MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN COMO REFERENTE PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR (IES)

Diego Mauricio Bernal Ríos[1]

Diana Paola Carreño León[2]

RESUMEN

La implementación de modelos de Gestión de la Información genera variables de confianza en la gestión del entorno referente a la información, ya que los sistemas de información, sus datos, estructura pueden ser sujetos a amenazas externas o internas que pueden afectar a la operatividad de los sistemas, para esto se deben identificar los riesgos, y se deben establecer medidas sobre la seguridad física, técnica y lógica (Vite Cevallos et al., 2018).

Este artículo nos ilustra las fases para diseñar un modelo de gestión de seguridad de la información, que busca disminuir amenazas y riesgos en las IES, siendo indispensable e importante contar con un plan de acción frente a estas, logrando mitigar el impacto y evaluar su funcionamiento.

Las directrices de la Norma ISO 27001 expresan los lineamientos, estándares y mejores prácticas de seguridad de la información para ser aplicadas e implementadas en las organizaciones.

PALABRAS CLAVE

Educación Superior, Gestión de la información, Modelos, Seguridad, Sistemas.

[1] Licenciado en Informática y Tecnología Universidad Pedagógica y Tecnológica de Colombia, Estudiante Especialización en Auditoría y Aseguramiento de la Información Universidad Santo Tomás Seccional Tunja.

[2] Contadora Pública - Universidad Santo Tomás Seccional Tunja, Especialista en Contabilidad Financiera Internacional - Pontificia Universidad Javeriana, Estudiante Especialización en Auditoría y Aseguramiento de la Información - Universidad Santo Tomás Seccional Tunja.

ABSTRACT

The implementation of Information Management models generates confidence variables in the management of the information environment, since the information systems, their data, and structure can be subject to external or internal threats that can affect the operation of the systems, for this, risks must be identified, and measures must be established on physical, technical and logical security (Vite Cevallos et al., 2018).

This article illustrates the phases to design an information security management model, managing to reduce threats and risks in HEIs, being essential and important to have an action plan against them, which allows to mitigate the impact.

The guidelines of the ISO 27001 Standard express the information security guidelines, standards and best practices to be applied and implemented in organizations.

KEYWORDS

Higher education, Information management, Models, Security, Systems

INTRODUCCIÓN

Los Sistemas de Gestión de Seguridad de la Información se implementan en las organizaciones con el fin de disminuir las amenazas, que se presentan siendo gestionado con gran facilidad gracias al uso de la tecnología, así mismo, buscan limitar riesgos y evitar afectaciones en el funcionamiento de sus actividades.

Para las Universidades la información es uno de los activos más importantes y por lo tanto debe ser protegido de forma adecuada. La seguridad de la información gira en torno a los conceptos de confidencialidad, integridad y disponibilidad de información y en los últimos años se ha incrementado su importancia en las organizaciones modernas, entre ellas en las instituciones de educación superior, como indica (Bongiovanni, 2019 ed all) citado por (Secaira et al., 2020)

Las entidades del sector educativo en el orden profesional son las salvaguardas de la información educativa de sus estudiantes activos y egresados, propenden por optar estrategias para evitar los delitos informáticos y de esta forma garantizar que la información que certifican es legítima y veraz, siendo este el objetivo primordial

de las autoridades y funcionarios a cargo de la información académica de las universidades colombianas. (Montilla Malaver & 10184589, 2020).

Las IES (Instituciones de Educación Superior) implementan plataformas tecnológicas que recopilan y almacenan sus datos, estos tienden a encontrarse dispersos, duplicados, incompletos o en diferentes formatos, pues son procesados en distintas aplicaciones. Esta situación hace que se puedan generar errores e inconsistencias en los reportes que son entregados a la comunidad interna y externa, quienes asumen la información recibida como cierta y veraz (OSORIO Sanabria et al., 2017, p. 3)

A raíz del aumento en la generación de los datos, dentro y fuera de las entidades, y con el aumento de las posibilidades de acceso a los mismos, cada vez más organizaciones se han dado cuenta de la importancia de gestionar y gobernar sus datos como un recurso a nivel estratégico que optimicen sus procesos. Las IES como organizaciones generadoras de conocimiento no son ajenas a esta situación dado que necesitan insumos y herramientas que apoyen la gestión de sus procesos misionales, de manera que puedan responder a las demandas de su entorno (OSORIO Sanabria et al., 2017).

En ese sentido y según La Republica (Paola Andrea Vargas Rubio, 2020), por la situación sanitaria actual, han tenido que implementar diferentes estrategias para la oferta de sus servicios lo cual ha traído consigo retos en materia de seguridad informática. En el caso de Colombia, el país se encuentra en el puesto 39 del ranking de ciberseguridad mundial. Dinamarca es el país que cuenta con mayor seguridad informática en el mundo, debido a que solo registra, por ejemplo, 2,57% de dispositivos móviles infectados con malware, 0,1% de ataques de malware financiero y 3,5% de computadoras infectadas con malware, según un estudio de Comparitech. Desde el punto de vista operativo, este escenario podría encender las alarmas a nivel nacional debido a que "*las conexiones durante la pandemia se han incrementado en más de 40%, lo cual hace que los riesgos aumenten dada la mayor exposición de los usuarios a ciberataques (...) Los delincuentes utilizan multitud de técnicas para sustraer de manera ilegal información*", aseguró Gerardo González, gerente transformación de Sonda Colombia.

El gerente de transformación de Sonda Colombia, explicó que "*en tiempos de*

cuarentena muchas personas han tenido que trabajar desde casa y los ciberdelincuentes sacan provecho de esto para hacerse pasar por organismo, infectar sistemas, conseguir datos o para secuestrar sistemas informáticos y pedir un rescate a cambio. Los ataques más frecuentados durante esta temporada son phishing, malware de red e ingeniería social".

En este escenario, las IES cuentan con diferentes documentos, herramientas informáticas o sistemas robustos para la recopilación de la información que obtiene en custodia de estudiantes aspirantes para ingreso, activos, egresados, graduados, docentes activos y no activos, administrativos, de recursos y otro sin número de información de la que no puede llegar a garantizar que sea una información consistente, confiable, completa, sin duplicidad y unificada proporcionando datos que generan errores en informes presentados externa e internamente, siendo un punto de partida para la aplicación de normas que permitan generar un nivel de confianza alto en cada proceso realizado por la IES en el manejo de la información.

Es así, como en el presente artículo se propone diseñar un modelo de gestión de seguridad de la información para IES tomando referentes nacionales e internacionales además de las directrices establecidas en la Norma ISO 27001, en pro de garantizar la seguridad, el buen manejo y gestión de la información evaluando se cuente, apliquen procesos y procedimientos de seguridad y privacidad de información evitando pérdidas, malversación, mal manejo y robo de información que impacte de manera directa el desarrollo de las funciones adjetivas y sustantivas de las IES.

DESARROLLO

REFERENTES TEÓRICOS

Durante el proceso de investigación, contamos con fundamentos teóricos que guiaron y aportaron al desarrollo de la misma, algunos de ellos son:

Sistema de Gestión

Un sistema de gestión es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización, el cual ayuda a lograr los objetivos de la organización mediante una serie de estrategias, que incluyen la optimización de procesos, el enfoque centrado en la gestión y el

pensamiento disciplinado. (Frayssinet Delgado, 2017)

Gestión de la Información

La gestión de la información es el proceso de organizar, evaluar, presentar, comparar los datos en un determinado contexto, controlando su calidad, de manera que esta sea veraz, oportuna, significativa, exacta y útil y que esta información esté disponible en el momento que se le necesite. Esta se encamina al manejo de la información, documentos, metodologías, informes, publicaciones, soportes y flujos en función de los objetivos estratégicos de una organización (Torres Lebrato, 2015)

La gestión de la información en las organizaciones educativas es de vital importancia, lo que implica determinar la información que se necesita, la fuente, el modo de obtención, almacenamiento, así como, establecer el método correcto de distribución y empleo. Ello significa que la información es un recurso estratégico que puede utilizarse para alcanzar objetivos, optimizar los procesos de toma de decisiones, enseñar, aprender y generar nuevos conocimientos. (Barzaga Sablón et al., 2019)

Sistemas de información

Un sistema de información es un conjunto de elementos interrelacionados que recaban, procesan, almacenan y distribuyen datos e información, y, además, proporcionan mecanismos de retroalimentación para alcanzar un objetivo. Diariamente interactuamos con sistemas de información tanto a nivel personal como profesional.

Es un conjunto de componentes interrelacionados que reúne, procesan, almacenan y distribuyen datos e información y proporcionan un mecanismo de retroalimentación para cumplir un objetivo. Este mecanismo es el que ayuda a las organizaciones a lograr sus objetivos, como incrementar sus ganancias o mejorar su servicio al cliente. (Ralph M. Stair; George W. Reynolds, 2016)

Seguridad de la información

La seguridad de la información es una disciplina asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación

y adecuada presentación (Valencia-Duque & Orozco-Alzate, 2017, p. 3)

La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 18)

Antes de abordar un enfoque metodológico para implementar un SGSI es necesario aclarar la diferencia entre seguridad informática y seguridad de la información, la cual radica en el tipo de recursos sobre los que actúa cada una. Mientras que la primera se enfoca en la tecnología propiamente dicha, i.e. En las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, la segunda está relacionada con la información en sí misma, como activo estratégico de la organización (Valencia-Duque & Orozco-Alzate, 2017)

ISO 27001

La ISO 27001 especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas. El SGSI está diseñado para obtener controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas (Instituto Colombiano de Normas Técnicas y Certificación, 2013).

Sistema de Gestión de Seguridad de la Información

La gestión de la información se refiere al conjunto de procesos que sirven para designar actividades orientadas a la generación, coordinación, almacenamiento, conservación, búsqueda y recuperación de la información tanto interna como externa contenida en cualquier soporte (Barzaga Sablón et al., 2019).

Un SGSI (Sistema de Gestión de Seguridad de la Información) proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información para lograr objetivos de negocio (Frayssinet Delgado, 2017).

Para estructurar un sistema de gestión de la seguridad de la información (SGSI) se adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), así mismo, el modelo PHVA también refleja los principios que controlan la seguridad de sistemas y redes de la información. La Figura 1 ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas.

Su implementación genera variables de confianza en la gestión del entorno referente a la información. El volumen de la información dentro de las organizaciones requiere del uso de medidas tecnológicas que faciliten la gestión adecuada, considerando la criticidad de los datos, de acuerdo a la actividad económica donde se desarrolle. (Vite Cevallos et al., 2018)

Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información

Según (Valencia-Duque & Orozco-Alzate, 2017) existen diversas formas de llevar a cabo una implementación de un SGSI en una organización, no obstante, para lograr cierto nivel de éxito y disminuir la incertidumbre en sus resultados, se debe adoptar un enfoque que permita abordar, desde una perspectiva sistémica, la forma de cumplir con los elementos que hacen parte de éste.

La metodología contempla cinco (5) fases secuenciales, las cuales serán detalladas para poder comprender los pasos a desarrollar no sólo desde el punto de vista conceptual sino metodológico, a partir de un proyecto que incorpore personas, tiempos y recursos, así como el respaldo de la alta Dirección, como un requisito fundamental para cumplir los objetivos previstos. Estas cinco fases con sus respectivas etapas están distribuidas en función de la norma ISO/IEC 27001.

Fase 1. Aprobación de la dirección para iniciar el proyecto: Para

cumplir con este propósito se deben llevar a cabo las siguientes actividades:

- Establecimiento de las prioridades de la organización para desarrollar un SGSI
- Definir el alcance preliminar del SGSI
- Creación del plan del proyecto para ser aprobado por la Dirección

Fase 2. Definir el alcance, los límites y la política del SGSI: Esta fase contempla los siguientes elementos:

- Definición del alcance
- Definición de la política y objetivos de seguridad
- Aprobación de la Dirección

Fase 3. Análisis de los requisitos de seguridad de la información:

- Establecer los requisitos de seguridad de la información
- Identificar los activos dentro del alcance
- Realizar una evaluación de la seguridad de la información

Fase 4. Valoración de riesgos y planificar el tratamiento de riesgos: Sin duda este es el eje principal del SGSI, cuyo principal referente es la norma ISO/IEC 27005. Al respecto se debe tener en cuenta:

- Establecimiento de contexto
- Parámetros de probabilidad
- Parámetros de impacto
- Determinación de la vulnerabilidad
- Criterios de aceptabilidad del riesgo
- Valoración del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo

Fase 5. Diseñar el SGSI: El diseño del SGSI contempla básicamente tres componentes:

- La documentación que debe tener el sistema
- La implementación de los controles previstos en el plan de tratamiento de riesgos

- El monitoreo constante de la seguridad de la información

Auditoría a la Seguridad de la Información

Según (Solarte Solarte et al., 2015) la metodología para realizar la auditoría a la seguridad de la información, se divide en etapas sucesivas y sistemáticas; ya que se plantea que la auditoría debe ser periódica o permanente dependiendo de la organización y los cambios en la tecnología de información usada en el tratamiento y procesamiento de la información.

Fase I. Determinación de vulnerabilidades, amenazas y riesgos: Se hace el estudio de las vulnerabilidades, amenazas y riesgos para los procesos y sistemas implementados actualmente en las organizaciones, que fueron objeto de la investigación.

Fase II. : Análisis de riesgos y diagnóstico de la seguridad de la información: Se realizará el proceso de análisis y evaluación de riesgos de acuerdo al estándar MAGERIT que permite valorar los riesgos en cada uno de los criterios de información evaluados, identificando las posibles causas que los originan y que posteriormente permitan definir un sistema de control de seguridad de acuerdo a los hallazgos confirmados, lo que permitirá disminuir el impacto en la organización y probabilidad de ocurrencia de los mismos

Fase III. Definición de controles para el diseño del SGSI que incluya políticas y procedimientos para mitigar los riesgos: Se hace el estudio de las causas que originan los hallazgos. Una vez confirmados, se definen los controles apropiados de acuerdo a la norma ISO/IEC 27002 se establece su tratamiento, y finalmente, se diseñan las políticas y procedimientos dentro de las cuales se incluyen los controles, y que finalmente irán en el diseño del SGSI.

METODOLOGÍA

El presente artículo se desarrolló a través de una investigación mixta documental - descriptiva de las necesidades de seguridad de la información en las IES. Se llevó a cabo por medio de una metodología de investigación exploratoria, la cual tuvo por objetivo general diseñar un modelo de Gestión de Seguridad de la Información en

Instituciones de Educación Superior.

Para el diseño del modelo de seguridad de la información se tuvieron en cuenta los modelos existentes de Valencia-Duque, F. J., & Orozco-Alzate, M. (2017), la UPTC - Universidad pedagógica y tecnológica de Colombia- y la ESAP -Escuela Superior de Administración Pública-, por medio de pasos, las cuales responden a los objetivos específicos propuestos de la siguiente manera:

Paso I. Se realizó el estado del arte de los modelos existentes para la Gestión de Seguridad de la Información en las IES, a través de una búsqueda literaria, mediante recursos tecnológicos como Google Scholar, Scielo, redaltcit, dialnet, la referencia, identificando los principales autores que hablan de seguridad de la información en el mundo, y se realizó una revisión de los diferentes modelos existentes aplicados en las diferentes IES u organizaciones similares.

Paso II. Se identificaron las debilidades de gestión de seguridad de información en las IES de carácter privado, como referente para este estudio se tomó la Usta Tunja, en donde se realizó una indagación (entrevista semi-estructurada) al Departamento de TIC (Tecnologías de la Información y Comunicación), con el fin de identificar posibles casos de ataques, así mismo, se verificó la existencia e implementación de políticas de tratamiento de datos y controles utilizados para determinar posibles falencias y oportunidades de mejora.

Paso III. Se realizó un análisis comparativo de los modelos existentes con el fin de identificar características o parámetros que se ajusten a las necesidades de seguridad de la información de las IES, por medio de recolección de datos de diferentes autores.

Paso IV. Se diseñó un modelo de gestión de seguridad de la información basado en los existentes, que permitiera suplir las debilidades y necesidades de seguridad de la información, y que sirviera como referente para la gestión de la información de IES o con características similares.

RESULTADOS

Los resultados se describen de esta manera:

Para el **paso I**, se identificaron modelos existentes similares como:

★ **Universidad Pedagógica y Tecnológica de Colombia UPTC**

La UPTC propuso y desarrolló el Modelo de Seguridad y Privacidad de la Información documentada por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC- en donde se implementan cinco (5) fases, las cuales buscan que las entidades gestionen adecuadamente la seguridad y privacidad de sus activos de información.

En este sentido, la seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad (UPTC, 2016).

Es así, como se muestra en la figura 1, que se desarrolla el Modelo de Seguridad y Privacidad de la Información MSPI con el siguiente modelo:

***Figura 1**:* Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Fuente: Modelo de seguridad y privacidad de la información UPTC

A continuación, se describe cada actividad específica desarrollada en cada fase del ciclo de operación del Modelo de Seguridad y Privacidad de la Información.

Fase I Diagnóstico: En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, Determinar el estado actual de la gestión de la seguridad y privacidad de la información al interior de la entidad, Identificar el avance de la implementación del ciclo de operación al interior de la entidad,

Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales, Identificar el uso de buenas prácticas en ciberseguridad.

Fase II Planificación: En esta fase es indispensable hacer uso de los resultados de la etapa anterior, elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información y generarla por medio de una metodología de gestión del riesgo. Para ello deben ajustarse las políticas, los procesos y procedimientos ya definidos en el modelo de seguridad con el fin de incorporar la privacidad con el alcance mencionado.

Fase III Implementación: Esta fase permite continuar con la implementación de la planificación realizada en la fase anterior del MSPI y con base a los resultados de la fase de planeación se deben ejecutar las siguientes actividades: Planificación y Control Operacional, Implementación del plan de tratamiento de riesgos, Indicadores De Gestión, Plan de Transición de IPv4 a IPv6

Fase IV Evaluación de Desempeño: El proceso de seguimiento y monitoreo se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Fase V Mejora Continua: Una vez se tengan los resultados del componente de evaluación del desempeño se toman los resultados obtenidos y se preparan los correctivos necesarios que permitan a la misma crecer en el nivel de responsabilidad demostrada.

En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño, este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI
- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI

★ **Plan de Seguridad y Privacidad de la Información Escuela de Administración Pública Territorial**

Según el Plan de Seguridad de la ESAP (ESAP Oficina de Sistemas e Informática - OSI Seguridad, 2018); considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, los procesos de la ESAP, y los lineamientos del Modelo de Seguridad y Privacidad de la Información MSPI con el fin de determinar la estrategia de implementación de los controles de seguridad requeridos para la ESAP.

En este Plan de Seguridad desarrolló la metodología como lo muestra la figura 2:

Figura 2: *Metodología Utilizada ESAP*

Fuente: Plan de seguridad y privacidad de la información ESAP

1. **CONTEXTO** Se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad.

   Entre los aspectos que se deben considerar para lograr este entendimiento están: La misión, La visión, Historia y antecedentes, Estructura organizacional, Procesos, Cultura y valores y Legislación pertinente

2. **SITUACIÓN ACTUAL** En esta fase se expresa el nivel de madurez que posee en este momento la ESAP con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina análisis GAP o análisis de brecha, como indica la figura 3. Para poder realizar el Plan de Seguridad y Privacidad de la Información es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios con el fin de plantear prioridades sobre su implementación.

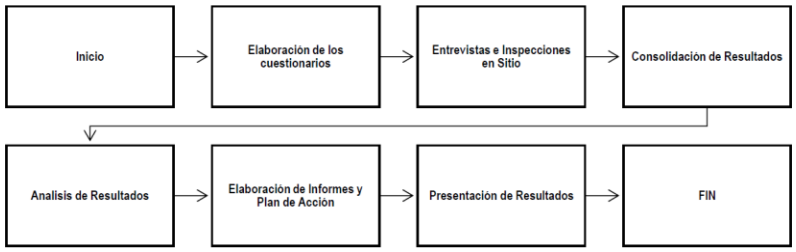

Figura 3. *Metodología utilizada en el GAP*

Fuente: Plan de seguridad y privacidad de la información ESAP

3. **DEFINICIÓN DE VARIABLES PARA EL ANÁLISIS** Para la realización del análisis dentro del Plan de Seguridad y Privacidad de la Información es necesario definir una serie de variables que ayuden a la priorización de los diferentes dominios de la NTC/ISO 27001:2013. Estos son: Prioridad de Planeación, Documentación política, Documentación procedimientos, Documentación estándares, Costo de implementación, Gasto de mantenimiento, Complejidad y Tiempo
4. **INFORME DE RESULTADOS** Con el fin de estimar las prioridades para cada uno de los dominios de la norma ISO 27001 se definieron una serie de variables que una vez calificadas se utilizaron para determinar la prioridad estratégica de implementación de los dominios y que fueron presentadas anteriormente

★ **Modelo Bell-LaPadula**

Modelo multinivel propuesto para fortalecer el control de acceso en aplicaciones militares y del gobierno. En estas aplicaciones, generalmente los sujetos están divididos en diferentes niveles de seguridad. Un sujeto puede acceder a objetos hasta ciertos niveles, determinado por su nivel de seguridad, por ejemplo: no cualquiera podría tener acceso a información clasificada como top secret (Arcila B, 2019).

El modelo Bell-Lapadula es un modelo enfocado en la confidencialidad y define dos reglas de control de acceso mandatorio (MAC) y una regla de control de acceso discrecional (DAC) con tres propiedades de seguridad:

- La propiedad de seguridad simple: un sujeto en un nivel de seguridad dado no puede leer un objeto de un nivel de seguridad mayor.

- ❖ La propiedad estrella: un sujeto en un nivel de seguridad dado no puede escribir en algún objeto de un nivel de seguridad menor.
- ❖ La propiedad de seguridad discrecional: el uso de una matriz de acceso para especificar el control de acceso discrecional.

★ **Modelo de BIBA**

Modelo que describe un conjunto de reglas de control de acceso diseñadas para asegurar la integridad de los datos, los datos y los sujetos son agrupados en niveles ordenados de integridad. El modelo se diseñó para que los sujetos no puedan acceder a objetos en un rango superior al de ellos o a objetos de menor rango (Arcila B, 2019, p. 35)

El modelo de Biba es similar al de Bell-Lapadula, pero este no puede leer hacia abajo ni escribir hacia arriba y además se diferencian en que este se concentra en la integridad de los datos. El modelo se basa en que la preservación de la integridad de los datos tiene tres objetivos:

- ❖ Prevenir la modificación de datos por entes no autorizados
- ❖ Prevenir la modificación de datos no autorizados por entes autorizados
- ❖ Mantener la consistencia interna y externa.

Para el **paso II**, se realizó indagación al Departamento de TIC, la Universidad Santo Tomás Seccional Tunja identificando que tienen establecidas las políticas de tratamiento de información personal aplicada a aquellas bases de datos de las que hace uso la Universidad.

La página Web de la Universidad en un periodo de tiempo de ocho años, fue atacada en dos oportunidades, eventos en los que fue restringiendo el acceso a información generando amenaza constante por la manipulación, pérdida y acceso a la información en custodia (datos personales de toda la comunidad universitaria). Desde la dependencia se realizó la recuperación y retoma del control del sitio web.

En cuanto a seguridad y privacidad de la información, la Universidad no tiene formuladas políticas, acuerdos o lineamientos que permitan prevenir la pérdida de información por diferentes causas, siendo esta una vulnerabilidad pues no se cuenta

con procedimientos establecidos en caso de presentarse alguna anomalía, amenaza, modificación de datos o ataque a la información institucional.

Ahora bien, si se realizan una serie de actividades individuales que buscan proteger la información en custodia como lo son; BackUp periódicos a los equipos de cómputo por medio del software Cobian, esta acción fue programada para ejecutarse en periodos de tiempo definidos como no concurrentes con el fin de captar la mayor cantidad de información y no generar duplicidad de datos, datos incompletos, no veraces, no consistentes y buscando controlar manipulaciones indebidas.

También, cuenta con control de acceso a los equipos, limitaciones en la realización de cambios, modificaciones en el sistema operativo, instalación de aplicaciones y control de acceso por medio de Firewall o cortafuegos permitiendo tener el control de posible fuga de información o ataques cibernéticos. Adicionalmente y entendiendo que la mayoría de agresiones realizadas a las organizaciones son por medios equipos tecnológicos y como puente se usa el correo electrónico, el Departamento TIC de la Universidad estableció controles para ingreso y salida de correos masivos, uno a uno asignando, permisos por rol y evitando la recepción de correos que contengan información fraudulenta y aplicaciones maliciosas.

Para el **paso III**, se tuvieron en cuenta las particularidades de cada uno de los modelos, las fases que se llevaron a cabo para la implementación, las similitudes y diferencias entre ellas y los plus o aspectos relevantes que muestran cada una, como lo muestra la tabla 1.

TABLA 1: Comparativo de Modelos

MODELO	FASES	SIMILITUDES	DIFERENCIAS	PLUS
Modelo de Seguridad y Privacidad de la Información MSPI	Fase I: Diagnóstico Fase II: Planificación Fase III: Implementación Fase IV: Evaluación de Desempeño Fase V: Mejora Continua	El Modelo de Seguridad y Privacidad de la Información fue establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, tanto el modelo implementado por la UPTC como el Plan de Seguridad y Privacidad de la ESAP tiene en su desarrollo fases, destacando la realización de un diagnóstico con el fin de conocer los requerimientos de la organización, el contexto en el cual está ubicada, las necesidades, el análisis de los resultados por medio de la evaluación.	Si bien, las semejanzas de los modelos son altas, cada uno tiene sus particularidades, unos evalúan el desempeño del modelo, otros generan informes de resultados, otros mantienen el control de acceso a la información dependiendo el rol dentro de la organización, y otro se enfoca en la prevención de modificaciones a la información generando diferencias claras. Ahora bien, los dos primeros modelos descritos se desarrollan por fases definiendo cada uno de los	Entendiendo que el modelo se genera en ciclo se puede evaluar el desempeño, reconocer errores y realizar un proceso de mejora continua.
Plan de Seguridad y Privacidad de la Información	Fase I: Contexto Fase II: Situación Actual Fase III: Definición de variables para el análisis Fase IV: Análisis de la información Fase V: Informe de resultados			Este Plan se basa en el análisis de la información recolectada en la fase de contexto y situación particular generando informe de resultados.

Modelo de BIBA	Esta modelo se basa en objetivos: 1. Prevenir la modificación de datos por entes no autorizados 2. Prevenir la modificación de datos no autorizados por entes autorizados 3. Mantener la consistencia interna y externa.	En comparación de los otros modelos encontrados con semejantes en los objetivos de cada uno, todos buscan prevenir, mantener y controlar el acceso a la información generando un nivel de privacidad y seguridad alto.	pasos a seguir a medida del cumplimiento de cada una, el modelo BIBA se base la ejecución de los objetivos planteados para la prevención y el modelo Bell LaPadula genera reglas en el control de acceso multiniveles y el cumplimiento de propiedades de seguridad.	Prevención de la integridad de los datos, generando seguridad y privacidad en el cumplimiento de los objetivos planteados en este modelo.
Modelo Bell-LaPadula	Este modelo se basa en el cumplimiento reglas y propiedades: **Reglas** Control de acceso mandatorio (MAC) Control de acceso discrecional (DAC) **Propiedades** · La propiedad de seguridad simple · La propiedad estrella · La propiedad de seguridad discrecional			Se basa en la confidencialidad de la información con base en el cumplimiento de reglas y propiedades de seguridad de información definiendo cada uno de los acceso y controles por roles en la organización.

Fuente: Elaborado por los autores

Para el **paso IV**, se propuso el siguiente modelo, como lo muestra la figura 4:

MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA IES

Figura 4: *Modelo de seguridad de Información para IES*

Fuente: Elaborado por los autores

Etapa 1: Diagnóstico

En este punto se identifica el estado actual de la Organización en cuanto a la Gestión de Seguridad de la Información, así mismo cumplimiento de legislación vigente relacionada con protección de datos personales y prácticas de ciberseguridad.

Etapa 2: Planificación

En este punto, de acuerdo con el diagnóstico anterior, se elabora un plan de seguridad de la información teniendo en cuenta la misión y los objetivos de la organización, con la finalidad de definir las acciones a implementar y generarla por medio de una metodología de gestión del riesgo, ajustando las políticas, procesos y procedimientos ya definidos en modelo de seguridad, con el fin de incorporar la nueva metodología de Seguridad de la información.

Etapa 3: Alcance, límites y política de SGSI

En este punto, la definición del alcance permite delimitar el proceso de gestión de riesgos y, por ende, pone foco a todo el proceso de implementación del SGSI, el alcance se establece en función del negocio, y debe ser adecuadamente definido para evitar ambigüedades, teniendo presente que su definición no conlleve a un proyecto inalcanzable en términos de tiempo y recursos.

En cuanto a la política de seguridad, esta refleja lo que la organización quiere hacer con respecto a la seguridad de la información, los objetivos que pretende conseguir, contemplando los requisitos legales y reglamentarios aplicables y teniendo en cuenta el compromiso de la Dirección para conseguirlos.

Etapa 4: Aprobación de la dirección

El SGSI, es un proyecto organizacional, es por esto que la dirección demuestra su apoyo, aprobando las políticas y objetivos del SGSI dentro del alcance, siendo estos compatibles con los objetivos estratégicos de la organización, y estableciendo las prioridades para desarrollarlo.

Etapa 5: Valoración y tratamiento de riesgos

Para realizar la evaluación de riesgos se deben establecer los parámetros de referencia (parámetros de probabilidad, parámetros de impacto, vulnerabilidad y criterios de aceptación del riesgo) para evaluar dichos riesgos, los cuales deben ser sencillos para utilizarlos a lo largo de la implementación del SGSI.

Así mismo se debe identificar los escenarios de riesgo (determinar qué podría suceder que cause una pérdida potencial), estimación del riesgo (se pueden llevar a cabo análisis cualitativo, semicuantitativo o cuantitativo, o bien, una combinación de los tres) y evaluación del riesgo (realizar una comparación de las vulnerabilidades resultantes de cada riesgo y confrontarlas contra el nivel de aceptación de riesgo).

Para el tratamiento de los riesgos, se realiza a través de controles propuestos, para lograr llevar el riesgo a un nivel aceptable, el cual requiere un análisis de costo-beneficio de los controles a implementar y el presupuesto asignado para la elaboración, priorizando los riesgos más críticos.

Etapa 6: Diseñar SGSI

El diseño del SGSI contempla tres componentes:

1. Documentación del sistema:
2. Implementación de controles previstos en el plan de tratamiento de riesgos.
3. Monitoreo constante de seguridad de la información.

Etapa 7: Mejora continua

En esta etapa se preparan los correctivos necesarios, es importante que la entidad

defina y ejecute el plan de mejora continua con base en los resultados de evaluación del desempeño, a través del seguimiento y monitoreo que arrojan los indicadores de seguridad de la información, para verificar la efectividad, la eficiencia y la eficacia de las acciones implementadas.

CONCLUSIONES

Dado que la información se ha convertido en un recurso estratégico, el cual debe ser utilizado de forma segura, generando transacciones de calidad, donde existan controles de acceso a la información, se hace necesario la implementación de un Modelo de Gestión de Seguridad de la Información, que ayuda a las organizaciones en el tratamiento responsable de datos, salvaguarda de la información, buenas prácticas, obtención de evidencias en el proceso auditor y generación de acciones preventivas y correctivas.

Estos modelos son instrumentos fundamentales en las organizaciones, ya que ayudan a identificar riesgos y proponen controles para ayudar a minimizar los riesgos, y permiten confidencialidad e integridad de los datos y de la información.
Es así como de acuerdo al gran volumen de datos manejados por las Instituciones de Educación Superior, esta información requiere la generación de controles de acceso definidos por roles y privilegios de usuario en el acceso a la información evitando amenazas, garantizando el normal funcionamiento de los sistemas y propiciando la efectividad en el desarrollo de las funciones.

El modelo planteado en el presente artículo, permitirá suplir las debilidades de seguridad y privacidad de la información dentro de las IES pero puede ser adaptado para uso de otras entidades tanto privadas como públicas. La aplicación de estos modelos se hace necesaria en las organizaciones ya que de esta manera se asegura la integridad, confidencialidad, disponibilidad y veracidad de la información, disminuyendo así la vulnerabilidad a ataques, proporcionando una ruta a seguir en casos determinados, generando planes de acción y de mejoramiento y ejecutando controles por medio de auditorías.

REFERENCIAS

Arcila B, L. E. (2019). Recomendaciones de seguridad para los servicios de

computación en la nube, a partir de los estándares y modelos de seguridad de la información. Universidad Católica De Colombia.

Barzaga Sablón, O. S., Vélez Pincay, H. J. J., Nevárez Barberán, J. V. H., & Arroyo Cobeña, M. V. (2019). Gestión de la información y toma de decisiones en organizaciones educativas. *Revista de Ciencias Sociales*, *25*(2), 120–130. https://doi.org/10.31876/rcs.v25i2.27341

ESAP Oficina de Sistemas e Informática - OSI Seguridad. (2018). Plan de seguridad y privacidad de la Información (p. 55).

Frayssinet Delgado, M. (2017). Taller de Implementación de la norma ISO 27001. *Oficina Nacional de Gobierno Electrónico e Informática*, 97. www.ongei.gob.pe

Instituto Colombiano de Normas Técnicas y Certificación. (2013). NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001 Requisitos Ntc-Iso/Iec 27001. *Icontec*, *571*, 37.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de La Información - Guía de Mejora Continua. 58. https://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf

Montilla Malaver, L., & 10184589. (2020). Estado actual de la seguridad informática en las instituciones de educación superior en Colombia IES. In *repository.unad.edu.co*. https://repository.unad.edu.co/handle/10596/34638

OSORIO Sanabria, M. A., GUERRERO Alarcón, C. A., & GONZÁLEZ-ZABALA, M. P. (2017). La gobernabilidad de datos como apoyo en la gestión de datos de instituciones de educación superior Data governance as support in the data management of institutions of higher education. *Espacios*, *38*(51), 11. https://www.researchgate.net/publication/324088708

Paola Andrea Vargas Rubio. (2020). *Colombia ocupa el puesto 39 en el ranking mundial sobre ciberseguridad*. https://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083

Ralph M. Stair; George W. Reynolds. (2016). Principios de Sistemas de Información. Angewandte Chemie International Edition, 6(11), 951–952.

Secaira, J., Ocampo, R., Zhuma, E., & Díaz, I. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). *Revista Científico - Educacional de La Provincia de Granma*, *16*, 14. https://revistas.udg.co.cu/index.php/roca/article/view/1562/2769

Solarte Solarte, F. N. J., Enriquez Rosero, E. R., & Benavides Ruano, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5), 497–498. http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Torres Lebrato, L. (2015). La gestión de información y la gestión del conocimiento. Arch. Méd. Camaguey, 19(2), 96–98.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibèrica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://doi.org/10.17013/risti.22.73-88

Vite Cevallos, H., Molina Montero, B., & Dávila Cuesta, J. (2018). Gestión de la Información en las Instituciones de Educación Superior (IES) con base a la norma ISO 27001. *Informática y Sistemas: Revista de Tecnologías de La Informática y Las Comunicaciones*, *2*(2), 28. https://doi.org/10.33936/isrtic.v2i2.1434

UPTC. (2016). Modelo de Seguridad y Privacidad de La Información - Guía de Mejora Continua. Diario Oficial, 58.