MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE APROVECHAMIENTO ESTUDIANTIL EN LA EDUCACIÓN GENERAL BÁSICA BASADO EN LA NORMA ISO 27002.

Magíster en Auditoría de Tecnologías de la Información

Por el Estudiante:
Luis Angel Pacheco Alvarado

Bajo la dirección de:
Rubén Antonio Pacheco Villamar

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador

Junio 2018

Políticas de Seguridad de la Información de aprovechamiento estudiantil en la EGB.

Information Security Policies for student achievement in the EGB

Luis Angel PACHECO ALVARADO[1]

Resumen

Dentro de la organización educativa actual, en donde se utilizan las tecnologías de la información y comunicación, las seguridades informáticas son un pilar fundamental para la estabilidad de la actividad institucional, especialmente por sus procesos inherentes a la información de los estudiantes. Ante este fenómeno, la información se ha convertido en uno de los activos más valiosos de toda institución educativa, lo que hace necesario elaborar Políticas de Seguridad de la Información de aprovechamiento estudiantil, en este caso, a través de la Norma ISO 27002 y la metodología de análisis de riesgo MAGERIT**,** que contribuyen a la clasificación de los activos de información y la disminución de falencias, amenazas y riesgos de la pérdida de información. En tal sentido, se realizó una investigación descriptiva en la escuela Zulima Vaca Rivera de la ciudad de Pasaje, para caracterizar las estrategias que utilizan con respecto a la confiabilidad, integridad y disponibilidad de los activos de información del proceso educativo. Se realizaron encuestas y entrevistas a docentes, estudiantes y autoridades, y se propuso un conjunto de políticas. Se arribó a la conclusión de que existen limitaciones de carácter subjetivo y objetivo que interfieren en el no uso de Políticas de Seguridad de la Información.

Palabras clave: Política de Seguridad, Seguridad de la Información, Normas ISO 27002, Metodología Magerit.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo-Ecuador, E-mail lupacheco@uees.edu.ec

Abstract

Within the educational organization where information and communication technologies are involved, computer security is a fundamental pillar for the stability of institutional activity, especially due to the processes inherent to student information. Faced with this phenomenon, information has become one of the most valuable assets of any educational institution, which makes it necessary to develop Information Security Policies for student achievement, for example, through ISO 27002 and the MAGERIT risk analysis methodology. This approach contributes to the classification of information assets and the reduction of shortcomings, threats and risks of information loss. In this sense, a descriptive investigation was conducted at the Zulima Vaca Rivera school in the city of Pasaje, to characterize the strategies they use with respect to the reliability, integrity and availability of the information assets of the educational process. Surveys and interviews were conducted with teachers, students and authorities, and, a group of security policies were developed and proposed. It was concluded that there are limitations of a subjective and objective nature that interfere in the non-use of Information Security Policies.

Key words | Security Policy, Information Security, ISO 27002 Standards, Magerit Methodology.

INTRODUCCIÓN

Los avances en la tecnología impulsan cambios en los mecanismos de defensa contra las amenazas a la seguridad de la información. Cualquier entidad pública o privada, y entre ellas, las instituciones educativas se encuentran en un proceso de cambio en lo que representa la cultura de la seguridad de la información, debido a que sus actividades están soportadas en tecnologías de la información y de la comunicación, por lo que necesitan dotar a su sistema e infraestructura, de medidas de protección que garanticen el desarrollo y sostenibilidad de su actividad.

La (PwC, 2017, p 1), indica en una encuesta realizada a nivel mundial de la Seguridad de la Información, que la causa que hace que las empresas o instituciones inviertan en ciberseguridad, se da en torno a los procesos de digitalización de los negocios, empresas e instituciones en general. Todo esto ha derivado en la transformación digital.

La (Asamblea Nacional Constituyente de Ecuador, 2008, p 175) , establece en el Art. 389 la necesidad de "Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión", obligación que, en las instituciones educativas, realmente no se cumple o se cumple de manera muy incompleta en la actualidad, en parte, por poco presupuesto, y en parte, por desconocimiento de las medidas de seguridad por parte de la comunidad educativa.

Por otro lado, los procesos y tareas, en los que se maneja información en el entorno educativo, tales como: el acceso a las distintas plataformas de Gestión de Control Escolar y Administración Docente, el uso del correo institucional y el acceso a internet, se hacen más frecuentes y necesarios, y la exposición se incrementa, por lo que se

encuentran más propensos a amenazas de alteración, divulgación no autorizada y sustracción. El riesgo se materializa incrementando el peligro de ataques que provengan desde la Internet o desde el interior del propio entorno educativo.

Por lo anterior, las instituciones educativas en Ecuador empiezan a adquirir conciencia de que es imperativo y urgente poner manos a la obra en lo que a seguridad se refiere. En este sentido, en algunas instituciones como la Escuela de Educación General Básica "Zulima Vaca Rivera" de la ciudad de Pasaje, se ha tomado la iniciativa para posicionarla como una de las primeras gestoras de proyectos de Seguridad de la Información (S.I.) entre las instituciones educativas de nivel primario de la Provincia de El Oro.

El objetivo principal de esta investigación es diseñar, elaborar y aplicar Políticas de Seguridad de la Información, a través de la metodología MAGERIT y la Norma ISO 27002 para la gestión del riesgo**,** con el fin de asegurar el cumplimiento de uno de los requerimientos de S.I., el del servicio de integridad de la información de aprovechamiento del servicio de gestión estudiantil.

Para cumplir con el objetivo se requiere contar con algunos insumos, tales como: un inventario de procesos, una clasificación de los datos desde el punto de vista de la seguridad, un inventario de la infraestructura de TI, etc. Una de las cosas que se detectó desde el principio, era la falta de un análisis de riesgos, lo que a su vez, ha provocado la ausencia de políticas o normas que garanticen la disponibilidad, integridad y confiabilidad de la información, lo que en su turno, ha derivado en la falta de formación y capacitación en el uso de estrategias de seguridad y hábitos seguros, por parte de estudiantes y docentes, en la ausencia de un inventario de seguridad dela información, que identifique responsabilidades y

responsables de los activos de la información, así como, en la falta de control en el acceso a los equipos de cómputo y servicios tecnológicos.

A medida que el trabajo de esta investigación avanzaba, el trabajo se orientó al ámbito de la seguridad y las causas por las cuales la integridad de la información está amenazada, finalmente la investigación se enfocó en utilizar las Políticas de Seguridad de la Información que recomienda la Norma ISO /IEC 27002.

La investigación tiene un enfoque cualitativo – descriptivo, para tener una mejor comprensión, análisis e interpretación de la realidad de los procesos y de la realidad social de los sujetos investigados, a la vez que presenta una propuesta alternativa de transformación en el contexto educativo. El utilizar la investigación cualitativa nos permitió establecer con precisión estándares más adecuados de comportamiento en seguridad de la información de la población en el entorno educativo escogido y de acurdo a sus características específicas.

MARCO TEÓRICO

1. 1 Seguridad de la Información en la Educación General Básica

La calidad de la Educación General Básica depende en cierta medida de las estrategias y medidas de Seguridad de la Información, ya que es a través de ella que se protege los activos de información de la institución educativa. El origen de la importancia de la Seguridad de la Información nace a finales del siglo XX (Tzu, 1972, p 5), aunque es mencionada de manera directa o indirecta, en obras antiguas como el libro El arte de la guerra, y en la obra de Nicolás Maquiavelo, en los que se discurre sobre la importancia de la seguridad de la información en los contextos de la política, los negocios, los deportes y las guerras, donde se constituye en una ventaja

el contar con el conocimiento previo, es decir, con la información, de ahí el riesgo de que se permeabilice a los adversarios para la toma de decisiones que podrían perjudicar a uno de los lados de la contienda, demostrándose así el valor que tiene la protección de la información.

En obras más recientes, ya en el siglo XXI, como por ejemplo, en (Borghello, 2001, p 10), se manifiesta que la seguridad de la información permite garantizar el material y los recursos tecnológicos de toda institución, es así que proteger a la información toma un sentido crucial y más aún cuando nos referimos al entorno educativo, enmarcando a la seguridad en tres principios fundamentales como es la confidencialidad, integridad y disponibilidad, para ofrecer servicios que permitan la gestión del control académico y administrativo de manera oportuna, confiable y segura.

La (ISO/ IEC JTC 1, 2005, p 14), establece otros principios de seguridad de la información que se pueden también involucrar en la investigación, tales como los servicios de autenticidad, responsabilidad, no repudiación y confiabilidad de la información, esto debido a que la seguridad de la información está relacionada con medidas preventivas con el fin de salvaguardar y proteger la información, considerando que la información que se quiere proteger se presenta tanto en formato físico como electrónico.

En el contexto educativo, la información es considerada como uno de los activos más valiosos; esto debido a la creciente necesidad de la interconexión requerida en prácticamente todos los aspectos de la labor educativa, por lo que dicha labor se encuentra expuesta a amenazas y vulnerabilidades, es así que toma mucha importancia proteger adecuadamente la información, la misma que se puede encontrar en formato impreso, escrita en papel, almacenada electrónicamente,

transmitida por correo, o utilizando medios electrónicos como películas o audios de conversaciones.

En este sentido, (Velasco, 2008, p 337), considera a la seguridad de la información como: la aplicación de un conjunto de medidas de orden físico y lógico a los sistemas de información, para de esta manera evitar la pérdida de la misma, siendo ésta una tarea de responsabilidad exclusiva de los departamentos de informática de las instituciones, pero hay problemas de seguridad de la información que pueden provenir desde la parte externa o interna, por incidentes relacionados con el propio personal de las entidades, como aquellos provocados maliciosamente, o por falta de conocimiento de estrategias de seguridad.

Los avances de la tecnología han permitido implementar soluciones en diversos ámbitos de la vida laboral de las personas e instituciones, lo que, a su vez, ha multiplicado la información en los últimos años dentro del contexto educativo. Por lo tanto, las instituciones de Educación General Básica deben adoptar y adaptar metodologías para proteger los datos y mantener en funcionamiento una infraestructura tecnológica adecuada que sirva para la custodia y salvaguarda de la información.

En este sentido, (Muñoz, Cortez, & Bustamante, 2011), mencionan que la seguridad de la información "involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial" (p. 26). Estas estrategias deben cuidar que los datos no sean modificables sin previa autorización, asegurando únicamente que la información llegue a los individuos, entidades o procesos autorizados, para garantizar la disposición y el correcto funcionamiento en el acceso a la información.

1.2 Breve definición del Riesgo de la Información

Según, (Solarte, Rosero, & Ruano, 2015, p 7), se define al Riesgo como: El problema que afecta a los sistemas de información o a los equipos de cómputo considerando una condición del mundo real en el cual se manifiesta una adversidad de circunstancias que se dan en un entorno, donde hay posibilidades de pérdidas de información, (González, 2017, p 20), que pueden ocurrir en sitios, durante un intervalo de tiempo determinado, con consecuencias negativas o positivas que impide el cumplimiento de los objetivos.

De la definición anterior se puede colegir que, si una institución educativa no tiene estrategias para salvaguardar los datos y la información, los riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, en este sentido (Freitas, 2009, p 43), considera que el riesgo es la probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular, (Chamorro, 2013, p 20), donde el riesgo se materializa y se convierte en una medida de las posibilidades del incumplimiento o exceso de los objetivos planteados por la institución educativa.

Un riesgo es la posibilidad de una amenaza que puede conllevar a dos tipos de consecuencia: Ganancia o Pérdida, con la posibilidad de la ocurrencia de un hecho o suceso no deseado, o la no-ocurrencia, que la información puede sufrir, determinando el grado de exposición y la perdida de la misma.

1. 2.1 Análisis del Riesgo.

La materialización de los riesgos según (Mujica & Alvarez, 2009, p 33), puede afectar a la información en general, a la disponibilidad y continuidad de los servicios internos o externos, a la eficacia de los procesos en los que se basan el registro de calificaciones y de asistencia, a la planificación curricular, y a los procesos requeridos para dar de alta a los usuarios en los servicios como el de correo institucional,

en el que se debe generar cuentas de usuarios con sus claves.

Por lo tanto, es necesario aplicarse en el ejercicio de un análisis de riesgo que permita crear políticas de seguridad basadas en una metodología, para controlar y reducir la manifestación de los riesgos, además, (Lozano & Troncoso, 2001,) considera que para establecer un análisis de riesgos, se deben tener claros los objetivos y una escala valorativa con cierta regla de priorización de los mismos; donde se muestre el nivel de impacto según la escala, estableciendo el estado actual en materia de seguridad de la información.

Del mismo modo, el análisis de riesgo es un método y modelo para ponderar o cuantificar el riesgo, y en su determinación se debe considerar lo siguiente:

1. Clasificar a los activos de información, en correspondencia con su valor, tomando como referencia el perjuicio que su degradación implica.

2. Determinar las amenazas a las que se exponen dichos activos de información identificados.

3. Definir las seguridades implementadas y el nivel de eficacia alcanzado ante los riesgos.

4. Calcular el daño, producto de la materialización de una amenaza, sobre los activos.

5. Evaluar el riesgo, ponderado de acuerdo a la frecuencia de ocurrencia de la amenaza (p 8).

Con la identificación de los riesgos, las valoraciones serán aproximaciones teóricas para aquellos casos donde no haya seguridades aplicadas, que sirven de base para bosquejar estimaciones realistas de impacto y riesgo.

1.2.2 Gestión del Riesgo.

La Gestión de Riesgos se da luego de que se identifican y se catalogan los riesgos para tomar alternativas como: aceptarlo, transferirlo, aminorar (implementando

políticas de Seguridad) y evitarlo eventualmente, estas alternativas serán tomadas por la relación costo/riesgo.

Sin embargo, (Rodríguez & Peralta, 2013) manifiestan que la Gestión de Riesgo implica dos grandes tareas a realizar:

• Analizar los riesgos, determinando la estructura organizacional, y donde influyen los riesgos y el impacto estimado en caso de que ocurra.

• Tratamiento de los riesgos, que permite organizar la defensa aplicada y prudente, reduciendo la probabilidad de que suceda un evento inesperado y negativo (p 7).

Tanto el análisis y tratamiento de los riesgos, se combinan en el proceso denominado Gestión de Riesgos. En este mismo sentido, para (SearchDataCenter en Español, 2005) en la labor de identificar los riesgos y las medidas de mitigación del riesgo, un método y proceso de gestión del riesgo ayudarán a:

- Determinar los activos críticos de información y sus características.
- Comprender porque los activos críticos escogidos son necesarios para las operaciones, ejecución de la misión y la continuidad de las operaciones (p 1).

De acuerdo con (Alberts, 2003, p 6), para la gestión del riesgo se deben considerar los criterios para su aceptación y priorización, considerando actividades transversales: monitoreo, revisión, comunicación y consulta, que permitan caracterizar cada uno de los riesgos para luego ser evaluados de forma cualitativa o cuantitativa. Todo esto se considera dentro de la llamada fase de valoración del riesgo. En la fase de la priorización el propósito es llevar a cabo alguna actividad para su tratamiento, donde su objetivo es la definición de las acciones a realizar con relación a los riesgos y la aplicación de controles de seguridad.

1.2.3 Amenazas.

De acuerdo con (Tarazona, 2007), los riesgos de la información aparecen claramente cuando coinciden: vulnerabilidades y amenazas. Si una de las dos está ausente no hay consecuencias. Las amenazas se aprovechan de las vulnerabilidades y provienen de cualquier parte, sea esta interna o externa, en nuestro caso dentro del entorno educativo.

Una amenaza, en términos simples, es una causa potencial del intento de hacer daño o un incidente no-deseado, el cual puede presentar un daño a la institución educativa. Por ello, podemos agrupar las amenazas a la información en cuatro grandes categorías:

- ✓ Factores Humanos (accidentales, errores)
- ✓ Fallas en los sistemas de procesamiento de información.
- ✓ Desastres naturales
- ✓ Actos maliciosos o malintencionados (p 146).

En este sentido (Vega, 2008), considera que entre las amenazas más frecuentes se encuentran:

-Catástrofes naturales: Son las que provocan la interrupción de los servicios, afectando principalmente a la disponibilidad de la información, ejemplos de este tipo de amenazas son los provocados por la naturaleza: las inundaciones, terremotos, tornados, etc.

-Amenazas físicas: Relativo al acceso físico a los recursos, pueden resultar en robos, daños físicos a los equipos, sabotajes. El acceso no autorizado pero que se logra mediante la ingeniería social, explotando la confianza de los empleados de una organización.

-Fraude Informático: Representados por el engaño a los clientes en la venta de productos y servicios a través de promociones y agencias que no existen.

-Intrusiones: el acceso no autorizado a los sistemas de comunicaciones, a los servidores

de una organización, con el fin de dañar la imagen u obtener beneficios económicos indebidos.

-Errores humanos: Como su nombre lo indica resultan de la acción humana, como, por ejemplo: claves fácilmente vulnerables, respaldos (backup) de los sistemas mal hechos, interrupción de los servicios, configuraciones incompletas de los dispositivos.

-Software ilegal: Las consecuencias de copiar software ilegal conducen a vulnerabilidades de los sistemas informáticos, ya que no se cuenta con las actualizaciones que los desarrolladores proporcionan, dentro del software ilegal se tienen también otras amenazas como los códigos maliciosos.

-Código malicioso: Es todo programa o parte de programa (software) que ocasiona problemas en los sistemas informáticos, como puede ser los virus, troyanos, gusanos, puertas traseras, cuando se activan en los sistemas finales. Este tipo de amenaza ha evolucionado gracias a la conectividad cada vez mayor en Internet y por los recursos de engaño de los que se valen los atacantes (p 65).

1.2.4 Criterio de Vulnerabilidades.

Las vulnerabilidades son una debilidad de los activos o los procesos relacionados con la información, por otro lado, (Santana, 2012), afirma que una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para que una amenaza se materialice.

En este caso (Voutssas, 2010, p 139), considera que una vulnerabilidad es una característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza, por ejemplo: la vulnerabilidad de un equipo para ser contagiado por virus de reciente creación mediante correo electrónico, debido a la desactualización del software antivirus o a que dicho sistema aún no reconoce el virus.

Se es vulnerable a cualquier evento, sin importar su naturaleza interna o externa que pueda afectar los activos de información, los datos o la información ante la posibilidad de la presencia de un ataque deliberado o no, por parte del personal interno o externo a la organización.

3. Metodología MAGERIT

Es una metodología que permite hacer un uso adecuado del Análisis de Riesgo y así asegurar los sistemas de información con una técnica para su implementación. El método MAGERIT (Sotelo, Torres, & Rivera, 2012), fue desarrollado por el Consejo Superior de Administración Electrónica, y publicado por el Ministerio de Administraciones Públicas de España, con el fin de cumplir dos procesos: El análisis de riesgo y la gestión de riesgos (Abril, Pulido & Bohada, 2013, p 40), que utiliza un enfoque de cuatro fases para proteger aspectos organizacionales y de tecnología como muestra la figura 1.

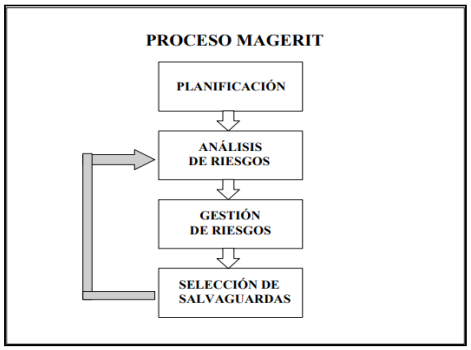

Figura 1: Fases de la Metodología MAGERIT
Fuente: Guía para Responsables del Dominio Protegible.

El proceso que se debe desarrollar en cada una de las fases de la metodología MAGERIT para lograr los resultados esperados son:

-**Planificación**: estableciendo las consideraciones necesarias para arrancar el proyecto, indagando la oportunidad de realizarlo, definiendo los objetivos que se deben cumplir y el dominio (ámbito) que abarcará, planificando los medios materiales y humanos para su realización e iniciando materialmente el propio lanzamiento del Proyecto.

-Análisis de riesgos: identificando y valorando los elementos y componentes

intervinientes en el riesgo, determinando una estimación de los límites de riesgo deseables.

-Gestión de riesgos: identificando posibles funciones y servicios de salvaguarda que minimicen el riesgo calculado, con base en las condiciones que existen se seleccionan los aceptables y otras restricciones, y se especifican los elegidos finalmente.

-Selección de salvaguardas: escogiendo los mecanismos de salvaguarda a implantar, se elabora una orientación de ese plan de implantación, se establecen los procedimientos de seguimiento para la implantación y se recopila la información necesaria para obtener los productos finales del proyecto y realizar las presentaciones de resultados.

El crecimiento de la tecnología dentro del contexto educativo se está dando de manera exponencial, donde toma cada vez más importancia, y se hace necesario el uso de metodologías para minimizar los riesgos asociados al uso de los sistemas garantizando la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los mismos, con la finalidad de generar confianza en los estudiantes, docentes y autoridades de la institución educativa.

La metodología MAGERIT es un marco de referencia que indica cómo llevar a cabo el análisis de riesgos. Se compone de tres libros, el primero; discurre sobre la estructura del modelo de gestión de riesgos, el segundo; presenta el inventario para enfocar el análisis de riesgos y el último; compila una guía de técnicas de trabajo para dicho fin.(Cocho & Romo, 2012, p 3).

El Objetivo del método MAGERIT, es como conocer el estado de seguridad de los sistemas de información y la implementación de medidas de seguridad, garantizar que no hayan elementos que queden fuera del análisis para que haya una profundidad adecuada en el mismo, mitigar las vulnerabilidades y asegurar el desarrollo del sistema en todas las fases de desarrollo, es

así que MAGERIT es la disciplina más utilizadas en el ámbito empresarial ya que les permite prepararse para procesos de auditorías, certificaciones y acreditaciones.

4. Norma ISO/IEC 27002

La norma ISO/IEC 27002, es un conjunto de estándares que proporciona un marco de gestión para la Seguridad de la Información, utilizable para todo tipo de organización o institución, contiene una guía de buenas prácticas a partir de objetivos de control y controles recomendables para el nivel de seguridad de la información, esta norma no es certificable y contiene 11 dominios, 39 objetivos de control y 133 controles. (ISO/IEC 27002, 2009, p 1)

Es relevante para la institución Zulima Vaca Rivera de la ciudad de Pasaje, la implementación de los dominios y controles de seguridad más relevantes que se enmarcan a los procesos que actualmente ejecutan los centros de Educación General Básica.

5. Políticas de Seguridad

Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos" (Farias, Mendoza, & Gómez, 2003, p 43). Las reglas que se encuentran documentadas en un Plan de Políticas de Seguridad son consideradas dinámicas (Wood, 2002, p 7) es decir, que deben ser ajustables y mejorarse continuamente según los cambios que se presentan en los ambientes educativos.

Estos cambios deben ser presentados como un recurso ventajoso y aplicable, recalcando que para que una política de seguridad sea efectiva, necesita contar con elementos indispensables que apoyen este proceso: La cultura organizacional, las herramientas y el monitoreo (Dussan, 2006, p 86).

6. Herramienta PILAR

Según Molina (2017, p 4), la herramienta PILAR soporta el análisis y la gestión del riesgo de un Sistema de información

siguiendo la metodología MAGERIT, es decir que posee un conjunto de parámetros y una biblioteca estándar de propósito general, que es capaz de realizar calificaciones de seguridad respecto a normas como ISO 27002 mediante las puntuaciones cuantitativas con los siguientes pasos:

1.- Se identifican los Activos acorde a las capas estándar que posee la herramienta, la misma que hace categorizaciones por capas, ubicando los equipos de cómputo que posee la institución.

2.-Cada elemento registrado en la herramienta es categorizado acorde a las funciones que cumple en relación con los procesos de gestión de la información dentro de la Institución Educativa.

3.-Asimismo, se identifica las amenazas a las que se expone cada elemento categorizado acorde a las opciones que brinda la herramienta.

4.-Finalmente se configura los dominios en los cuales convergen los riesgos para los equipos e información, tomando en cuenta los siguientes parámetros: disponibilidad, integridad de los datos, confidencialidad de los datos, y autenticidad de los usuarios y de la información. A cada parámetro se le define los criterios de valoración que definirán los riesgos.

5.-Realizadas las configuraciones, la herramienta permite la generación de reportes de valoración acumulada de los riesgos, así como del impacto, tal como se muestra a continuación.

6.- Los informes demuestran el nivel de exposición a riesgos por parte de los activos que gestionan la información.

METODOLOGÍA.

La investigación se inscribió en un estudio de metodología cualitativa debido a que se pretende comprender la realidad social con los aportes de los sujetos investigados, y a la vez presentar una dinámica de transformación social, con los resultados de la técnica de observación.

La estrategia metodológica asumida en la presente investigación contempla una revisión de literatura, que tiene un alcance descriptivo, que permitió recoger, organizar, resumir, presentar, analizar y generalizar los resultados de las encuestas aplicadas a estudiantes para conocer los criterios de seguridad de la información que aplican actualmente la institución.

Como la aplicación de entrevista a docentes y personal administrativo que permitió definir el tipo de activos de información que son más vulnerables a los riesgos. La investigación a través del método descriptivo permite la indagación en tres campos:

Tabla N° 1. *Población de la investigación*

Tipo de Población	Población
Personal Administrativo	5 personas
Docentes	35 personas
Estudiantes Tercero de Bachillerato paralelo "A-B-C"	98 personas
Total	138 personas

Fuente: Guía de Observación
Elaboración: Autor.

Se trabajó con una población total de 138 personas, la cual fue tomada en el año 2018.

ANÁLISIS DE RESULTADOS Y DISCUSIÓN

Los instrumentos empleados para validar la investigación describen la presencia de los supuestos teóricos, así como los resultados adquiridos de las encuestas y entrevistas aplicados a los estudiantes, personal docente y administrativo considerada la población de la investigación, que caracteriza la situación de las amenazas y vulnerabilidades a las que se encuentra expuesta la EGB Zulima Vaca Rivera de la ciudad de Pasaje.

A continuación, se demuestra los datos obtenidos de las encuestas y entrevistas aplicadas bajo los estándares de la Norma ISO/IEC 27002 para el análisis y gestión del riesgo.

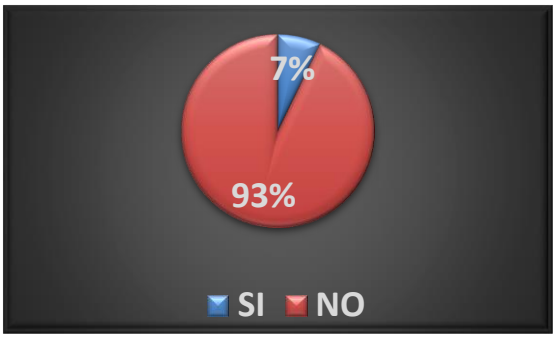

Figura 2. Normas para el uso de dispositivos de almacenamiento externo.
Fuente: Encuestas aplicadas a Estudiantes.
Elaboración: Autor.

El 93% de los encuestados consideran que no existen normas que regulen el uso de dispositivos de almacenamiento, que representa 91 encuestados de las 98 encuestas realizadas. Lo que devela que el personal utiliza medios de almacenamiento portátil sin supervisión, que a su vez deriva en la manipulación descontrolada de la información.

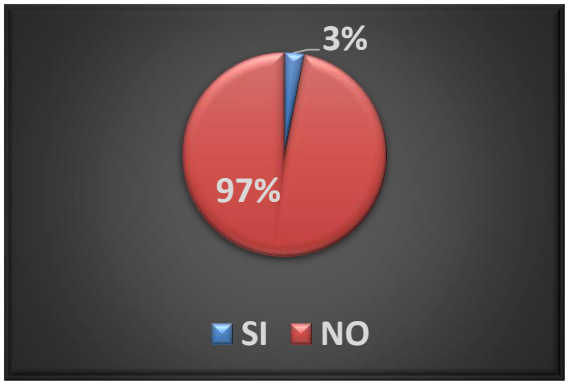

Figura 3. La información es asequible sin restricciones.
Fuente: Encuestas aplicadas a Estudiantes.
Elaboración: Autor.

De los 98 encuestados, el 97% que representa 95, opina que la información no está restringida y que puede ser accedida desde cualquier punto con una conexión a Internet. En sentido general, significa según su opinión una vulnerabilidad grave la facilidad de acceso, y su libre distribución mediante dispositivos de almacenamiento, y herramientas de almacenamiento en la nube sin control.

En la entrevista a los docentes y personal administrativo, se establece que existen responsabilidades divididas para el control y gestión de equipos, donde las instituciones educativas del Estado se encuentran obligadas a llevar un registro de los activos tecnológicos con los que se cuenta, sin embargo, no cuentan con conocimientos adecuados a niveles de seguridad de la información, que en sí provoca debilidades en los niveles de acceso a la información y los dispositivos que la administran.

Estos resultados coinciden con los obtenidos por (Bortnik, 2010, p 1), quien determinó que la fuga de información se considera una tendencia creciente en lo que refiere a pérdidas de información, a partir de estadísticas de Data Breaches y del Indetify Theft Center, solo en Latinoamérica, en los últimos dos años la cantidad de incidentes de

fuga de información afecto al 90% de los habitantes, lo cual sería como si en el último par de años se hubiera visto filtrada información sensible de 9 de cada 10 habitantes de la región.

Es necesario capacitar al personal con conocimientos sobre mecanismos para la seguridad de la información, con miras a disminuir la incertidumbre ante posibles ataques, pérdidas o robos de la información de la Institución Educativa, sin embargo, existen criterios similares emitidos por Gordillo (2017, p 2) que indican que es necesario crear cultura de seguridad de información para que el personal tome conciencia de la importancia de mantener la información confidencial protegida, y crear políticas las de protección de datos respectivas.

Crear políticas de protección de datos para categorizar los niveles de protección para el tratamiento de la información acorde a su importancia, evitando fugas de información debido a la ausencia de procedimientos que gestionen los medios de almacenamientos.

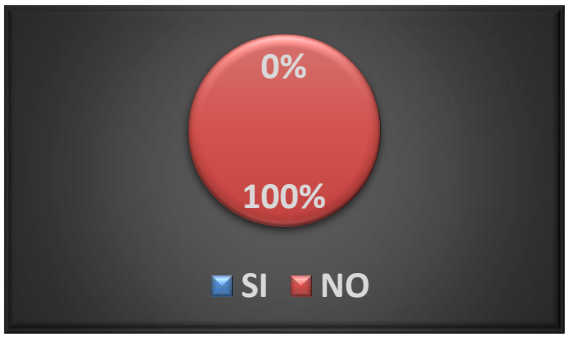

Figura 4. Acceso a los equipos de cómputo acorde al tipo de usuario y privilegios.
Fuente: Encuestas aplicadas a Estudiantes.
Elaboración: Autor.

El 100% de los encuestados manifestó que tiene libre acceso a los equipos de cómputo, sin la necesidad de especificar usuario o niveles de privilegios, es decir, que la falta de especificación de privilegios y accesos a los equipos de cómputo genera ausencia de confidencialidad de la información que en ellos se procesa y manipula, generando amenazas a la información de los usuarios.

Figura 5. Cambio periódico de contraseñas para el acceso a los equipos de cómputo
Fuente: Encuestas aplicadas a Estudiantes.
Elaboración: Autor.

Todos los encuestados coinciden en que no existen mecanismos que controlen un adecuado cambio de contraseñas para el ingreso a los equipos de cómputo. Esto se genera por la ausencia de privilegios de acceso acorde al tipo de usuario se denota la falta de control para el cambio periódico de contraseñas que se deberían de administrar para el uso de los equipos de cómputo de la Institución por parte de los estudiantes.

El control de acceso y su gestión son escasos en la Institución Educativa, lo que se ve reflejado en la falta de políticas que regulen los tipos de usuarios y sus privilegios, así como procedimientos que aseguren el control periódico de contraseñas de acceso a los equipos de cómputo y a la interconexión.

Donde los controles de acceso son débiles lo cual incrementa el peligro de ataques, o accesos indebidos a las instalaciones y por ende a la información que reposa en dispositivos de cómputo y almacenamiento.

El riesgo se incrementa por la ausencia de políticas que clasifiquen a los usuarios estableciendo privilegios, y la manera en que se deben establecer las contraseñas.

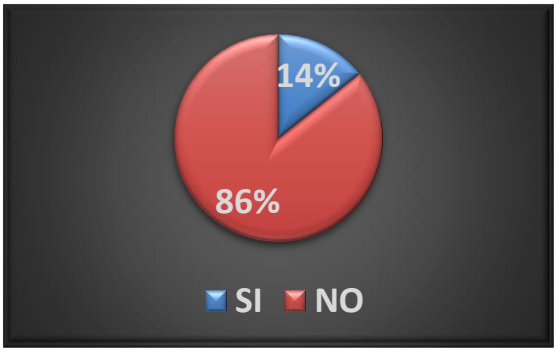

Figura 6. Corrige rápidamente los fallos que se presenten en los equipos de cómputo.
Fuente: Encuestas aplicadas a Estudiantes.

De los 98 encuestados, 84 coinciden en que no se da solución inmediata a los fallos que ocurren en los equipos de uso durante su

manipulación, lo que representa el 86%. El 14% restante expresa lo contrario.

La falta inmediata de soluciones conlleva demoras y exposición de la información a riesgos que generarían la pérdida o corrupción de la misma, debido a la falta de políticas que expresen los procedimientos que serán tomados en cuenta en casos específicos de daños en equipos.

Las opiniones por parte de los docentes y autoridades en las encuestas consideran que no existen planes que prevengan daños en los activos tecnológicos de la Institución, ni controles establecidos para la identificación de personal no autorizado a dependencias donde se hallen equipos de cómputo e información. Tampoco existen mecanismos que permitan la rápida corrección de daños que se presentasen en activos tecnológicos.

Ecuador no está preparado para enfrentar desastres naturales, y ningún gobierno ha dispuesto planes ni rubros exclusivos para atender a su población cuando resulte damnificada.

La exposición a riesgos provocados por desastres naturales es inevitable. Al respecto Román (2006, p 264), considera que el Ecuador no está preparado para enfrentar desastres naturales, pero las instituciones educativas están obligadas a elaborar un Plan de Reducción de Riesgo contra desastres naturales, ya que esto no minimiza su daño aplicando medidas que salvaguarden al personal y los equipos e información que reposan en la Institución con una correcta política de seguridad.

Debido a la naturaleza pública de la Institución, el control para el ingreso de las personas es escaso, por la ausencia de guardias y sistemas de video vigilancia que impida el acceso a oficinas donde haya equipos e información utilizada en las actividades académicas de la Institución Educativa.

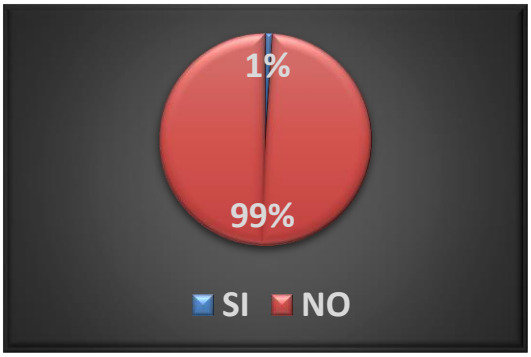

Figura 7. Controla la detección, prevención y recuperación de problemas con la concientización de los usuarios.
Fuente: Encuestas aplicadas a Estudiantes.
Elaboración: Autor.

El 99% de los encuestados, que representa un total de 97 personas, considera que no se concientiza con ellos sobre los procedimientos a seguir en caso de la ocurrencia de desperfectos en el manejo de la información mediante los equipos de cómputo. Esto es posible si se garantiza el apoyo de los usuarios mediante un comportamiento adecuado para el tratamiento de la información, que incluya medidas para detectar, prevenir y recuperarse de daños o alteraciones en equipos de cómputo e información. Esto es fundamental, pero es un aspecto que no se aplica en la Institución Educativa y que genera amenazas difíciles de controlar y detectar en los tiempos adecuados.

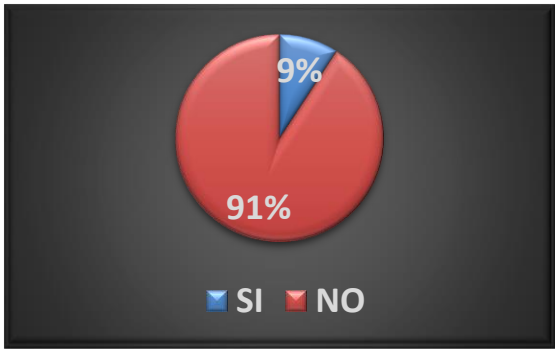

Figura 8. Controla la instalación de software.
Fuente: Encuestas aplicadas a Estudiantes.
Elaboración: Autor.

De los 98 encuestados 89 consideran que no hay control para instalar software en los equipos donde manipulan información, lo que representa el 91% del total. El 9% restante opina que se controla la instalación de software.

No controlar la instalación de software es un factor que influye en gran medida en las amenazas que atentan contra la integridad de la información, por lo que la implementación de políticas de seguridad que regulen este factor permitirá asegurar la confiabilidad y confidencialidad de la información y los equipos donde ésta se manipula.

En los datos proporcionados por las entrevistas se considera que no existen manuales procedimentales, ni planes de recuperación de procesos que guíen a los usuarios ante eventuales inconvenientes a los que se enfrenten. No se regula el proceso de respaldos de información, cuyos tiempos de ejecución son inciertos e inconstantes. Además, no se regula la instalación de nuevos programas, incrementándose de esta manera los riesgos de ataques por malware que expondrían la información.

En este sentido la ausencia de manuales y políticas, deriva en el incremento de riesgos y problemas tanto para los usuarios como para quienes se encargan de la administración de los equipos de cómputo, interconexión e información. Esto dificulta la protección y el acceso controlado a la información y su distribución, lo que con la ausencia de controles para la instalación de software pone en riesgo la información y operaciones que se llevan a cabo, debido a la libertad de los usuarios para instalar cualquier software sin salvaguardar la integridad de los equipos y la información.

PROPUESTA

Acorde a la información analizada, producto de las entrevistas y encuestas realizadas, así como el análisis de la misma mediante la utilización de la herramienta PILAR, para la medición de los riesgos y la exposición que tiene la información a estas amenazas, se propone un conjunto de políticas de seguridad que deberán ser aplicadas y utilizadas por todo el personal de la Institución Educativa, basadas en los siguientes dominios de la Norma ISO 27002:

- Política de Seguridad
- Aspectos Organizativos de la Información.
- Seguridad Ligada a los Recursos humanos.
- Gestión de Activos
- Seguridad física y del entorno
- Control de acceso

- Gestión de incidentes en la seguridad de la información.

POLÍTICA DE SEGURIDAD

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Documento de políticas de seguridad de la información: se debe definir todas las responsabilidades en cuanto a seguridad de la información.

La Institución Educativa debe formalizar documentalmente las responsabilidades para la administración de la información. Se definirán roles a los usuarios de la información, clasificando a los mismos por departamentos y/o permisos para la administración o manipulación de la información. Definiendo las siguientes áreas: Directiva: **que asegurará la disponibilidad de la información.** Tendrá como responsabilidad el envío y recepción de la información referente a actividades administrativas y académicas desde y hacia el exterior de los dominios de la Institución.

Administración: manipulará la información proveniente de la Docencia, sin alterar la misma, siendo filtro para el posterior envío de la información a la Directiva.

Docencia: gestará la información de aprovechamiento académico, producto de las actividades que realice como parte del proceso enseñanza aprendizaje con los estudiantes de la Institución.

Estudiantil: que no tendrán acceso a la información de aprovechamiento académico, pero si acceso a la utilización de equipos de cómputo como parte de las actividades académicas.

Revisión y Evaluación: la política de seguridad debe ser revisada periódicamente ante la posible ocurrencia de cambios significativos para garantizar su uso continuo, y su efectividad.

ASPECTOS ORGANIZATIVOS DE LA INFORMACIÓN.

Compromiso de la dirección con la seguridad de la información: los

responsables de la seguridad de la información brindaran asesoramiento constante que asegure el tratamiento de la información por parte de los usuarios, direccionando procesos que garanticen la confidencialidad e integridad de la información, asumiendo la responsabilidad de la seguridad de la información.

Coordinación de seguridad de la información: la ejecución de las actividades relacionadas con la seguridad de la información se garantizará designando responsables para la implementación de sistemas de seguridad de la información.

Asignación de las responsabilidades para seguridad de la información: se debe definir una estructura organizativa y funcional con la definición de responsabilidades como apoyo para garantizar la seguridad de la información en cada área de usuarios previamente definida.

Proceso de autorización de recursos para el procesado de la información: la directiva autorizará el uso de nuevos equipos de almacenamiento, con el apoyo de los encargados de la seguridad de la información, generando los permisos necesarios para el traslado de información entre dispositivos, o hacia el exterior.

Acuerdos sobre confidencialidad: se aplicará convenios o actas de confidencialidad de la información, que serán celebradas por los usuarios que formen parte de las áreas Directiva, Administrativa y de Docencia, donde se estipulará las responsabilidades en caso de pérdida o divulgación de información confidencial.

GESTIÓN DE ACTIVOS

Inventario de Activos: todos los activos deben ser identificados previo a su integración a la Institución, definiendo un esquema para la codificación de los dispositivos de tratamiento de la información, definiendo un esquema que contenga 3 caracteres que definan el área a la que pertenece el equipo, seguido de una

secuencia numérica de 3 dígitos que identifique el número de equipo.

Propiedad de los activos: se definirá para cada activo el nivel de información que maneja, y los permisos que tendrá cada área para el tratamiento de la misma.

Uso adecuado de los activos: se definen reglas que garanticen el uso responsable y razonable de los activos, mediante la firma de convenios o actas de compromiso con los usuarios designados para el uso de los equipos.

Guías de clasificación: la información se clasificará acorde a su valor, estableciendo niveles de confidencialidad acorde al criterio de la directiva. De la misma manera los equipos tendrán una clasificación que especifique el nivel de importancia que tiene el activo en cuanto al tratamiento de la información.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Inclusión de la seguridad en las responsabilidades y funciones laborales: los usuarios bajo relación de dependencia con la Institución tendrán como parte de sus obligaciones laborales, funciones definidas que colaboren con el tratamiento adecuados de los activos de información, y su confidencialidad e integridad.

Conocimiento, educación y entrenamiento de la seguridad de la información: el personal que sea seleccionado para su ingreso a las funciones directivas, administrativas, o de docencia se someterá a un proceso de inducción sobre la criticidad de información que se manejará, así como los recursos a los cuales tendrá acceso y que funciones podrá desempeñar

SEGURIDAD FÍSICA Y DEL ENTORNO.

Perímetro de seguridad física: el acceso a las instalaciones será restringido, permitiendo únicamente el ingreso en horarios específicos tanto del personal, como

de usuarios de los servicios de la Institución Educativa. Las áreas donde se encuentren activos de información, deberán tener control de acceso en las puertas, las cuales siempre se mantendrán cerradas y con seguro.

Controles físicos de entrada: Tanto en la entrada a la Institución, como a las áreas donde se hallen activos de información se realizará un control de ingreso, mediante la solicitud de identificación, y el registro de bitácoras.

Protección contra amenazas externas y ambientales: las oficinas y laboratorios de computación deben contar con artículos para la prevención y contención de incendios, como extintores. Se desarrollarán periódicamente simulacros que preparen al personal ante una eventualidad, para cuidar el recurso humano y posteriormente la información.

Se protegerá los accesos a las oficinas con la construcción de bordes de cemento que prevengan el ingreso de agua en caso de inundaciones.

Seguridad de los equipos: los equipos se ubicarán en lugares convenientemente elegidos, que cumplan con las siguientes características: lejos de fuentes de calor natural o artificial, lejos de tomas de agua, protegidos de la luz solar y contra lugares propensos a goteras.

Cuando no se utilicen los equipos deberán estar protegidos contra el polvo con la ayuda de cobertores.

Todos los equipos contaran con suministros independientes de energía eléctrica, así como respaldos de energía suficiente en caso de cortes energéticos que permitan el apagado correcto del equipo y el registro de la información.

Los cableados que lleven el flujo de energía, así como las conexiones a las redes informáticos deberá estar protegido por canaletas, y ubicados estratégicamente de manera que no intervenga en los corredores o accesos al personal y/o usuarios.

Mantenimiento de equipos: los mantenimientos preventivos serán periódicos, registrados en bitácoras, por personal designado con los conocimientos comprobados para el tipo de actividades designados. En caso de contratar personal externo para la actividad, estos deberán se acompañados por el personal encargado de la seguridad de la información de la institución.

En el caso de los mantenimientos correctivos, también serán registrados en bitácoras priorizando la seguridad de la información contenida, generando los respaldos necesarios. El desarrollo de cronogramas para la elaboración de mantenimientos es responsabilidad de los encargados de la seguridad de la información.

CONTROL DE ACCESO

Gestión de Acceso de Usuario: se definirá como política el acceso obligatorio mediante contraseñas a los activos de la información.

Gestión de Privilegios: los responsables de la seguridad de la información definirán los privilegios de cada usuario para la manipulación de la información, así como para el uso de los sistemas operativos de los equipos de cómputo.

Gestión de contraseñas de usuario: las contraseñas serán gestionadas por los responsables de la seguridad de la información, quienes tendrán un registro de las contraseñas que hayan definidos los usuarios. Se exigirá el cambio periódico de contraseñas, en un intervalo que será definido por la Directiva.

Control de acceso a la red: las contraseñas de acceso a la red, cableada e inalámbrica serán responsabilidad de los encargados de la seguridad de la información**,** quienes configurarán el acceso a los equipos, sin necesidad de divulgar las contraseñas.

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Reporte de eventos de la seguridad de la información: se realizará campañas de concientización con los usuarios y personal para el manejo adecuado de eventos que afecten la seguridad de la información, los cuales deben ser reportados lo más rápido posible. En el caso de eventos que afecten la seguridad física de las instalaciones, se implementará reportes de incidentes que serán generados por los implicados al momento de producirse la vulnerabilidad.

Reportes de debilidades en la seguridad de la información: las campañas de concientización deben hacer referencia a identificar debilidades que se convertirán en vulnerabilidades a la integridad y confidencialidad de la información.

CONCLUSIONES

- Se encontró que la implementación de un Plan de Políticas de Seguridad de la Información amparada en la normativa ISO 27002 y los procedimientos de control que han sido desarrollados por los técnicos encargados de las Tecnologías de la Información y Autoridades de la Institución, es una alternativa de solución que no busca solo proteger y administrar de manera eficiente los procesos de control de gestión escolar, sino que también busca proteger, prevenir o disminuir los incidentes provocados por amenazas y riesgos a la información.
- Para el desarrollo de la investigación se encontraron limitaciones como la falta de investigación y datos estadísticos de las Políticas de Seguridad de la Información en el área de la Educación General Básica; de la misma manera los procesos y autorizaciones tardías por parte del Distrito de Educación para brindar las facilidades a la aplicación de las técnicas de investigación.
- En la investigación realizada a través de las entrevistas a las autoridades, se demuestra que el 85% si mantienen estrategias de seguridad, pero en las

encuestas aplicadas a los docentes se encuentra que desconocen de normas o estrategias de seguridad dentro de la institución, siendo en su mayoría la información producida por los docentes, para la gestión de la información de forma externa como es el acceso a las plataformas de control de gestión escolar, se vuelve obligatorio el hecho de que deben cambiar periódicamente (por ejemplo de manera mensual o trimestral) la clave de su correo institucional, y de las herramientas de aplicación, que son accedidas desde cualquier computador, quedando expuesta a múltiples amenazas a la seguridad e integridad de la información.

- Con los resultados obtenidos en la investigación, se propone una metodología para la implementación de Políticas de Seguridad de la Información en el área de la Educación General Básica, especialmente en las instituciones de tipo público, en donde tienen limitaciones con recursos económicos, tecnológicos y humanos, para trabajar con documentación que requieren de una investigación.
- La metodología MAGERIT, aplicada en sus tres guías; método, catalogo y técnica de la versión en español, permitió la clasificación de los activos de información, el valor, la identificación de las amenazas, impacto y riesgo, salvaguardas para el Análisis y Gestión del Riesgo de los sistemas de Información de la institución de la EGB.
- La metodología propuesta se encuentra trabajada en los siete dominios que sostiene la norma ISO 27002, los cumplimientos de estas Políticas tienen como fin, mejorar la calidad de servicio entregado a la comunidad estudiantil de la Escuela General Básica.
- La herramienta PILAR permitió la validación de la situación actual y una proyección simulada de tres meses y un año de la efectividad de la aplicación de los controles en tres dimensiones: confiabilidad,

disponibilidad y autenticidad, que permitan salvaguardar, aplicar las normas y los procedimientos de seguridad en la institución educativa.

Una investigación futura podría centrarse en la aplicación de la propuesta resultante en diferentes instituciones de educación básica a nivel país, y también en instituciones de nivel secundario.

REFERENCIAS BIBLIOGRÁFICAS

Abril, A., Pulido, J., & Bohada, J. A. (2013). Análisis de Riesgos en Seguridad de la Información, *1*. Recuperado de https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121/113

Alberts, A. (2003). Analisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El enfoque ISO 27001-2005, 6.

Asamblea Nacional Constituyente de Ecuador. (2008). *Constitución de la República del Ecuador* (p. 218). Recuperado de http://www.wipo.int/edocs/lexdocs/laws/es/ec/ec030es.pdf

Borghello, C. (2001). *Seguridad Informática sus implicancias e implementación*. Universidad Tecnológica Nacional, Argentina.

Bortnik, S. (2010). ¿Qué es la fuga de información? En *welivesecurity*. Recuperado de https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

Chamorro, V. (2013). *Plan de Seguridad de la Información basado en el Estándar ISO 13335 Aplicado a un Caso de Estudio.* Escuela Politécnica Nacional, Quito. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/5617/1/CD-4645.pdf

Cocho, J., & Romo, M. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Consultora SEMA GROUP. Recuperado de http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

Dussan, C. (2006). Políticas de Seguridad Informática. *Entramado, 2*(1), 86–92.

Farias, M., Mendoza, M., & Gómez, L. (2003). Las Políticas de Seguridad como Apoyo a la Falta de Legislación Innformática. *Techno-legal Aspects of Information Society and New Economy: An Overview*, *I*, 185–191.

Freitas, V. D. (2009). Analisis y evaluación del riesgo de la información: caso estudio Universidad Simón Bolívar, *6 (1)*, 43–55.

González, J. (2017). *Auditoria de Seguridad Informática para la Institución Educativa Departamental Luis Carlos Galán- Municipio de Yacopí Cundicamarca*. Universidad Nacional Abierta y A Distancia, CEAD – LA DORADA - CALDAS. Recuperado de https://docplayer.es/93345142-Auditoria-de-seguridad-informatica-para-la-institucion-educativa-departamental-luis-carlos-galan-municipio-de-yacopi-cundinamarca.html

Gordillo, S. (2017). Fuga de información la mayor amenaza para la imagen corporativa. *Universidad Militar Nueva Granada*, 22.

ISO/ IEC JTC 1. (2005). *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información* (II). Organización Internacional de Normalización, Comisión Electrotécnica Internacional. Recuperado de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

ISO/IEC 27002. (2009). ISO/IEC 27002:2005. Recuperado de http://www.iso27000.es/download/ControlesISO27002-2005.pdf

Lozano, B., & Troncoso, M. (2001). El Analisis de Riesgo: Base de una buena Gestión, 8.

Molina, M. (2017, diciembre). Análisis de Riesgos de Centro de Datos Basados en la Herramienta PILAR DE MAGERIT, *Vol. 1*. Recuperado de http://www.revistaespirales.com/index.php/es/article/view/125/68

Mujica, M., & Alvarez, J. (2009). El Análisis de Riesgo en la seguridad de la informaci´on, *4*, .33–37.

Muñoz, P., Cortez, A., & Bustamante, V. (2011). La seguridad de la información, *8 (1)*, 25–31.

PwC. (s/f). Encuesta Mundial sobre ciberseguridad 2017. *2017*, *I*, 1.

Rodríguez, J. M., & Peralta, I. (2013). *Gestión de Riesgos*. tiThink Consultoría. Recuperado de https://www.tithink.com/publicacion/MAGERIT.pdf

Román, M. (2006). *Plan de prevención para emergencias por desastres Naturales en la provincia de pichincha, su Organización y aplicación en la educación básica en la Próxima década*. INSTITUTO DE ALTOS ESTUDIOS NACIONALES. Recuperado de http://repositorio.iaen.edu.ec/bitstream/24000/51/1/CD-IAEN-0110.pdf

Santana, C. (2012, septiembre 7). Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? Recuperado de https://www.codejobs.com/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

SearchDataCenter en Español. (2005). Gestión de riesgos de seguridad de la

información: Comprensión de los componentes. Recuperado de https://searchdatacenter.techtarget.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes

Solarte, F., Rosero, E., & Ruano, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001, *28*(5), 492–507.

Sotelo, M., Torres, J., & Rivera, J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. Recuperado de http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf

Tarazona, T. C. (2007). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología. *uexternado.edu.co*, 146.

Tzu, S. (1972). El Arte de la Guerra, 64.

Vega, W. (2008). Politicas y Seguridad de la Información. Recuperado de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

Velasco, A. (2008). El Derecho Informático y La Gestión de la Seguridad de la Información una Perspectiva con Base en la Norma ISO 27 001. *Revista de Derecho*, *29*, 333–366.

Voutssas, J. (2010). Preservación documental digital y seguridad informática. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Wood, C. (2002). *Políticas de Seguridad Informática - Mejores Prácticas Internacionales*. Houston, Estados Unidos de América: NetIQ.