9. Seguridad física y ambiental
10. Gestión de Comunicaciones y Operaciones.
11. Control de Acceso.
12. Adquisición, Desarrollo y Mantenimiento De Sistemas de Información.
13. Gestión de Incidentes en la Seguridad de la Información.
14. Gestión de la continuidad educativa
15. Cumplimiento.

**CONTENIDO DE LA NORMA.**

11 dominios, 39 objetivos de control y 133 controles

Los 133 controles y 39 objetivos están agrupados dentro de los 11 dominios descritos enseguida:

A5. Política De Seguridad: El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.

A6. Aspectos Organizativos de La Seguridad de la Información: La gerencia debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.

A7. Gestión de Activos: Inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial.

A8. Seguridad Ligada a los Recursos Humanos: Los roles y responsabilidades de la seguridad debieran ser definidos y claramente comunicados a los candidatos para el puesto durante el proceso de pre-empleo.

A9. Seguridad Física y del Entorno: Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

A10. Gestión de Comunicaciones y Operaciones: Procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación; tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad.

A11. Control de Acceso: Establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.

A12. Adquisición, Desarrollo y Mantenimiento De Sistemas de Información: Identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

A13. Gestión de Incidentes en la Seguridad de la Información: Procedimientos formales de reporte y de la intensificación de un evento, ejemplo: cambios del sistema no controlados, mal funcionamiento del software o hardware, violaciones de acceso.

A14. Gestión de la Continuidad del Negocio: Desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.

A15. Cumplimiento: Definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes, y el enfoque de la

organización para satisfacer esos requerimientos, para cada sistema de información y la organización.

## METODOLOGÍA.

A. UNIVERSO Y MUESTRA

El estudio se restringe a tres universidades de países latinoamericanos y cuatro Instituciones educativas en el Estado de México en los diferentes departamentos de Tecnologías de Información (TI), para recopilar información entre académicos, estudiantes y administrativos. Dicho estudio es de interés compartido en la red RILCO y por tanto se realiza de manera simultánea con diversos levantamientos y análisis de información local, para generar estudios comparativos y resultados en las universidades participantes. Lo anterior puede incluir un segundo estudio en las regiones previstas por este trabajo por lo que en cada una se sugiera implementar el modelo.

## DISEÑO GENERAL DE LA INVESTIGACIÓN.

Con el presente trabajo se lleva cabo una investigación con diseño cuantitativo, descriptivo, no experimental y transversal, generando investigaciones documentales y principalmente de campo.

## DESCRIPCIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES.

Las variables para este estudio están basados en la Norma ISO 27005. En base a lo anterior podemos identificar las dimensiones que pueden explicar el modelo a seguir:

La variable dependiente esta manifestada por:

Sistemas Integrados de Calidad en Seguridad de la Información universitaria

Las variables independientes están dadas por:

- Controles de acceso de la Norma según los anexos A, B, C y D de la misma norma.
- Tecnologías educativas.

A su vez con cada una de estas se identifican las características que definen los controles escolares educativos.

El estudio es descriptivo. La población y muestra está compuesta por personal involucrado en las Instituciones de educación superior. Para la recolección de datos se utilizaron técnicas como el análisis de documentos, encuestas a personal y algunas entrevistas; los formatos utilizados fueron cuestionarios.

**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, Encargados de Sistemas de Información, siendo su opinión y experiencia muy importantes, por estar involucrado de manera directa con la gestión de la información; *encuestas* donde los participantes evaluaron la situación actual de la institución frente a la seguridad de la información. 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.

El cuestionario fue respondido por algunas personas, entre los cuales respondieron los Directivos, los Encargados de TICs, profesores o encargados de Control Escolar. Fue elaborado en base a la Norma ISO 27001 y tiene la finalidad de saber cómo está en la institución Educativa encuestada. Se realiza con el objetivo de analizar los riesgos informáticos con los que actualmente estas instituciones tienen que convivir y así puedan prevenir pérdidas de información, financieras, problemas jurídicos, entre otras.

La tarea consiste en realizar un análisis del cuestionario respondido basado en los probables riesgos identificando los activos críticos de la institución educativa en los diferentes departamentos de Tecnologías de Información (TI) y los probables riesgos asociados.

Adicionalmente, se elabora un dictamen de tratamiento de probables riesgos que permiten proponer medidas que faciliten la implementación de algunos controles en cada institución educativa. Se expone el problema en el cual se ponen de evidencia los

inconvenientes que actualmente tiene la institución educativa por no contar con un Sistema de Gestión de Calidad en Seguridad de la Información (SGCSI) implementado.

Se propone una posible sugerencia o solución tecnológica. Se identifican los posibles riesgos que se pueden causar por diversas acciones dentro de las instituciones educativas y el tratamiento de cada una con el fin de poder minimizar el impacto negativo dentro de estas con el objetivo de prevenir vulnerabilidades y amenazas sobre el sistema de seguridad.

La importancia del SGCSI permite determinar los objetivos, procesos y procedimientos para el establecimiento de políticas y controles de seguridad que ayudarán a evitar los riesgos en la seguridad de la información que manejan en las Instituciones de Educación Superior.

Un SGCSI permite mejorar la situación actual que vive la Institución Educativa 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.

## MATERIALES Y MÉTODOS.

Dentro de esta investigación de tipo descriptiva aplicada, se utilizan 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:

Las Variables y dimensiones son:

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 Operación, Seguridad en las Telecomunicaciones.

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 Institución Educativa que está directamente relacionada con los problemas detectados en la investigación preliminar. Entre los puntos principales están los siguientes:

A.6 Oganización de la seguridad de la información

A.6.1 Organización interna.- Objetivo: Manejar la seguridad de la información dentro de la Institución.

A.6.2 Entidades externas.- Objetivo: Mantener la seguridad de la información de la Institución y los medios de procesamiento de información a los cuales las entidades externas tienen acceso y procesan; o son comunicados o manejados por entidades externas.

A.7 Gestión de activos.

A.7.1 Responsabilidad por los activos.- Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.

A.7.2 Clasificación de la información.- Objetivo: Asegurar que la información reciba un nivel de protección apropiado.

A.8 Seguridad de los recursos humanos

A.8.1 Antes del empleo.- Objetivo: Asegurar que los alumnos, profesores, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.

A.8.2 Durante el empleo.- Objetivo: Asegurar que todos los alumnos y profesores, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad Institucional en el curso de su trabajo normal, y reducir los riesgos de error humano.

A.8.3 Terminación o cambio del empleo.- Objetivo: Asegurar que los alumnos y profesores, contratistas y terceros salgan de la Institución o cambien de empleo de una manera ordenada.

A.9 Seguridad física y ambiental

A.9.1 Áreas seguras.- Objetivo: Evitar el acceso físico no autorizado, daño e

interferencia al local y la información de la Institución.

A.9.2 Seguridad del equipo.- Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la Institución.

A.10 Gestión de las comunicaciones y operaciones

A.10.1 Procedimientos y responsabilidades operacionales.- Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información

A.10.2 Gestión de la entrega del servicio de terceros.- Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.

A.10.3 Planeación y aceptación del sistema.- Objetivo: Minimizar el riesgo de fallas en los sistemas.

A.10.4 Protección contra software malicioso y código móvil.- Objetivo: Proteger la integridad del software y la información.

A.10.5 Respaldo (back-up.- Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.

A.10.6 Gestión de seguridad de redes.- Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

A.10.7 Gestión de medios.- Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.

A.10.8 Intercambio de información.- Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.

A.10.9 Servicios de comercio electrónico.- Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.

A.10.10 Monitoreo.- Objetivo: Detectar actividades de procesamiento de información no autorizadas.

A.11 Control de acceso.-

A.11.1 Requerimiento comercial para el control del acceso.- Objetivo: Controlar acceso a la información

A.11.2 Gestión del acceso del usuario.- Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.

A.11.3 Responsabilidades del usuario.- Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.

A.11.4 Control de acceso a redes.- Objetivo: Evitar el acceso no-autorizado a los servicios en red.

A.11.5 Control de acceso al sistema de operación.- Objetivo: Evitar acceso no autorizado a los sistemas operativos.

A.11.6 Control de acceso a la aplicación e información.- Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

A.11.7 Computación móvil y tele-trabajo.- Objetivo: Asegurar la seguridad de la información cuando se utilice medios de computación móvil y tele-trabajo.

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información.

A.12.1 Requerimientos de seguridad de los sistemas.- Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.

A.12.2 Procesamiento correcto en las aplicaciones.- Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.

A.12.3 Controles criptográficos.- Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.

A.12.4 Seguridad de los archivos del sistema.- Objetivo: Garantizar la seguridad de los archivos del sistema

A.12.5 Seguridad en los procesos de desarrollo y soporte.- Objetivo: Mantener la seguridad del software e información del sistema de aplicación.

A.12.6 Gestión de vulnerabilidad técnica.- Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

A.13 Gestión de incidentes en la seguridad de la información

A.13.1 Reporte de eventos y debilidades en la seguridad de la información.- Objetivo: Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información ya sea comunicada de una manera que permita tomar una acción correctiva oportuna.

A.14 Gestión de la continuidad comercial

A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial.- Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres

importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

A.15 Cumplimiento

A.15.1 Cumplimiento con requerimientos legales.- Objetivo: Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.

A.15.2 Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico.- Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

A.15.3 Consideraciones de auditoría de los sistemas de información.- Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoría de los sistemas de información.

**RESULTADOS.**

El análisis de los resultados obtenidos, tras la aplicación de los cuestionarios, permitirá identificar, analizar y diagnosticar una serie de factores que condicionan la seguridad de la información en la Institución Educativa.

Se puede analizar que no existe un gran interés en materia de seguridad de la información dentro de algunas Instituciones educativas, y se observa en la falta de políticas, normas y controles de seguridad.

Se adoptó la norma ISO/IEC 27001:2013, en el diseño del SGCSI, como estrategia de mejora. Esta norma internacional, proporciona 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.

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.

## DISCUSIÓN Y CONCLUSIONES.

El diseño de un Sistema de Gestión de la Calidad en Seguridad de la Información permite mejorar la situación actual de la Institución educativa 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.

Se pretende que el avance en la solución propuesta en este trabajo de investigación con el diseño de un SGCSI, sea válida, ya que muchas Organizaciones adoptan esas metodologías y estándares con muy buenos resultados. Todo esto ha sido elaborado 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 privadas ó públicas y la Institución educativa no podría ser la excepción.

Con un SGCSI, 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 adapte en la actualidad y se pueda actualizar siempre, debido a las revisiones periódicas a las que está sujeto el SGCSI.

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 importante que todo el personal, interno o externo, esté debidamente concientizado, 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.

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 debe decidir cómo manejar la seguridad de su información y qué controles 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 SGCSI de la Institución educativa, se analizan diversas metodologías, optándose finalmente por desarrollar una propia que se ajuste 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.

Un SGCSI debe involucrar a todo el personal de la institución, desde el Nivel Gerencial hasta el operativo. Si no se cuenta con el apoyo de la Dirección, no se contará con el soporte necesario para lograr los objetivos del SGCSI. Asimismo, si el personal de la Institución educativa, 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 las Instituciones Educativas, por lo que se deben seleccionar aquellos que permitan mitigar los riesgos y excluirse aquellos que no estén enfocados en el alcance del SGCSI. 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 Institución Educativa, 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 SGCSI, 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 necesaria la asignación de un Responsable de la 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 SGCSI tras su implementación.

La implementación de un SGCSI 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 SGCSI 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.

**AVANCE DE LA NUEVA PROPUESTA O CONTINUIDAD.**

Esta investigación es de nueva creación y se desarrolla debido a la propuesta de integrantes del Cuerpo Académico: “Administración de Organizaciones Educativas” realizado en la reunión anual de la Red de Investigación Latinoamericana en Competitividad Organizacional (RILCO), de la cual somos integrantes.

Se envió el cuestionario para conocer el medio ambiente que rodea a cada Institución Educativa. Actualmente, se recibió la información de Universidades de Brasil, Ecuador, Nicaragua y de 4 Instituciones educativas del Estado de México, misma que se está identificando, analizando y diagnosticando. Una vez concluida la presente investigación,

se desarrollará el modelo y metodología para que se pueda utilizar en las universidades, lo cual requiere del precedente de esta investigación para poder proponer una mejor manera de tener seguridad en la información.

## REFERENCIAS BIBLIOGRÁFICAS Y HEMEROGRÁFICAS.


Project Management Institute (PMI) (2016). A Guide to the Project Management Body of Knowledge (PMBoK Guide). Philadelphia, Pennsylvania: PMI.

Tackling ISO 27001: A Project to Build an ISMS. SANS Institute InfoSec Reading Room. (Disponible en Internet: http://www.sans.org/reading_room/whitepapers/leadership/tackling-iso-27001- project-build-isms_33169.

Directrices de la OCDE para la Seguridad del Información: Hacia una cultura de seguridad. OCDE, 2017. (Disponible en Internet: http://www.oecd.org/dataoecd/15/29/34912912.pdf.

Norma UNE-EN ISO 27001:2005. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).

Norma UNE-EN ISO 27002:2009. Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.

Norma UNE-EN ISO 19011:2012 Directrices para la auditoría de los sistemas de gestión.

Método MAGERIT. (Disponible en Internet: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P8002922512 93651550991&langPae=es&detalleLista=PAE_1276529683497133.

Esquema Nacional de Seguridad (Disponible en Internet: http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

Guías STIC Serie 800 (Disponible en Internet: https://www.ccncert.cni.es/index.php?option=com_content&view=article&id=2420&Itemid=211&lang=es.

Portal ISO 27000 en español: http://www.iso27000.es.

International Organization for Standarization (ISO): http://www.iso.org/iso/home.html

International Register of Certificated Auditors (IRCA): http://spain.irca.org/auditorcert.html

Information Systems Audit and Control Association (ISACA): http://www.isaca.org/Certification/CISA-Certified-Information-SystemsAuditor/Pages/default.aspx

SANS Institute: www.sans.org/. ¬ Entidad Nacional de Acreditación (ENAC): http://www.enac.es. ¬ Centro Criptológico Nacional (CCN): https://www.ccn.cni/ ¬ Capacidad de Respuesta a Incidentes de Seguridad de la Información (CCNCERT) https://www.ccn-cert.cni.es/.

https://es.scribd.com/doc/124454177/ISO-27005-espanol