Scientia Et Technica
ISSN: 0122-1701
scientia@utp.edu.co
Universidad Tecnológica de Pereira
Colombia

Benavides Sepúlveda, Alejandra; Blandón Jaramillo, Carlos
Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico
Scientia Et Technica, vol. 23, núm. 1, 2018, Enero-Marzo, pp. 85-92
Universidad Tecnológica de Pereira
Colombia

Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico

Model information security management system for entry-level educational institutions.

Alejandra Benavides Sepúlveda, Carlos Blandón Jaramillo
Facultad de Ingeniería de Sistemas, Universidad Autónoma de Manizales, Manizales, Colombia
alejandra.benavides@autonoma.edu.co
carlos.blandonj@autonoma.edu.co

***Resumen*— El Ministerio de Tecnologías de la Información y las Comunicación – MINTIC ha establecido directrices que permiten implementar sistemas de gestión de seguridad de la información – SGSI en las entidades del estado. La educación pública es un servicio y un derecho de los niños y niñas consagrado en la Constitución Política de Colombia, circunscrito en el Decreto Reglamentario 1078/2015, que contiene a su vez lo lineamientos para la implementación de la estrategia de gobierno en línea – GEL, incluyendo un SGSI basado en la norma NTC ISO/IEC 27001.**

El proyecto consiste en realizar un análisis de riesgos con base en la norma ISO 27005 identificando los activos críticos del área de secretaría académica de las instituciones educativas – IED's de nivel básico y los riesgos asociados, para generar un plan de tratamiento de riesgos que permita proponer una declaración de aplicabilidad, así mismo analizar la normatividad del Ministerio de Educación, del MINTIC y los requisitos de la norma NTC ISO/IEC 27001 que permitan proponer un modelo general que facilite la implementación de un SGSI en este tipo de instituciones.

El modelo resultante cumple con los requisitos obligatorios establecidos en la norma NTC ISO/IEC 27001, y constituye una base para garantizar la disponibilidad, integridad y confidencialidad de la información sensible de los niños, cumpliendo las disposiciones pertinentes del sector educación, sector TIC componente seguridad y privacidad de la información.

***Palabras clave*—Análisis de riesgos, Confidencialidad, Disponibilidad, Instituciones educativas, Integridad, Seguridad**

***Abstract*— The Ministry of Information and Communication Technologies (MINTIC) has established guidelines for the implementation of information security management systems (ISMS) in state entities. Public education is a service and a right of children enshrined in the Political Constitution of Colombia, circumscribed in Regulatory Decree 1078/2015, which contains once again the guidelines for the implementation of the online government strategy - GEL, Including an ISMS based on the standard NTC ISO/IEC 27001.**

The project consists of carrying out a risk analysis based on the guidelines of ISO 27005, identifying the critical assets of the academic secretariat area of educational institutions - basic level and associated risks, to generate a risk management plan That allows to propose a declaration of applicability, as well as to analyze the regulations of the Ministry of Education, of MINTIC and the requirements of the norm NTC ISO/IEC 27001 that allow a general model that facilitate the implementation of an ISMS in this type of institutions.

The resulting model complies with the mandatory requirements established in the NTC ISO/IEC 27001 standard and provides a basis for ensuring the safety, integrity and confidentiality of sensitive information of children, complying with the relevant provisions of the education sector, Privacy of information.

***Key Word* — Availability, Confidentiality, Educational institutions, Integrity, Risk analysis, Security.**

I. INTRODUCCIÓN

En las últimas décadas, el vertiginoso avance de las herramientas para el procesamiento de información, así como el desarrollo de los mecanismos empleados para establecer comunicaciones, han generado dinamismo en los procesos productivos y de prestación de servicios, pero de manera proporcional han surgido riesgos a la seguridad de la información, que se contrastan con la preparación precaria de las organizaciones que adoptan la tecnología como elemento esencial para el desarrollo de sus actividades; en consecuencia se han desarrollado diversas guías de buenas prácticas para la

Fecha de Recepción: 26 de mayo de 2017
Fecha de Aceptación: 15 de marzo de 2018

administración de los activos de información, que se convierten en estrategias para la preservación de la confidencialidad, integridad y disponibilidad de la información.

Las entidades del estado en cumplimiento del Decreto Reglamentario 1078/2015, deben implementar un SGSI que garantice los aspectos antes mencionados; que tiene dentro de sus funciones brindar educación, la cual comprende los niveles de primaria, secundaria y media, a través de las Secretarías de Educación.

Los riesgos de la información sensible de los niños en las IED's y la escasa preparación de sus administrativos sobre este particular requieren de un SGSI adaptado a las necesidades del entorno escolar que facilite su implementación y a la vez garantice el cumplimiento de los criterios de la seguridad de la información, siendo coherente con la reglamentación del MINTIC, el MEN y los requisitos establecidos en la norma NTC ISO/IEC 27001.

II. LA EDUCACIÓN BÁSICA Y LA SEGURIDAD DE LA INFORMACIÓN

La educación es un derecho incluido en la declaración de los derechos humanos [1], la convención de los derechos del niño [2], y el pacto internacional de los derechos económicos, sociales, y culturales [3]. El gobierno de Colombia incluye en la carta magna de 1991, las normas que reglamentan la educación, por cuanto es importante analizar la relación y los puntos de convergencia entre los requerimientos de seguridad de la información emanados por el MINTIC a través de la estrategia de Gobierno en Línea, el MEN y los requisitos de la norma NTC ISO/IEC 27001.

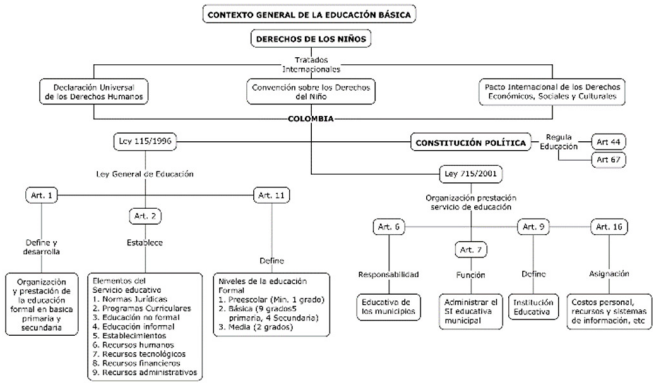

Figura 1. Contexto general de la educación en Colombia

La población atendida por las instituciones educativas será asignada de acuerdo a las variables de la prestación del servicio educativo y dependiendo de su ubicación rural o urbana [4]. El Decreto 1078/2015 describe las directrices que todas las instituciones del Estado deben seguir para acogerse a la estrategia GEL [5], dentro de las cuales se encuentran los ministerios, los departamentos administrativos y las superintendencias por parte del sector central de la administración pública nacional y las gobernaciones, alcaldías y las secretarías de despacho en el correspondiente nivel territorial [6].

En relación a los sistemas de información en la prestación del servicio de educación básica el Decreto 1526 de 2002 establece la reglamentación para la administración de los sistemas de información del sector educativo y la evaluación de sus resultados [7].

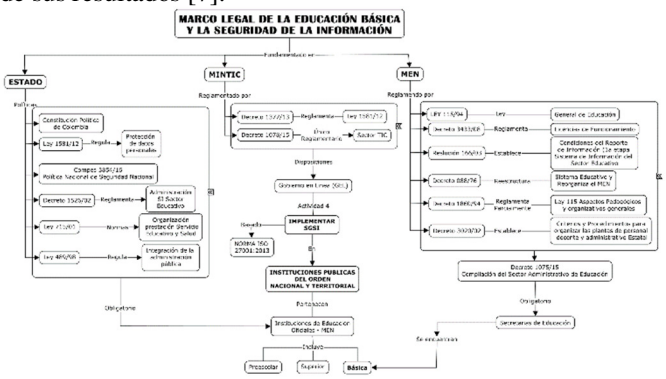

Figura 2. Marco legal de la educación básica y la seguridad de la información en Colombia

La implementación de un SGSI 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.

EL Decreto 1075/2015 establece la estructura del sector educativo en cabeza del MEN por parte del gobierno nacional, secretarias de educación departamentales, secretarias de educación municipales, quienes velarán en su jurisdicción por el adecuado manejo del servicio educativo de todas las instituciones educativas [4].

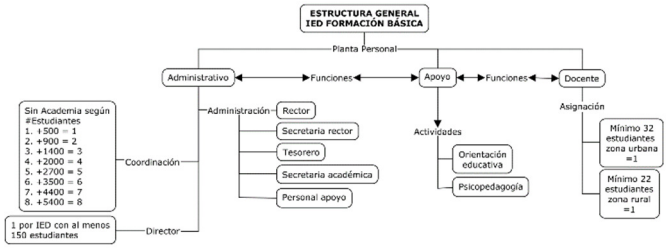

Figura 3. Estructura general IED de formación básica

III. DIAGNÓSTICO DEL SGSI EN LOS ESTABLECIMIENTOS EDUCATIVOS

La recolección de información y aplicación de los instrumentos empleados se realizó a cuatro sujetos de estudio de la comuna universidad de la ciudad de Pereira, Risaralda, Colombia.

A. Brechas de cumplimiento de requisitos de la norma NTC ISO/IEC 27001

Índice escala de valoración	% de cumplimiento (EV)	Descripción
1	0%	No documentado / no existente
2	25%	Aplicado, no documentado
3	50%	Documentado, no aplicado
4	75%	Aplicado y documentado
5	100%	Aplicado, documentado y controlado
6	N/A	No aplica

Tabla 1. Escala de valoración diagnóstico inicial

El porcentaje de cumplimiento de los requisitos establecidos en la norma NTC ISO/IEC 27001 [8] fue calculado mediante el total de cumplimiento de debes normativos por cláusula mediante la ecuación 1.

$$TDC = \sum_{i=1}^{5} DE_i - DE_6 \qquad \text{Ecuación 1}$$

Donde, TDC es el total de debes normativos por cláusula, DE es la cantidad de debes normativos, i es el índice de la escala de valoración, DE_6 es la cantidad de exclusiones.

Así mismo el porcentaje de cumplimiento por cláusula se determinó mediante la ecuación 2.

$$PI = \left(\sum_{i=1}^{5}(DE_i \times EV_i)\right) \div TDC \qquad \text{Ecuación 2}$$

Donde PI corresponde al porcentaje de implementación, DE es la cantidad total de debes normativos, EV es el valor porcentual de cumplimiento, TDC es el total de debes normativos por cláusula e i es el índice de la escala de valoración.

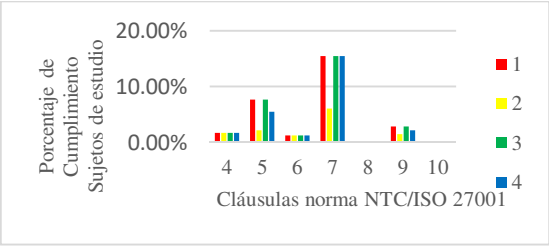

Figura 4. Porcentaje de cumplimiento de requisitos

Cláusulas	Sujetos de estudio comuna universidad			
	1	2	3	4
4	1.67%	1.67%	1.67%	1.67%
5	7.61%	2.17%	7.61%	5.43%
6	1.22%	1.22%	1.22%	1.22%
7	15.52%	6.03%	15.52%	15.52%
8	0.00%	0.00%	0.00%	0.00%
9	2.86%	1.43%	2.86%	2.14%
10	0.00%	0.00%	0.00%	0.00%

Tabla 2. Porcentaje de cumplimiento de requisitos NTC ISO/IEC 27001

Las brechas de cumplimiento obtenidas reflejan que ninguno de los sujetos de estudio adelanta acciones de manera activa para dar cumplimiento al Decreto Único Reglamentario 1078/2015 [5], los resultados fueron calculados mediante las ecuaciones 3 y 4.

$$PTI = \sum_{i=1}^{5}(DE_i \times EV_i) \div \sum_{j=4}^{10} TDC_j$$

Ecuación 3

$$Brecha = PTI - 100 \qquad \text{Ecuación 4}$$

Donde, PTI es el porcentaje de implementación total SGSI, DE es la cantidad de los debes normativos, EV es el valor porcentual de cumplimiento, TDC es el total de debes normativos por cláusula, i es el índice de la escala de valoración, j indica el índice de cláusula de la norma.

Sujetos de estudio	Porcentaje obtenido	Brechas de cumplimiento
1	4.79%	95.21%
2	2.10%	97.90%
3	4.79%	95.21%
4	4.34%	95.66%

Tabla 3. Brechas de cumplimiento de los sujetos de estudio

B. Grado de madurez

El modelo propuesto por MINTIC [9] consta de cinco niveles de madurez:

- Inicial.
- Gestionado.
- Definido.
- Gestionad cuantitativamente.
- Optimizado.

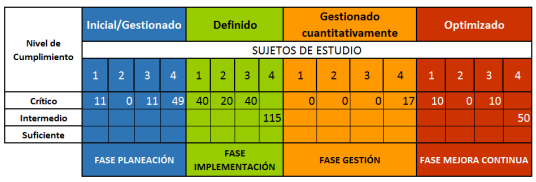

Figura 5. Grados de madurez IED's

Los sujetos de estudio se ubicaron en fase de planeación en nivel crítico, teniendo en cuenta que el instrumento del MINTIC establece que no puede pasar de fase en tanto no se cumpla el 100% de los requisitos de la fase previa. Los resultados obtenidos reflejan que no se han adelantado actividades tendientes a la definición de una estrategia metodológica que permita gestionar adecuadamente la seguridad de la información.

IV. ANÁLISIS DE RIESGOS DE LAS INSTITUCIONES EDUCATIVAS

El análisis de riesgos se llevó a cabo teniendo en cuenta los lineamientos de la norma ISO/IEC 27005 [10] y elementos de la norma NIST 800-30 [11].

A. Alcance

Se determinó que el área con información más sensible es la de secretaría académica, estableciendo está como alcance del estudio.

B. Inventario de activos

Se identificaron en total 21 activos comunes en los sujetos de estudio para el alcance establecido.

C. Factores de criticidad de los activos

Se identificaron los factores de criticidad de los activos de acuerdo a los criterios de disponibilidad, integridad y seguridad.

CRITERIO	FACTOR	CUESTIONAMIENTO
DISPONIBILIDAD	FINANCIERO	¿Es posible que se genere afectación financiera por falta de disponibilidad del activo?
	LEGAL	¿Es posible que se genere afectación legal por la falta de disponibilidad del activo?
	IMAGEN	¿Es posible que se genere afectación a la imagen de la IED y la satisfacción del cliente por falta de disponibilidad del activo?
INTEGRIDAD	FINANCIERO	¿Es posible que se genere afectación financiera por cambios no autorizados en el activo?
	LEGAL	¿Es posible que se genere afectación legal por cambios no autorizados en el activo?
	IMAGEN	¿Es posible que se genere afectación a la imagen de la IED y la satisfacción del cliente por cambios no autorizados en el activo?
CONFIDENCIALIDAD	FINANCIERO	¿Es posible que se genere afectación financiera por divulgación no autorizada de información sensible?
	LEGAL	¿Es posible que se genere afectación legal por divulgación no autorizada de información sensible?
	IMAGEN	¿Es posible que se genere afectación a la imagen de la IED y la satisfacción del cliente por divulgación no autorizada de información sensible?

Figura 6. Factores para determinar la criticidad de los activos

D. Niveles de criticidad de los activos

CRITERIO DE EVALUACIÓN	CALIFICACIÓN	CRITICIDAD
El activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información	>=33%	ALTO
El activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información	22%	MEDIO
El activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información	11%	BAJO
El activo no compromete la integridad, confidencialidad y disponibilidad de la información	0%	NO CRITICO

Figura 7. Niveles de criticidad de los activos

La calificación de los factores de criticidad de los activos, se da en un rango de 0 a 1 sin fracciones, por cuanto el máximo valor posible que pueden obtener es 9, calculando la criticidad mediante la ecuación 5.

$$NCA = \sum CFA \div Max(CFA) \qquad \text{Ecuación 6}$$

Donde NCA es el nivel de criticidad del activo, CFA representa la calificación de factores para el activo y Max(CFA) es el máximo valor posible de calificación de los factores para el activo.

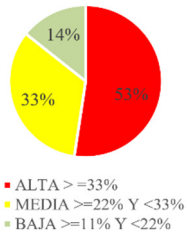

Figura 8. Criticidad de los activos

E. Escenarios de riesgos

Se identificaron un total de 55 escenarios de riesgos, en cada uno de los cuales se identificó el posible origen de ocurrencia, siendo DE = deliberado, AC = accidental y AMB = ambiental.

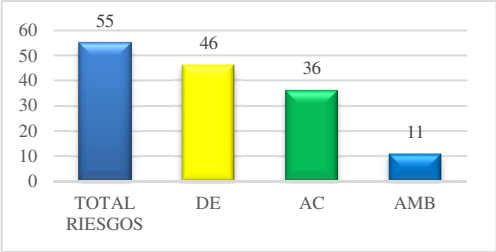

Figura 9. Escenarios de riesgos

F. Calificación de la probabilidad

VALOR	PROBABILIDAD	DESCRIPCIÓN
1	BAJO	Menos de 2 veces al año o baja probabilidad de ocurrencia
2	MEDIO	Entre 2 y 5 veces al año o mediana probabilidad de ocurrencia
3	ALTO	Más de 5 veces al año o alta probabilidad de ocurrencia

Figura 10. Calificación de probabilidad

G. Impacto potencial

CRITERIO	BAJO	MODERADO	ALTO
	1	2	3
CONFIDENCIALIDAD	La divulgación no autorizada de información de estudiantes y/o docentes podría tener un efecto adverso limitado en las operaciones de la IED, los activos o sus individuos	Se podría esperar que la divulgación no autorizada de información de estudiantes y/o docentes tenga un efecto adverso serio sobre las operaciones de la IED, los activos o sus individuos.	La divulgación no autorizada de información de estudiantes y/o docentes podría tener un efecto adverso grave o catastrófico en las operaciones de la IED, los activos o individuos.
INTEGRIDAD	La modificación o destrucción imprevista de información académica, personas, herramientas, dispositivos, etc podrían tener un efecto adverso limitado en las operaciones de la IED, los activos o sus individuos	La modificación o destrucción imprevista de información académica, personas, herramientas, dispositivos, etc podrían tener un efecto adverso serio en las operaciones de la IED, los activos o sus individuos	La modificación o destrucción imprevista de información académica, personas, herramientas, dispositivos, etc podrían tener un efecto adverso grave o catastrófico en las operaciones de la IED, los activos o sus individuos
DISPONIBILIDAD	La interrupción del acceso o uso de información académica o a un sistema de información podría tener un efecto adverso limitado en las operaciones de la IED, los activos o sus individuos.	La interrupción del acceso o uso de información académica o a un sistema de información podría tener un efecto adverso serio en las operaciones de la IED, los activos o sus individuos.	La interrupción del acceso o uso de información académica o a un sistema de información podría tener un efecto adverso grave o catastrófico en las operaciones de la IED, los activos o sus individuos.

Figura 11. Impacto potencial

H. Vulnerabilidad inherente

Para hallar la vulnerabilidad inherente se consignan los valores pertinentes a la probabilidad y el impacto para cada uno de los factores relacionados con confidencialidad,

integridad y disponibilidad. El cálculo del impacto total se realiza mediante la ecuación 7.

$$ITotal = Ic + Ii + Id \qquad \text{Ecuación 7}$$

Donde ITotal es el impacto total, Ic es la calificación del impacto en la confidencialidad, Ii es la calificación del impacto en la integridad y Id es la calificación del impacto en la disponibilidad.

La vulnerabilidad inherente por factor se calcula con la ecuación 8.

$$VIf = (P \times If)/Max(P \times If) \text{ Ecuación 8}$$

Donde, VIf es la vulnerabilidad inherente para cada factor, Ic es la calificación del impacto para el factor medido, P es la calificación de la probabilidad y Max(PxIf) es el máximo valor posible de la probabilidad por el impacto del factor medido.

Para hallar la vulnerabilidad inherente total se utiliza la ecuación 9.

$$VIt = (P \times (Ic + Ii + Id) \div Max(P \times (Ic + Ii + Id)) \text{ Ecuación 9}$$

Donde, VIt es la vulnerabilidad inherente total, Ic, Ii e Id es la vulnerabilidad inherente para la confidencialidad, integridad y disponibilidad respectivamente y Max(Px(Ic+Ii+Id)) es el máximo valor posible de la probabilidad por el impacto.

I. Aceptabilidad del riesgo

Identificación	Criterio	Calificación
Verde	Aceptable	<=25%
Amarillo	Tolerable	>25% y <=50%
Rojo	Inaceptable	>50%

Tabla 4. Aceptabilidad del riesgo

J. Mapas de temperatura de vulnerabilidad inherente

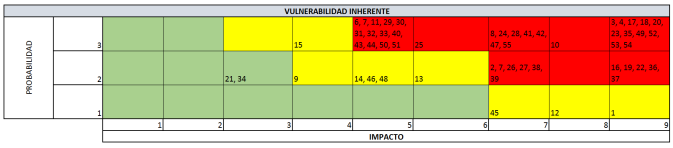

Figura 12. Vulnerabilidad inherente total

K. Controles del anexo A de la norma NTC ISO/IEC 27001 identificados actualmente

Se identificaron un total de 20 controles del anexo A de la norma NTC ISO/IEC 27001 [8], que actualmente se emplean en las IED's.

L. Mapas de temperatura de vulnerabilidad residual

Se empleó la misma metodología que para el cálculo de la vulnerabilidad inherente.

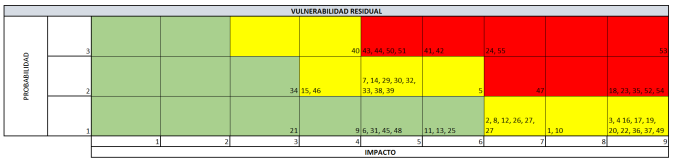

Figura 13. Vulnerabilidad residual total

M. Plan de tratamiento de riesgos

Se definió un plan de tratamiento de riesgos que fuera alcanzable desde el punto de vista de la ejecución presupuestal, involucrando 38 controles del anexo A de la norma NTC ISO/IEC 27001 adicionales a los ya identificados.

N. Declaración de aplicabilidad

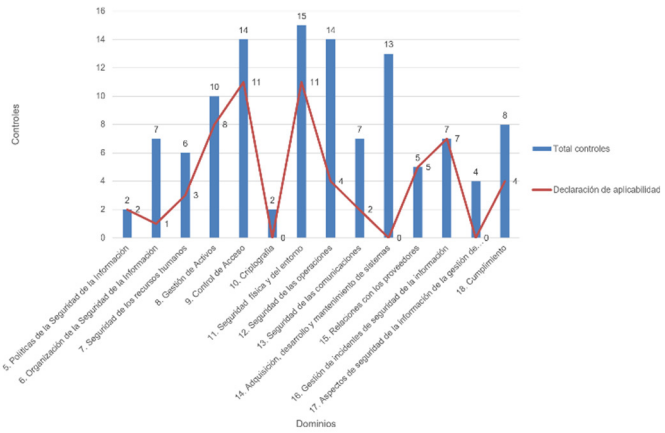

Figura 14. Declaración de aplicabilidad

Se emplearon en total 11 dominios de los 14 propuestos por el anexo A de la norma NTC ISO/IEC 27001 y 58 controles.

V. MODELO DE SGSI PROPUESTO PARA IED'S

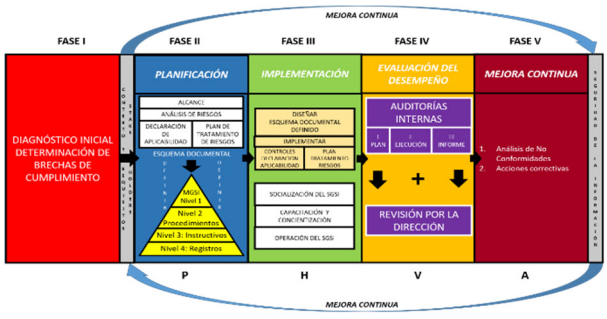

Figura 15. Esquema general del modelo de SGSI propuesto

El modelo propuesto acoge las mejores prácticas propuestas por MINTIC, para el logro de la estrategia de GEL, así como

las disposiciones del MEN y los requisitos de la norma NTC ISO/IEC 27001. Las fases propuestas se encuentran alineadas con el Modelo de Seguridad y Privacidad establecido por MINTIC, esquematizando la relación secuencial y las actividades relevantes en cada una de ellas, facilitando su implementación en las IED's.

A. Fase I – diagnóstico inicial

El objetivo de esta fase es determinar el grado de cumplimiento de la IED con relación a la totalidad de requisitos establecidos en la norma NTC ISO/IEC 27001.

B. Fase II – planificación

Se lleva a cabo el análisis de riesgos, se define el plan de tratamiento de riesgos y se determina la declaración de aplicabilidad, igualmente de acuerdo a los resultados obtenidos se define la documentación necesaria para dar cumplimiento a los requisitos normativos.

Es importante realizar un análisis de riesgos un análisis de riesgos asociado a las características particulares de la IED con el fin de cubrir el 100% de las vulnerabilidades institucionales asociadas a temas de mejoramiento y sostenibilidad de su infraestructura.

C. Fase III – implementación

La IED debe diseñar y poner en marcha la documentación en todos sus niveles, igualmente debe gestionar la operación del plan de tratamiento de riesgos y la aplicación de los controles establecidos en la declaración de aplicabilidad.

Es necesario planificar un proceso de concientización y socialización de los riesgos a los cuales se encuentra expuesta la IED con la planta de personal en términos de la vulnerabilidad de la información sensible de los niños.

D. Fase IV – evaluación del desempeño

Se deben planificar la ejecución de las auditorías internas y las revisiones por la dirección.

E. Fase V – mejora continua

En esta fase se revisan los resultados de la fase anterior, permitiendo el análisis de causas para las desviaciones o no conformidades encontradas, de tal manera que los planes de mejoramiento se conviertan en acciones contundentes que impidan la repetición de la desviación.

La documentación está conformada por 4 niveles, organizados en forma piramidal.

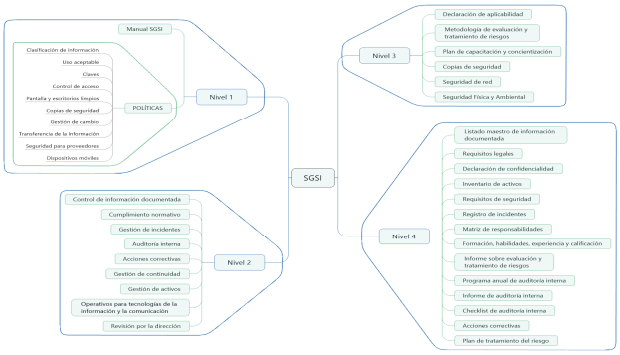

Figura 16. Esquema documental base

El nivel 1 contiene los manuales y las políticas, el nivel 2 los procedimientos, el nivel 3 los instructivos y el nivel 4 los formatos.

Es importante tener en cuenta que las IED's emplean controles tendientes a la mitigación de la probabilidad de ocurrencia, descuidando notablemente los controles que mitiguen el impacto nocivo de la materialización de los riesgos identificados.

VI. CONCLUSIONES

- El establecimiento de un modelo de sistema de gestión de seguridad de la información basado en la norma NTC ISO/IEC 27001 para IED's de carácter público, proporciona una línea base para el cumplimiento del Decreto Único Reglamentario 1078/2015 componente "seguridad y privacidad de la información", a la vez que permite cumplir con los mandatos emanados por el Decreto 1526/2002 del MEN, en lo referente a la calidad de la información y la responsabilidad de las entidades territoriales de realizar auditorías por lo menos una vez al año a la población matriculada y a los docentes ayudando a preparar a las IED's para estos procesos de verificación.
- En concordancia con lo estipulado por el Decreto 1377/2013 Art. 7, en referencia a la capacitación sobre la identificación de riesgos en los niños, niñas y adolescentes respecto del tratamiento indebido de la información personal, la aplicación de los controles seleccionados permite disminuir los riesgos que con respecto al particular fueron encontrados en el área de secretaría académica.
- Las contiendas políticas incrementan los riesgos de exposición de información institucional, particularmente en temporada de elecciones, constituyendo este un riesgo que va en detrimento de la IED y de la información de los niños, niñas, adolescentes, docentes y personal administrativo.
- Existe una falta de entendimiento por parte del personal responsable de la administración, mantenimiento y control de la información de los niños, niñas, adolescentes y docentes sobre el

impacto de la materialización de los riesgos de seguridad de la información.

- El modelo de SGSI constituye una herramienta que genera cultura sobre la disposición de los desechos tecnológicos de las IED's previniendo que las áreas circundantes se vean contaminadas visual y químicamente por el inadecuado manejo de los activos que han sido dados de baja del inventario.
- El modelo de SGSI propuesto, da su aporte social evitando que la información sensible de los niños, niñas y adolescentes sea manipulada por personas inescrupulosas que la emplean con la finalidad de involucrar a los menores en redes de prostitución y pornografía infantil.
- El modelo constituye una base para garantizar la Confidencialidad, la Integridad y la Disponibilidad de la información sensible de niños, niñas adolescentes, docentes y personal administrativo, en procura del cumplimiento de lo dispuesto en el Decreto Único Reglamentario 1075/2015 del Sector Educación, el Decreto Único Reglamentario 1078/2015 del Sector TIC componente "Seguridad y privacidad de la información", alineado con el modelo expuesto por MINTIC.

REFERENCIAS

[1]. Comisión de derechos humanos. (1948). Declaración universal de los derechos humanos. Paris, Francia.

[2]. UNICEF Comité Español. (2006). Convención sobre los derechos del niño. Madrid, España: Nuevo siglo.

[3]. Naciones Unidas. (1976). Pacto internacional de los derechos económicos, sociales y culturales.

[4]. León Zuluaga, M., & Grajales Valencia , L. (2016). Diagnóstico del grado de madurez de los controles de seguridad establecidos en la Norma NTC ISO/IEC 27001:2013 para asegurar la confidencialidad, integridad, disponibilidad y control de la información en instituciones públicas de educación preescolar de la. Pereira, Risaralda.

[5]. Decreto 1078. (2015). "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". Bogotá.

[6]. Ley 489. (1998). por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189. Bogotá.

[7]. Presidencia de la Republica de Colombia. (2002). Decreto 1526. Bogotá.

[8]. NTC ISO/IEC 27001. (2013). Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá.

[9]. Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC. (2015). Guía encuesta diagnóstico modelo de seguridad de la información para las entidades del estado. Bogotá, Colombia.

[10]. Ramírez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16(2).

[11]. Betancourt Correa, L., Posada Bonilla, D., & Rangel García, C. (2014). Diseño del sistema de gestión de seguridad de la información (SGSI) para el proceso administrativo de la alcaldía de Manizales. Tesis, Universidad Autónoma de Manizales, Manizales, Caldas.

[12]. Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC. (2015). Modelo de seguridad y privacidad de la información. Bogotá, Colombia.

[13]. Aliaga Flórez, L. C. (2013). Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo. Lima, Perú.

[14]. AS/NZS. (1999). Estándar Australiano AS/NZS 4360:1999 Administración de riesgos.

[15]. Betancourt Correa, L., Posada Bonilla, D., & Rangel García, C. (2014). Diseño del sistema de gestión de seguridad de la información (SGSI) para el proceso administrativo de la alcaldía de Manizales. Tesis, Universidad Autónoma de Manizales, Manizales, Caldas.

[16]. Buitrago Estrada, J. C., Bonilla Pineda, D. H., & Murillo Varón, C. E. (2012). Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información SGSI en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001. Universidad EAN, Bogotá.

[17]. Caviedes Sanabria, F., & Prado Urrego, B. (2012). Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización. Tesis, Universidad ICESI, Santiago de Cali, Valle del Cauca.

[18]. Codesocial. (2009). Organización del Sistema Educativo, Conceptos Generales de la Educación Preescolar, Básica y Media. Revolución Educativa Colombia aprende, 11.

[19]. Condori Benavides, I. (2015). Informe de Control Interno II Congreso Nacional de Contabilidad. Universidad Autónoma del Perú, Lima, Perú.

[20]. Constitución Política de Colombia. (1991). Constitución Política de Colombia. Bogotá.

[21]. Departamento Nacional de Planeación. (2016). Política nacional de seguridad digital. Consejo Nacional de Política Económica y Social, Bogotá, Colombia.

[22]. Détienne, F., Rouet, J.-F., Burkhardt, J.-M., Deleuze-Dordron, C., Kumar, R., Khan, S., . . .

Turnes, L. (2002). Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. En N. I. Technology, Journal of Systems and Software (Vol. 30, págs. 1-22). Falls Church, VA: Booz Allen Hamilton Inc. doi:10.1111/j.1745-6622.2008.00202.x

[23]. Espinosa Betancur, J. G., García Gallo, R. S., & Giraldo Restrepo, A. (2016). Sistema de gestión de seguridad de la información para los tres procesos misionales de la corporación autónoma regional de risaralda (CARDER). Manizales, Caldas.

[24]. Espinosa T., D., Martínez P., J., & Amador D., S. (02 de 12 de 2014). Gestión del riesgo en la seguridad de la información base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología octave-s. Ing. USBMed, 5(2), 33-43.

[25]. Fernández Martín, I. (2013). Implantación de la metodología BPM en la Eps: Aplicación para la gestión de comisiones. Alicante.

[26]. Garimella, K., Lees, M., & Williams, B. (2014). BPM - Gerencia de procesos de negocios.

[27]. Grinnel, R. (1997). Social work research of evaluation: Quantitative and qualitative approaches (5a. ed.). Itasca, Illinois: Peacock Publishers.

[28]. Irrazabal, M., Gómez, D., & Cardoso, W. (2013). SGSI: de la academia a la práctica. Montevideo, Uruguay: ISACA.

[29]. ISACA. (2009). Marcos de riesgos de TI. Rolling, meadows.

[30]. ISACA. (2012). COBIT 5 Un marco de negocio para el gobierno y la gestión de las TI de la empresa. Rolling Meadows, EE.UU. Obtenido de www.isaca.org/COBITuse

[31]. ISO. (2009). Norma ISO 31000 versión 2009: Gestión de riesgos - principios y guías. Switzerland. Obtenido de www.iso.org

[32]. ISO. (2014). International standard ISO/IEC 27000. Switzerland: ISO. Obtenido de www.iso.org

[33]. ISO/IEC 31000. (2009). Gestión de RIesgos. Bogotá.

[34]. ISO27000.es. (16 de enero de 2017). El portal de ISO 27001 en español. Obtenido de Iso27000.es: http://iso27000.es/iso27002.html

[35]. ISO27000.es. (s.f.). ISO 27000.es. Obtenido de http://www.iso27000.es/sgsi.html

[36]. Ley 115. (1994). Por la cual se expide la ley general de educación. Bogotá.

[37]. Ley 1581. (2012). Por lo cual se dictan disposiciones generales para la Protección de Datos Personales. Bogotá.

[38]. Ley 715. (2001). Por la cual se dictan normas orgánicas en materia de recursos y competencias de conformidad con los artículos. Bogotá.

[39]. M. Talabis, M. R., & L. Martín, J. (2013). Herramientas para la Evaluación de Riesgos. United States of America: ELSEVIER.

[40]. Ministerio de hacienda y administraciones publicas, Gobierno de España. (2012). MAGERIT - versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información. Dirección general de modernización administrativa procedimientos e impulso de la administración electrónica. Madrid, España: Ministerio de Hacienda y Administraciones Públicas. Obtenido de http://administracionelectronica.gob.es/

[41]. Ministerio de la Presidencia. (2010). Boletín oficial del Estado. España. Obtenido de https://www.boe.es

[42]. MINTIC. (2015). Índice de Gobierno en Línea. Obtenido de Indice de Gobierno en Línea: http://indicegel.gobiernoenlinea.gov.co/Resultados_Sector.aspx

[43]. MINTIC. (2015). Manual estrategia de gobierno en línea. Bogotá, Colombia. Obtenido de http://estrategia.gobiernoenlinea.gov.co

[44]. MINTIC. (2016). Guía de gestión de riesgos. Bogotá, Colombia.

[45]. Monserrat, S. (2008). La Ecología de la Información: Un nuevo paradigma de la infosfera. Pliegos de Yuste (7 - 8).

[46]. Muñoz, M. (2013). Introduccion Octave. En S. E. Institute, Journal of Chemical Information and Modeling (págs. 1689-1699). Carnegie Mellon University. doi:10.1017/CBO9781107415324.004

[47]. Novoa, A., & Helena, C. (2015). Metodología para la Implementación de un SGSI en la Fundación Universitaria Juan de Castellanos, Bajo la Norma ISO 27001:2005. Tesis, Universidad Internacional de la Rioja, Tunja, Boyacá.

[48]. OSI ISO-7498-2. (1989). Modelo Arquitectura de Seguridad.

[49]. Peña Ibarra, J. (2009). Metodologías y normas para el análisis de riesgos. Monterrey. México: ISACA.

[50]. Torres Bermúdez, A. (2010). Introducción a la seguridad informática. Bogotá, Colombia.

[51]. Velásquez Isaza, J. (2015). Modelamiento de los procesos de auditoría en seguridad de la información asociados a los dominios 6, 8, 13 Y 14 del anexo A de La norma ISO 27001 mediante una herramienta de flujo de trabajo. Tesis, Universidad Tecnológica de Pereira, Pereira, Risaralda. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/11059/5118/1/0058V434.pdf