PANORAMA ACTUAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN ESTABLECIMIENTOS EDUCATIVOS OFICIALES DE EDUCACIÓN BÁSICA Y MEDIA EN COLOMBIA

JIMMY ORLANDO SALCEDO MÉNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CEAD IBAGUÉ

2022

PANORAMA ACTUAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN ESTABLECIMIENTOS EDUCATIVOS OFICIALES DE EDUCACIÓN BÁSICA Y MEDIA EN COLOMBIA

JIMMY ORLANDO SALCEDO MÉNDEZ

Proyecto de Grado – Monografía presentado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMATICA

Christian Reynaldo Ángulo Rivera

Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍAS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CEAD IBAGUÉ

2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ibagué, Fecha sustentación

DEDICATORIA

Este trabajo lo dedico a Dios primeramente por darme la vida y la oportunidad de alcanzar mis metas, igualmente se lo dedico a mis padres e hijos por el apoyo emocional que siempre me han brindado y finalmente a mi esposa quien con su carisma y comprensión me acompañó en cada etapa vivida, me apoyó y motivó para que mi formación académica llegará a feliz término.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

LISTA DE CUADROS

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

RESUMEN

En la actualidad los servicios informáticos brindan grandes ventajas en el manejo y conservación de la información, pero también se tienen desventajas como son los accesos indebidos a la información, produciendo riesgos para las instituciones propietarias de la misma. El robo es un acto ilegal, las personas para prevenir los robos cierran las puertas y las ventanas de los hogares; pero también se debe bloquear los sistemas de información. Al igual que las personas que cierran sus puertas, las Instituciones Educativas en Colombia siempre se han preocupado por proteger sus valiosos recursos físicos y de infraestructura, pero en su gran mayoría descuida la seguridad de la información confidencial contenida en los registros de los estudiantes y del personal que labora en la misma.

Mediante la presente monografía se logrará describir el panorama actual sobre la seguridad de la información en establecimientos educativos oficiales de educación básica secundaria y media de Colombia, lo cual permitirá elaborar las recomendaciones necesarias para reducir los riesgos y vulnerabilidades de la información sensible que manejan estos establecimientos.

Este análisis está basado en informes de estudios realizados en algunos países y datos recolectados sobre la seguridad de la información en establecimientos educativos de Colombia, estableciendo la importancia de la protección de la información teniendo en cuenta lo vulnerable que esta puede ser y lo necesario de salvaguardar dicha información.

PALABRAS CLAVES: Ciberseguridad, vulnerabilidad, Instituciones Educativas, seguridad, Seguridad Informática, Amenazas informáticas, Ciberespacio, Ciberseguridad.

ABSTRACT

At present, computer services offer great advantages in the management and conservation of information, but it also has disadvantages such as improper access to information, producing risks for the institutions that own it. Theft is an illegal act, people to prevent theft close the doors and windows of homes; but information systems must also be blocked. Like the people who close their doors, Educational Institutions in Colombia have always been concerned with protecting their valuable physical and infrastructure resources, but the vast majority neglect the security of confidential information contained in student records and staff working in it.

By means of this monograph, it will be possible to describe the current panorama on information security in official educational establishments of basic secondary and secondary education in Colombia, which will make it possible to prepare the necessary recommendations to reduce the risks and vulnerabilities of the sensitive information that these establishments handle.

This analysis is based on reports of studies carried out in some countries and data collected on the security of information in educational establishments in Colombia, establishing the importance of the protection of information taking into account how vulnerable it can be and what is necessary to safeguard such information.

KEY WORDS: Cybersecurity, vulnerability, Educational Institutions, security, Computer Security, Computer threats, Cyberspace, Cybersecurity.

INTRODUCCIÓN

En la actualidad se observa como las empresas en general y las Instituciones educativas, vienen implementando las nuevas tecnologías para el manejo de la información permitiendo un uso de estrategias colaborativas, interactivas y conectadas globalmente, pero de esta forma también, se abren puertas a amenazas digitales. Antes del uso generalizado de los sistemas informáticos, los rectores de las Instituciones educativas eran responsables de proteger los registros en papel que a menudo se guardaban en archivadores. Los gabinetes probablemente estaban cerrados con llave en la oficina del rector o de las secretarias, y ellos tenían la única llave.

En los últimos años, sin embargo, la mayoría de las Instituciones educativas se han unido a otras entidades del sector público y privado para adoptar la tecnología como el medio principal por el cual organizan y acceden a la información. Compartir información a través de computadoras y redes informáticas ha demostrado una y otra vez que es una forma rentable de hacer las cosas. De hecho, la sociedad actual depende de las computadoras ahora más que nunca y lo más probable es que continúe aumentando el uso de la tecnología. Como dice el refrán, la información es poder.

En las Instituciones educativas, es el poder de hacer más eficiente todo el proceso educativo. La información sobre los estudiantes, el personal, los grupos, los programas, las instalaciones y las actividades fiscales se recopila y mantiene para que las escuelas puedan coordinar de manera efectiva los servicios ofrecidos a los estudiantes, medir el progreso del aprendizaje, asignar y monitorear las responsabilidades del personal y el uso de los recursos, y proporcionar otros servicios valiosos a sus comunidades.

Pero a pesar de lo nueva que es la tecnología para el lugar de trabajo, su aplicación es una extensión de la forma en que las Instituciones educativas siempre han llevado a cabo sus actividades. Si bien los equipos informáticos y las redes contribuyen a la eficiencia del mantenimiento de los registros educativos, el acceso y el uso de datos, no han

cambiado las razones por las que las Instituciones educativas necesitan mantener, compartir y usar la información de los estudiantes y el personal. La comunidad educativa siempre ha requerido este tipo de información para llevar a cabo su misión de instruir a los estudiantes.

Aunque puede ser apropiado discutir analogías entre archivos en papel en gabinetes de madera y archivos electrónicos en discos duros, existen diferencias significativas en los procesos específicos requeridos para mantener la seguridad adecuada en la era de las redes informáticas. Con solo pulsar un interruptor, la información puede dañarse de forma irreparable. Con un giro descuidado de su cabeza, un disco de bolsillo que contiene miles de registros puede desaparecer. Y con la conexión de un solo cable, el material sensible se puede compartir con millones de usuarios.

La misma tecnología que puede ser fuente de tanta preocupación cuando está en manos de usuarios no capacitados, puede usarse para proteger la información de forma segura, garantizando la seguridad de la información.

Hoy en día se cuenta con diferentes modelos de seguridad informática, que pueden ser usados en los diferentes equipos de almacenamiento de la información y en las redes de datos. Si se utiliza un estándar se garantiza un esquema adecuado a las necesidades de una empresa u organización y de esta forma implementar políticas de seguridad que beneficiarán a la institución el resguardo y seguridad de la información. Algunos de estos estándar son: OSSTMM3, ISO 27001, NIST, COBIT 5, entre otros.

El último informe anual del Foro Económico Mundial[1] indica que los ciberataques para robo de información en el 2021 aumentaron 150% en todo el mundo. Es así como la información almacenada en una Institución Educativa se ha vuelto muy apetecida por los ciberdelincuentes; una de las cosas que más les llama la atención es el robo de datos sensibles del personal administrativo, docentes y estudiantes, como también pueden acceder a información financiera, información de convocatorias o datos de proveedores

[1] WORLD ECONOMIC FORUM. Global Cybersecurity Outlook 2022. [Consultado 27 diciembre de 2021]. Disponible en: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

y de esta forma acceder a beneficios económicos; o se puede hacer plagio de proyectos, y no menos importante la modificación de calificaciones o la eliminación de información en las bases de datos de la Institución educativa, con el propósito de obtener beneficios personales propios o de terceros.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La información almacenada en las Instituciones Educativas, se ha vuelto muy apetecida por los ciberdelincuentes, con el propósito de obtener beneficios propios o de terceros; la poca conciencia que asumen las instituciones educativas y los bajos recursos económicos y tecnológicos de las mismas, vienen aumentando el riesgo en muchas formas, del acceso no autorizado de la información, o la manipulación y modificación de la misma.

Desde el año 2020, a causa de la pandemia del covid 19 y el aislamiento obligatorio, las instituciones del estado, colegios y empresas privadas, se vieron obligadas a implementar el teletrabajo y la atención al público de forma virtual, incrementando enormemente los trámites y transacciones virtuales. Las Instituciones Educativas oficiales del país se vieron obligados a implementar plataformas virtuales para realizar sus matrículas, certificados, registros, evaluaciones, clases, etc. Igualmente se incrementaron las ventas virtuales y más en los días sin IVA, los “BlackFraday o los “Cyberlunes”. Esto ha incrementado igualmente los ataques cibernéticos en el país y en general en el mundo.

Según estudios realizados por distintas entidades del orden nacional o internacional como el documento publicado por el Foro Nacional de Estadísticas Educativas de los Estados Unidos[2], describe qué y por qué, algunos tipos específicos de datos sobre los estudiantes y sus familias se consideran confidenciales o por ejemplo el artículo publicado por Aguirre[3] periodista del programa radial LA FM donde indica que el 67% de los colegios en Latinoamérica han sido víctimas de ataques cibernéticos, y que el 44% de las empresas encuestadas no le prestan atención a la seguridad de la información;

[2] The National Forum on Education Statistics (NFES). Protecting the Privacy of Student Education Records. U.S. Department of Education. 1997. p. 41-54.
[3] AGUIRRE, Jhon. El 67% de los colegios en Latinoamérica han sido víctimas de ataques cibernéticos. *La FM*. [En línea] 28 Mayo 2018. [Consultado 27 diciembre de 2021]. Disponible en: https://www.lafm.com.co/tecnologia/el-67-de-los-colegios-en-latinoamerica-han-sido-victimas-de-ataques-ciberneticos

igualmente se puede encontrar la publicación titulada “Colombia fue uno de los países con más ataques cibernéticos el año pasado” del diario La República[4] donde indica que Colombia fue uno de los países con más ataques cibernéticos en el año 2018 y además que dos de cada tres encuestados has sufrido ataques cibernéticos.

De acuerdo al estudio Tendencias del Cibercrimen 2019-2020[5], emitida por la Policía Nacional - Centro Cibernético, en asocio con el Tanque de Análisis y Creatividad de las TIC - TicTac de la CCIT dan a conocer las cifras y modalidades de los ciberdelitos en 2019 y las tendencias que enfrentarían las empresas Colombianas y los ciudadanos en 2020, sin embargo posteriormente se siguen haciendo estos estudios como último entregado por las mismas entidades investigadoras con el Informe SAFE - Tendencias del Cibercrimen 2021 – 2022. En este informe se indica que “al analizar el comportamiento del cibercrimen en Colombia reflejado en el número de denuncias instauradas ante el ecosistema de la Fiscalía General de la Nación, las policías judiciales del CTI y la Policía Nacional (DIJIN-SIJIN) a través del aplicativo a denunciar, al finalizar el mes de noviembre del 2021 se habían registrado 46.527 denuncias por distintos delitos lo que equivale a un incremento del 21% respecto al 2020. Si se tienen en cuenta comparativamente los años 2019 y 2021, es decir sin contabilizar el año de pandemia, el incremento alcanzó un 107% acumulado entre el suscitado durante el 2020 y el aumento continuo durante el 2021”[6]. Es así como todos los estudios hechos, muestran que los ciberdelitos en Colombia en los últimos tres años vienen en un crecimiento enorme en comparación con los años anteriores y esto debido a la pandemia, el crecimiento del comercio electrónico en general.

[4] La Reprublica. Colombia fue uno de los países con más ataques cibernéticos el año pasado. [En línea]. [Consultado 27 diciembre de 2019]. Disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

[5] Policia Nacional, CCIT. Informe de las Tendencias del cibercrimen en Colombia (2019-2020). [En línea]. [Consultado 15 diciembre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[6] CCIT. Informe SAFE - Tendencias del Cibercrimen 2021 – 2022. [En línea]. [Consultado 15 diciembre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

En cuanto a la información digital, “la Violación de Datos Personales con 13.458 casos es el delito de mayor crecimiento en el país durante el 2021 con un 45% de variación porcentual respecto a los casos registrados durante el 2020”[7]. Lo anterior se debe al aumento del uso de delitos como el Phishing, logrando los ciberdelincuentes enviar enlaces que logran redireccionar hacia otros sitios web los cuales contienen formularios que son utilizados para obtener la información personal de las víctimas, tales como, nombres y apellidos, datos de nacimiento para conocer su edad, documentos de identidad, dirección de residencia y demás, información necesaria para gestionar trámites y hacer procedimientos fraudulentos correspondientes a solicitudes de préstamos de dinero, solicitud de tarjetas de crédito, fraudes en seguros o sencillamente vender estos datos en la internet profunda.

La revista portafolio en su página web presenta información sobre ciberdelincuencia en este 2021 diciendo que “Entre las ciudades con mayor afectación por los ciberdelitos se destacan Bogotá (10.643), Medellín (2.223), Cali (2.086), Barranquilla (1.264), Cartagena (745) y Bucaramanga (570)”[8].

Estos y otros estudios más han mostrado que el riesgo en la seguridad de la información en los establecimientos educativos va en aumento día a día en Colombia y en general en Latinoamérica.

Los delincuentes cibernéticos han logrado acceder de manera fraudulenta información sensible de la comunidad educativa como identidades o datos personales de administrativos, docentes y estudiantes, como también información financiera, información de convocatorias o datos de proveedores, entre mucha otra información más; información que en manos corruptas pueden causar mucho daño social o económico. Por lo que se requiere tener un panorama actual sobre la seguridad de la información en

[7] CCIT. Informe SAFE - Tendencias del Cibercrimen 2021 – 2022. [En línea]. [Consultado 15 diciembre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

[8] Portafolio. Las entidades que reportan mayor suplantaciones por cibercriminales. [En línea]. [Consultado 15 diciembre de 2021]. Disponible en: https://www.portafolio.co/innovacion/entidades-colombianas-que-reportan-mayor-suplantaciones-por-cibercriminales-559465

establecimientos educativos oficiales de educación básica y media en Colombia para redactar una serie de recomendaciones en aras de proteger y garantizar la seguridad e integralidad de la información que se manejan en dichos establecimientos educativos.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se encuentra en la actualidad la seguridad de la información en establecimientos educativos oficiales de educación básica y media en Colombia y cómo se puede llegar a prevenir los riesgos a los que se enfrentan?

2 JUSTIFICACIÓN

En Colombia de acuerdo a la Constitución Nacional[9] el Estado, la sociedad y las familias están obligadas a garantizar los derechos de los niños y jóvenes para que tengan un desarrollo integral y se les garantice su seguridad en todo sentido. Los establecimientos educativos están obligados igualmente a garantizar estos derechos de los niños y los jóvenes. Las Instituciones educativas manejan información privada de cada estudiante y de sus acudientes o padres de familia, como lo son nombres completos, direcciones de residencia o trabajo, contactos telefónicos, números de documentos, fechas de nacimiento y edad, entre muchos otros datos sensibles.

Dado que la institución es en última instancia responsable de la integridad y seguridad de sus datos, las Instituciones educativas oficiales de educación básica y media de Colombia, deben tomar medidas activas para garantizar que los equipos valiosos y, lo que es más importante, la información (como los registros privados de estudiantes y personal) estén protegidos adecuadamente. Si una Institución educativa no protege su información confidencial de una manera que satisfaga los "estándares del debido cuidado" y las "salvaguardias razonables", se abre a una serie de problemas potenciales, desde acusaciones de negligencia e incompetencia, hasta demandas judiciales por delitos cometidos por el acceso a la información en custodia y ramificaciones legales de las violaciones de la privacidad.

Por consiguiente, se requiere hacer un análisis pertinente, que ilustre el panorama actual de los establecimientos educativos en cuanto a los ataques perpetuados a estos y en general en cuanto a la seguridad de la información que manejan los establecimientos educativos y de acuerdo al análisis elaborar unas sugerencias para la prevención ante estas vulnerabilidades.

[9] Constitución Política de Colombia [Const]. Art. 42. 7 de julio de 1991 (Colombia).

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Describir el panorama actual sobre la seguridad de la información en establecimientos educativos oficiales de educación básica secundaria y media de Colombia, con el propósito de realizar las recomendaciones necesarias para reducir los riesgos y vulnerabilidades de la información sensible que manejan estos establecimientos.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar la normatividad actual del país en pro de la seguridad de la información, con el propósito de evaluar y tratar los riesgos de Seguridad Digital.
- Recopilar información mediante consultas en Internet, sobre estudios realizados a la seguridad de la información de establecimientos educativos oficiales de educación básica y media de Colombia.
- Indagar sobre el panorama actual de la seguridad de la información en los establecimientos educativos oficiales de educación básica secundaria y media de Colombia, mediante el análisis de reportes e informes de ciberataques a estos tipos de establecimientos o de otro sector educativo.
- Elaborar algunas recomendaciones de acuerdo con el panorama descrito para garantizar la seguridad de la información en los establecimientos educativos oficiales de educación básica secundaria y media de Colombia.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

La empresa DigiSOC– (*Information Security Operation Center of Digiware*)[10], recopiló información en más de 13.000 dispositivos monitoreados en el primer trimestre de 2018, revelando porcentajes correspondientes a ataques cibernéticos a distintas empresas y establecimientos educativos de América Latina y hace ubicación en orden de ataque a los países que conforman la misma.

La revista "Tierra Infinita"[11] originaria del país del Ecuador, presenta un estudio también sobre la seguridad de la información en las Instituciones Educativas, la cual presenta un artículo denominado "COMPARACIÓN DE MODELOS TRADICIONALES DE SEGURIDAD DE LA INFORMACIÓN PARA CENTROS DE EDUCACIÓN".

El programa periodístico "LA FM"[12] también presenta un estudio sobre la seguridad de la información en Colombia y otros países. Se puede analizar en este informe datos correspondientes sobre ciberseguridad dando cifras alarmantes sobre la inseguridad de las empresas consultadas y establecimientos educativos de Colombia en cuanto al manejo que le dan a la información.

Otro estudio realizado sobre la seguridad de la información en establecimientos educativos es el presentado en la Universidad de Guayaquil en el país del Ecuador, por

[10] DIGIWERE - ¿A qué amenazas cibernéticas se enfrentará el sector educativo con la transformación digital?, [En línea]. [27 diciembre de 2019] disponible en: http://www.digiware.net/?q=es/blog/a-que-amenazas-ciberneticas-se-enfrentara-el-sector-educativo-con-la-transformacion-digital

[11] LARA Elva G, CORELLA Flavio A. Comparación de modelos tradicionales de seguridad de la información para centros de educación. Revista Tierra Infinita N° 4. Jun-Ago.2018, p. 20-28.

[12] AGUIRRE, Jhon. El 67% de los colegios en Latinoamérica han sido víctimas de ataques cibernéticos. *La FM*. [En línea] 28 mayo 2018. [Consultado 27 diciembre de 2019]. Disponible en: https://www.lafm.com.co/tecnologia/el-67-de-los-colegios-en-latinoamerica-han-sido-victimas-de-ataques-ciberneticos

Parra y Yánez[13] quienes en su estudio hacen un análisis de vulnerabilidad tecnológica en un centro de educación superior, mediante herramientas de testeo y usando metodologías estándar o modelos internacionales preparados para garantizar la seguridad de la información.

Esquivel Triana[14] en el 2014 en su escrito titulado “Modelos de Seguridad”, presenta los modelos CMMI, MBOK, ITIL y COBIT, entre otros modelos y estándares, al igual PMOGuide[15], el cual es un canal de investigación mexicano se encarga de hacer análisis, estudio y opinión de la Gestión de Proyectos, así como de las diferentes metodologías, estándares y marcos de referencia existentes, entre otros temas; esta página web presenta un comparativo entre los modelos CMMI, PMBOK, ITIL y COBIT para escoger cual es el más apropiado en la gestión del riesgo.

Los estudiantes de la Universidad Uniminuto, Bermudez Sanmiguel y Tafur Torres realizaron un trabajo de grado titulado “Sistema de Seguridad Informático para el Colegio Cooperativo Espíritu Santo De Girardot”[16] donde hacen un análisis sobre la seguridad de los equipos de cómputo en el Colegio Cooperativo Espíritu Santo.

Una herramienta útil que se encuentra en internet es la página web de la empresa Kaspersky[17] en donde se hacen análisis sobre las ciberamenazas a nivel mundial, mostrando estadísticas importantes para realizar diagnósticos y conocer el panorama mundial y nacional en estos aspectos.

---

[13] PARRA BARZOLA Liliana M.; YÁNEZ CEDEÑO Erick S. Análisis de vulnerabilidades en la Infraestructura tecnológica de una empresa, utilizando herramientas de test de Intrusión. Trabajo de investigación .Guayaquil: Universidad de Guayaquil. Facultad de Matemáticas y Física, 2017. 154p.

[14] EZQUIVEL TRIANA, Ricardo. Modelos de seguridad. Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacional, Bogotá. 2014. 26p

[15] PMOGuide. Comparativa – PMBOK, CMMI, COBIT, ITIL, [Sitio web]. Mexico. [Consultado 12 noviembre de 2020]. Disponible en: https://ipmoguide.com/comparativa-pmbok-cmmi-cobit-itil/

[16] BERMUDEZ SANMIGUEL, Edgar y TAFUR TORRES, Diego. Sistema de Seguridad Informático para el Colegio Cooperativo Espíritu Santo De Girardot. Trabajo de grado realizado para optar al título de tecnólogo en redes de computadores y seguridad informática. Girardot: Corporación Universitaria Minuto de Dios. Facultad de Ingeniería de Sistemas, 2011. 33p.

[17] KASPERSKY. Ciberamenaza Mapa en Tiempo Real. [Sitio web]. Rusia. [Consultado 12 noviembre de 2020]. Disponible en: https://cybermap.kaspersky.com/es

La empresa MARSH cuenta con un blog denominado “El Riesgo en Contexto” [18] en el cual se publican análisis y estudios sobre la seguridad de la información en establecimientos educativos titulado “El sector educativo, un blanco perfecto para ciberataques”.

La Universidad del Rosario en Colombia llevó a efecto un estudio denominado “Colombia no está preparada ante un ciberataque” [19], en el que presenta de distintas formas un panorama sobre la seguridad de información en Colombia.

La Universidad Santo Tomas presenta en su página web, un informe denominado “Los Ataques Informáticos en el Sector Educativo”[20], donde se presenta un análisis sobre esta temática correspondiente a la seguridad de la información en los establecimientos educativos.

La Revista Dinero, presenta también un informe llamado “En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos”[21] donde indica que el Servicio de inteligencia de amenazas de la compañía Fortinet publicó un estudio en el último congreso ANDICOM que se lleva a cabo en Cartagena, y presenta cifras concernientes a ataques perpetuados a empresas y establecimientos educativos.

En los últimos años se han incrementado exponencialmente los ataques a los sistemas informáticos de empresas y establecimientos educativos, poniendo en riesgo la información que allí se maneja.

---

[18] FRASER, John. El sector educativo, un blanco perfecto para ciberataques. *BLOG: EL RIESGO EN CONTEXTO*. [En línea]. 2018, [consultado 15 octubre de 2020]. Disponible en: https://www.marsh.com/co/insights/risk-in-context/sector-educativo-ciberataques.html

[19] UNIVERSIDAD DEL ROSARIO. Colombia no está preparada ante un ciberataque. [En línea]. [consultado 30 diciembre de 2019] disponible en: https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante- un-ciberataque/

[20] UNIVERSIDAD SANTO TOMÁS. Los Ataques Informáticos en el Sector Educativo. [En línea]. [consultado 05 enero de 2020] disponible en: https://auditoriainterna.usta.edu.co/index.php/120-los-ataques-de-hacking-en-el-sector-educativo

[21] DINERO. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [En línea]. [Consultado 10 enero de 2020]. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

La universidad Libre de Colombia mediante el estudio denominado “Crecen los ataques de Phishing en Colombia”[22] hace detalles sobre este tipo de ataque dando a conocer cifras sobre ataques perpetuados en Colombia.

Otro estudio de este mismo tipo es el publicado por la Universidad Tecnológica de Pereira mediante un artículo denominado “Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico”[23] en la revista *Scientia et Technica*, donde hace un análisis de riesgos con base en la norma ISO 27005 y hace una identificación de los activos críticos del área de secretaría académica de las instituciones educativas nivel básico y los riesgos asociados.

En América Latina los países vienen implementando mejoras en las estrategias para garantizar la seguridad de la información, pero se ha visto muy complicado que a nivel interno los países logren engranar estas políticas de seguridad en todos los Ministerios.

De esta misma manera en la Revista Latinoamericana de Ingeniería de Software presenta un artículo denominado “Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local”[24] en el cual se hace un comparativo basado en el enfoque Top-Down desde una visión global a una visión local en Argentina y hace un análisis detallado de cómo están avanzando en Latinoamérica los países en cuestión de ciberseguridad.

A continuación, se muestra un cuadro comparativo de las Políticas de Ciberseguridad empleadas por los Estados latinoamericanos en selección.

[22] UNIVERSIDAD LIBRE. Crecen los ataques de Phishing en Colombia. [En línea]. [05 enero de 2020] disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/424-crecen-los-ataques-de-phishing-en-colombia

[23] Benavides S. Alejandra, Blandón J. Carlos. Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. Scientia et Technica Año XXII, Vol. 23, No. 01, marzo de 2018. Universidad Tecnológica de Pereira. ISSN 0122-1701

[24] Leiva, Eduardo. 2015. Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642, p169

Cuadro 1. Cuadro comparativo de las políticas de ciberseguridad en la Región

	BLOQUE GEOPOLÍTICO	OEA			
	PAÍS	COL	BRA	CHILE	ARG
PROTEGE	Infraestructuras criticas	X	X	X	X
	Economía		X		
	Seguridad Nacional		X		
	Bienestar Social	X	X		
ENFOQUE	Concientización	X	X	X	
	Conocimiento		X		
	Educación	X	X	X	
	Capacidades cibernéticas militares	X			
SECTOR PUBLICO	Liderazgo/coordinación	X	X	X	X
	Marco jurídico	X			X
SECTOR PRIVADO	Participación en la estrategia	X	X	X	
COOPERACIÓN INTERNACIONAL	Cooperación en su grupo	X	X	X	X
	Cooperación con otros países	X	X	X	X

Fuente: Leiva, Eduardo. 2015. Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642, p169

De acuerdo al cuadro comparativo Colombia y Brasil son los países que más están implementando políticas de ciberseguridad. Es así como en américa Latina los gobernantes aprobaron una declaración sobre el “Fortalecimiento de la Ciberseguridad en las Américas” en marzo de 2012.

4.2 MARCO CONCEPTUAL

En el mundo de la seguridad de la información se pueden encontrar herramientas que ayudan a garantizar la protección de la información, una de estas herramientas es el OSSTMM[25] (manual de metodología de pruebas de seguridad de código abierto), es una metodología completa para la prueba, el análisis y la medición de la seguridad operativa para construir buenas defensas de seguridad, esta metodología ayuda y facilita a encontrar cuan segura es una red y lo que tiene que ver en cuanto a la seguridad en varios aspectos de la protección de la información, también el OSSTMM cuenta con el propósito de examinar la organización, mediante pruebas de seguridad que se realizan desde adentro de la organización hacia afuera.

De acuerdo con Valdez Alvarado[26], este manual contempla el cumplimiento de estándares y buenas prácticas como las establecidas en el NIST, ISO 27001-27002 e ITIL, entre otras, es uno de los estándares profesionales más completos y comúnmente utilizados a la hora de revisar la seguridad de los sistemas desde Internet, lo que permite que sea ideal para la aplicación de pruebas a la seguridad de la información en las instituciones educativas.

Existe una guía de gestión de riesgos para sistemas de tecnología de la información, cuyas recomendaciones las hace el Instituto Nacional de Estándares y Tecnología, llamada NIST SP 800-30[27] la cual orienta sobre la protección de la información y se puede aplicar en la seguridad de la información que se maneja en las Instituciones Educativas, esta metodología se aplica en forma de guía y es desarrollada por el departamento de comercio del gobierno de los Estados Unidos. Uno de los propósitos de esta metodología es el dar recomendaciones básicas de seguridad cibernética para empresas mediante

[25] HERZOG Pete. OSSTMM 3. The Open Source Security Testing Methodology [Manual]. Isecom.org. USA. 2010. 211p

[26] VALDEZ ALVARADO, Aldo. OSSTMM 3. *Revista de Información, Tecnología y Sociedad*. [En línea]. 2013, junio No 8. [consultado 15 octubre de 2020] ISSN 1997-4044. Disponible en: http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100013&script=sci_arttext

[27] STONEBURNER, Gary, GOGUEN Alice y FERINGA Alexis. Risk management guide for information technology systems: recommendations of the National Institute of Standards and Technology. [Manual]. *National Institute of Standards and Technology*. USA. 2012. 65p.

procesos de evaluación de riesgos. El NIST SP 800-30, se encuentra conformado por 5 secciones que se llevan a efecto o ejecutan de forma secuencial: **iniciación**, se expresa la necesidad de un sistema de gestión de seguridad de la información y se documenta el propósito y alcance del mismo; seguidamente se tiene el **desarrollo o adquisición**, en el cual el sistema de gestión de seguridad de la información está diseñado, comprado, programado, desarrollado o construido; continua con la **implementación**, aquí Las funciones de seguridad del sistema deben configurarse, habilitarse, probarse y verificarse; luego viene la **operación o mantenimiento,** en esta sección el sistema informático se modifica de forma continua mediante la adición de hardware o software y mediante cambios en los procesos, políticas y procedimientos de la organización; finalmente se tiene la sección **disposición**, en esta fase, se puede involucrar la disposición de la información, las actividades pueden incluir mover, archivar, descartar o destruir información y desinfectar tanto la parte física como la lógica.

De acuerdo con el artículo publicado en la revista "*Journal of Information Systems*"[28], COBIT, actualmente en su quinta edición, es un marco de buenas prácticas para el gobierno empresarial de TI. Existe una investigación académica limitada que analiza este modelo para auditar la gestión y el control de los sistemas de información y tecnología, explora el uso de COBIT y posiciona a COBIT como un marco para el gobierno empresarial de TI. Igualmente describen las principales direcciones y principios básicos del marco de gestión y hacen conexiones de estas instrucciones y principios con la literatura relevante. Por lo anterior es que la implementación del modelo COBIT es una buena forma de proteger la información digital y física de las Instituciones educativas, es importante porque ayuda a las empresas a alcanzar niveles aceptables de riesgos y uso de recursos.

[28] DE HAES Steven, VAN GREMBERGEN Wim y DEBRECENY Roger S. COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. En: Journal of Information Systems Vol. 27 No 1. (Mar-May.2013); p. 307-324. DOI: 10.2308/isys-50422.

La empresa Advisera presenta de forma gratuita un informe técnico desarrollado por 27001Academy denominado "*How to integrate ISO 27001, COBIT and NIST*"[29], este documento técnico explica cómo integrar los enfoques ISO 27001, COBIT y NIST para mejorar la seguridad de la información. En el mismo se presenta de forma detallada el concepto de COBIT, qué es el marco de seguridad cibernética del NIST, qué es ISO 27001, similitudes y diferencias entre COBIT, NIST CSF e ISO 27001, cómo integrar ISO 27001, COBIT y el marco de seguridad cibernética de NIST.

De acuerdo con la información que suministra la empresa ISOtools la norma "ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan" [30]. Según la misma empresa el estándar permite a las organizaciones evaluar el riesgo y aplicar controles necesarios para reducirlos o eliminarlos. El SGSI se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

El estándar ISO 27001 implementa una metodología que permite determinar los requisitos necesarios para crear los sistemas de gestión de la seguridad de la información (SGSI). Esta norma permite medir la efectividad del programa de seguridad de la información, las políticas, los controles y planes para el tratamiento del riesgo; la revista Tecnológica Espol – RTE publicó un artículo donde los autores tienen como objetivo:

> Desarrollar habilidades en los ingenieros de sistemas, que les permitan conducir proyectos de diagnóstico, para la implementación e implantación de sistemas de seguridad de la información – SGSI alineado con el estándar ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002. Se presentan los resultados de una experiencia aplicando las fases de auditoría y la metodología de análisis y evaluación de riesgos con el diseño y aplicación de diversos instrumentos como cuestionarios aplicados a los administradores, clave de seguridad, entrevistas al personal del área informática y usuarios de los sistemas, pruebas de intrusión y testeo que permitieron establecer el diagnóstico de seguridad actual. Posteriormente se aplica una lista de chequeo basada en la norma, para verificar la existencia de controles de seguridad en los procesos organizacionales. Finalmente, y de acuerdo a los resultados del análisis y evaluación de los riesgos, se proponen los

[29] 27001ACADEMY - How to integrate ISO 27001, COBIT and NIST, [En línea]. [Consultado 27 noviembre de 2019]. Disponible en: https://info.advisera.com/27001academy/free-download/how-to-integrate-iso-27001-cobit-and-nist

[30] ISOtools. Sistemas de Gestión de Riesgos y Seguridad. [En línea]. [Consultado 27 noviembre de 2019]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/#

controles de seguridad para que sean integrados hacia el futuro dentro de un SGSI que responda a las necesidades de seguridad informática y de la información acorde a sus necesidades[31].

En el mundo entero se han venido diseñando y adaptando estándares y guías especializadas en ciberseguridad en pro de mejorar la integralidad y privacidad de la información, pudiendo ser estas aplicadas a diferentes ámbitos en general, como en el sector empresarial, el comercial, el educativo entre otras. Sin embargo, a pesar de ya contar con estas herramientas, la gran mayoría de empresas ven su implementación como un gasto adicional y prefieren no invertir en ello sin tener en cuenta las dificultades que se puedan dar por no tener una ciberseguridad apropiada.

[31] SOLARTE SOLARTE, Francisco, ENRIQUEZ ROSERO, Edgar y BENAVIDES RUANO, Mirian. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnologica Espol – RTE*. 2015, vol. 28, nro. 5, p. 492-507.

5 DESARROLLO DE LOS OBJETIVOS

5.1 NORMATIVIDAD ACTUAL DEL PAÍS EN PRO DE LA SEGURIDAD DE LA INFORMACIÓN

En el esquema más amplio, la información educativa a menudo se considera confidencial por su propia naturaleza, es decir, ciertos tipos de información sensible (en particular, registros de estudiantes y del personal identificables individualmente) deben, por ley, estar protegidos.

Los establecimientos educativos hoy en día hacen almacenamiento en la nube (Internet) de alguna o gran parte de la información que manejan, lo que requiere que se lleven a efecto buenas prácticas que garanticen prevenir incidentes de seguridad que afecten la seguridad de la información, es por ello que el Gobierno de Colombia realizó un documento que orienta a las entidades del Estado mediante lineamientos y aspectos a tener en cuenta para el aseguramiento de la información en la nube presentados mediante el documento en línea denominado “Seguridad en la nube”[32].

5.1.1. Plan de Seguridad y Privacidad de la Información del MINTIC 2020. El Ministerio de las TIC elaboró una serie de guías y metodologías para garantizar la seguridad de la información, una de ellas es el Plan de Seguridad y Privacidad de la Información, cuyo objetivo es “Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos del Ministerio de Tecnologías de la Información y las Comunicaciones– MINTIC ”.

[32] Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. Seguridad en la Nube, Guía 12, [En línea]. [27 diciembre de 2019] disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

Este plan de seguridad y privacidad de la información permite que las Instituciones educativas del sector público puedan conocer y considere formalizar los elementos normativos sobre los temas de protección de la información. Igualmente le permitirá a las Instituciones educativas gestionar los riesgos de seguridad y privacidad de la información que se manejan en estos establecimientos y se puedan establecer mecanismos de aseguramiento físico y digital, con el propósito de fortalecer la confidencialidad e integralidad de la información.

5.1.2. Modelo de Seguridad y Privacidad de la Información MSPI. La política de alto nivel o política general del Estado Colombiano, manifiesta la necesidad de la implementación de un SGSI denominado Política General MSPI v4, documento maestro dirigido a las Entidades del Estado con fecha 22 de febrero de 2021 en su versión 4, cuyo objetivo principal es "Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado"[33].

Las Instituciones Educativas de Educación básica secundaria y Media del sector público hace parte de las Entidades del Estado, por consiguiente, es pertinente tener en cuenta estos lineamientos de buenas prácticas en Seguridad y Privacidad de la información que se manejan en estos establecimientos, teniendo en cuenta que esta información es muy sensible ya que es información de menores de edad y sus acudientes.

5.1.3. Controles de Seguridad y Privacidad de la Información. El Ministerio de las TIC también contempla el cómo proteger la información de las entidades del Estado, lo que incluye los establecimientos educativos públicos, también los mecanismos utilizados para el procesamiento de la información, el cual se debe proteger de posibles amenazas internas o externas, como también amenazas deliberadas o accidentales, todo esto

[33] Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, [En línea]. [Consultada 10 diciembre de 2021] disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

debido a que se debe garantizar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información, todo contemplado en la guía 8 denominada “Controles de Seguridad y Privacidad de la Información”[34].

Estos controles aportan gran información a las Instituciones Educativas de carácter público de educación básica secundaria y media, en cuanto como prever amenazas externas e internas de tipo accidental o deliberada que permitan el acceso a la información de forma no autorizada y la misma sea usada para fines delictivos. Igualmente, guía a las Instituciones Educativas a conocer gran variedad de información y conceptos claves que permitan asegurar la información que se maneja.

5.1.4. Guía de indicadores de gestión para la seguridad de la información. Los indicadores de gestión se crean con el propósito de orientar principalmente la medición de efectividad, eficiencia y eficacia de los procedimientos y componentes del SGSI, estos indicadores ayudaran enormemente en el componente de mejora continua correspondientes a la seguridad de la información, estos indicadores se encuentran escritos en la guía 9 del Ministerio de las TIC denominado “Guía de indicadores de gestión para la seguridad de la información”[35].

Las Instituciones de educación básica secundaria y media deben implementar la elaboración de indicadores de gestión para la seguridad de toda la información que se administra sobre los estudiantes, padres, docentes, directivos y administrativos, con el propósito de conocer si se va por buen camino o se debe realizar modificaciones pertinentes para mejorar los componentes del Sistema de Gestión de la Seguridad de la Información SGSI.

[34] Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. Controles de Seguridad y Privacidad de la Información. Guía 8, [En línea]. [27 diciembre de 2019] disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf
[35] Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. Guía de indicadores de gestión para la seguridad de la información. Guía 9, [En línea]. [27 diciembre de 2019] disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

5.1.5 CONPES Consejo Nacional de Política Económica y Social. En Colombia el Consejo Nacional de Política Económica y Social, junto con el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación, diseñaron en el año 2016 el documento denominado CONPES 3854 Política Nacional de Seguridad Digital[36], donde plasman las políticas de la gestión del riesgos de seguridad digital, que buscan promover un entorno digital confiable y seguro, mediante un plan de acción que se ejecutó durante los años 2016 a 2019 con una inversión total de 85.070 millones de pesos. Posteriormente en el año 2020 se crea el CONPES 3995 Política Nacional de Confianza y Seguridad Digital, el cual formula una política nacional que tiene como objetivo:

> establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital. Para alcanzar este objetivo, en primer lugar, se fortalecerán las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; en segundo lugar, se actualizará el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías[37].

Con este documento se busca que toda entidad oficial se encamine a adquirir las habilidades y destrezas para proteger y garantizar la integridad de la información que maneja. Es por ello que los Establecimientos educativos de educación básica y media deben conocer e implementar estas Políticas de gestión de la seguridad de la información, teniendo en cuenta que en la actualidad se diligencia plataformas del sector educativo como el Sistema de matrículas “SIMAT”, el Sistema de Información para el Monitoreo, Prevención y Análisis de la Deserción Escolar “SIMPADE”, entre otras plataformas en línea que están obligados los establecimiento educativos a mantener actualizados y que contienen información sensible de la comunidad educativa.

---

[36] Consejo Nacional de Política Económica y Social. Política Nacional de Seguridad Digital. CONPES 3854, [En línea]. [10 diciembre de 2021] disponible en: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

[37] Consejo Nacional de Política Económica y Social. Política Nacional de Confianza y Seguridad Digital. CONPES 3995, Bogotá D.C. 2020, p 3.

5.1.6. Ley 1273 de 2009. Ley de Delitos Informáticos en Colombia. En el año 2009, exactamente el 5 de enero, el CONGRESO DE LA REPÚBLICA DE COLOMBIA de Colombia expidió la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”[38].

Todo personal que labora en las Instituciones Educativas de Educación básica y media del país debe ser actualizado en cuanto a los distintos tipos de delitos informáticos legislados en Colombia a través de esta Ley. Es importante que todo el personal conozca cuales son los delitos informáticos, sus sanciones y consecuencias, por el acceso a información sin autorización, o la destrucción de la misma. Igualmente, el instalar software malicioso o suministrar a terceros información personal privada.

5.1.7. Ley estatutaria 1581 de 2012 y Decreto Nacional 1377 de 2013. Esta ley 1581 de 2012[39] constituye el marco general de la protección de los datos personales en Colombia, dicha Ley fue reglamentada parcialmente por el Decreto Nacional 1377 de 2013[40] y hace referencia a la garantía de los derechos y libertades estipuladas en el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Es apropiado que todo el personal que pertenece a los Establecimiento Educativos públicos del país de educación básica secundaria y Media sea conocedor de esta ley estatutaria y su decreto reglamentario con el propósito de dar a conocer a toda la

[38] Congreso de la República. Ley 1273 del 5 de enero de 2009. [En línea]. [10 diciembre de 2021] disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[39] Congreso de la República. Ley 1581 del 17 de octubre de 2012. [En línea]. [10 diciembre de 2021] disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
[40] Congreso de la República. Decreto 1377 del 27 de junio de 2013. [En línea]. [10 diciembre de 2021] disponible en: https://www.mintic.gov.co/arquitecturati/630/articles-9011_documento.pdf

comunidad educativa los principios y disposiciones contenidas en esta ley ya que son aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública como lo son las Instituciones Educativas. Se requiere que el personal que maneja la información personal de estudiantes, padres, docentes, directivos y administrativos le dé el adecuado tratamiento de datos personales de acuerdo normas e indicaciones dadas por el Gobierno Colombiano.

5.1.8. Ley 1266 de 2008 y Decreto 1081 de 2015. Ley por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones[41]. Esta Ley fue reglamentada por la presidencia de la Republica en su artículo 3° mediante el decreto 1081 de 2015[42] , en el artículo 2.1.1.4.1.1. Acceso general a datos semiprivados, privados o sensibles.

La Ley 1266 y el decreto 1081 son aplicable también a las Instituciones Educativas de educación básica secundaria y media del sector público del país, ya que estos establecimientos manejan también información financiera, crediticia, comercial y de servicios. Todo el personal que maneja este tipo de información debe conocer cuáles son sus deberes en el manejo de esta información y cuáles son los derechos que tienen los titulares de la misma información.

[41] Congreso de la República. Ley 1266 de 2008. [En línea]. [12 diciembre de 2021] disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34488

[42] Presidencia de la República. Decreto 1081 del 26 de mayo de 2013. [En línea]. [12 diciembre de 2021] disponible en: http://es.presidencia.gov.co/normativa/normativa/Decreto-1081-2015.pdf

5.1.9. Resolución 500 de 2021. El MinTIC emite la Resolución 500 de 2021, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital[43]". Esta resolución tiene por objetivo establecer los lineamientos generales para la implementación del MSPI y la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital. Asimismo, establece las directrices y estándares para la estrategia de seguridad digital[44].

En los establecimientos educativos se debe tener en cuenta estos lineamientos entre todos los servidores que componen los equipos de trabajo con el propósito de garantizar la seguridad e integralidad de la información de la comunidad educativa en general.

En los últimos años en Colombia se han venido elaborando y actualizando un número significativo de reglamentaciones y legislaciones en pro de mejorar la confidencialidad, integridad y disponibilidad de la información y de castigar al ciberdelincuente. Sin embargo, esta normatividad no es muy difundida, ni de exigencia obligatoria de cumplimiento en los establecimientos del Estado y se da prácticamente autonomía de aplicarlas o no, ya que no existe un control por parte del Estado Colombiano y en este sentido las Instituciones Educativas oficiales del país no son la excepción.

5.2 ESTUDIOS REALIZADOS A LA SEGURIDAD DE LA INFORMACIÓN DE ESTABLECIMIENTOS EDUCATIVOS OFICIALES DE EDUCACIÓN BÁSICA Y MEDIA DE COLOMBIA.

La mayoría de las personas ve la necesidad de proteger los equipos informáticos. Las máquinas cuestan dinero y, por lo tanto, tienen valor en sí mismas. Pero si se toma un momento para considerar por qué las organizaciones están tan dispuestas a gastar

[43] Ministerio de Tecnologías de la Información y las Comunicaciones. Resolución 500 de 2021. [12 diciembre de 2021] disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf
[44] Ministerio de Tecnologías de la Información y las Comunicaciones. MinTIC expide la resolución que establece los lineamientos y estándares para la estrategia de seguridad digital. [12 diciembre de 2021] disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/162626:MinTIC-expide-la-resolucion-que-establece-los-lineamientos-y-estandares-para-la-estrategia-de-seguridad-digital

grandes cantidades de dinero en sus sistemas informáticos, para almacenar, acceder y transmitir información, el valor de esa información se vuelve más evidente.

Después de todo, no tiene sentido gastar grandes cantidades de recursos limitados en equipos para procesar información a menos que la información en sí sea valiosa. Y debido a que la información se ha vuelto tan útil, no solo el equipo exige protección, sino también los datos.

En la comunidad educativa, la información sobre los estudiantes, el personal y otros recursos es mucho más valiosa para el funcionamiento de las Instituciones educativas oficiales que incluso el equipo más costoso.

Los datos educativos pueden representar años de inversión en actividades de recolección y mantenimiento, y pueden ser insustituibles como activo.

La Asociación Colombiana de Ingenieros de Sistemas (ACIS) llevó a efecto una encuesta nacional sobre seguridad informática en el año 2021 donde se entrevistaron a 13 sectores del país, entre los que se encuentran el sector educación.

La figura 1 muestra los tipos de incidentes de la encuesta nacional y se hace una diferencia con respecto a la encuesta realizada en el año 2020, donde se muestra que el error humano es el incidente que más se presenta al igual que el año anterior, pero con la característica que se redujo en un 12%. Dentro del análisis se observa que las brechas de seguridad provocadas por terceros, es el incidente que presenta mayor incremento con un 4%, le siguen en su orden el acceso no autorizado en la web con un 3% y la suplantación de identidad con un 2%.

En todo el mundo se presentan ataques a la información de las instituciones educativas, en especial en los últimos años; así se puede ver en diferentes informes o estudios, uno de ellos es el elaborado por la empresa DigiSOC– (*Information Security Operation Center*

de Digiware)[45], recopiló información desde 2019 a 2020, presentando resultados a nivel mundial, mostrando que los ataques contra universidades se dispararon un 100%, según BlueVoyant, revelando el 61% de ataques cibernéticos en el sector educativo y detección del 15,4%, también la detección de filtración de información en correo electrónico con el 15,2% y el 1.2% en herramientas de hacking, con grandes índices de ataques en los periodos del mes de febrero y marzo en América Latina.

Figura 1. Incidentes presentados en las organizaciones participantes

Fuente: ACIS, SISTEMAS: SISTEMAS No. 159 (2021). Resiliencia Digital. La nueva frontera para las organizaciones del siglo XXI. DOI: 10.29236/sistemas pag 33

Igualmente, este informe indicó que cada 5 de 6 ciberdelitos exitosos se deben a la suplantación de usuarios digitales, vulnerabilidades y falta de parcheo. Este mismo

[45] DIGIWERE - Ciberseguridad en la educación: conozca los nuevos retos cibernéticos del sector educativo, [En línea]. [10 marzo de 2022] disponible en: https://www.digiware.net/post/ciberseguridad-en-la-educaci%C3%B3n-conozca-los-nuevos-retos-cibern%C3%A9ticos-del-sector-educativo

informe indica que la principal debilidad que han tenido las Instituciones educativas fueron las aplicaciones web, encontrando que un 67% de las amenazas provienen de fuera del país, y un 33% dentro del mismo país.

En este mismo sentido la revista "Tierra Infinita"[46] hace un análisis donde se determina las mejores prácticas de seguridad con el propósito de ser utilizadas de acuerdo a las necesidades de la empresa, ya que se debe tener en cuenta que no todas las empresas tienen las mismas características o necesidades en cuanto el envío o manejo de la información. El artículo menciona cuatro modelos de seguridad de la información (OSSTMM3, ISO 27001, NIST y COBIT 5), y posteriormente hace la comparación de sus características, todo con el propósito de definir la mejor opción para ser aplicada en las instituciones educativas. Lara y Corella citan textualmente "Para conseguir esta orientación es necesario el aporte de los otros modelos de gestión de la seguridad, con sus características esenciales, que los hacen adecuados para los diferentes aspectos a considerarse durante la planificación e implementación de un sistema de gestión de la seguridad de la información. Por ejemplo, se puede utilizar el *framework* de ciberseguridad de NIST para ayudar en el diseño de los controles de TI de ISO 27001"[47]. Finalmente recomienda que el modelo específico de seguridad informática a seguir debe escogerse teniendo en cuenta la realidad del entorno donde se aplicará dicho sistema de seguridad.

"LA FM"[48] presenta estudio al respecto de la seguridad de la información en Colombia y otros países y manifiesta que los colombianos tienen poca cultura relacionada con la ciberseguridad y la necesidad de proteger la información del uso no autorizado. Da cifras sobre el alto número de empresas consultadas que no cuentan con los controles básicos

[46] LARA Elva G, CORELLA Flavio A. Comparación de modelos tradicionales de seguridad de la información para centros de educación. Revista Tierra Infinita N° 4. Jun-Ago.2018, p. 20-28.
[47] LARA Elva G, CORELLA Flavio A. Comparación de modelos tradicionales de seguridad de la información para centros de educación. Revista Tierra Infinita N° 4. Jun-Ago.2018, p. 27.
[48] AGUIRRE, Jhon. El 67% de los colegios en Latinoamérica han sido víctimas de ataques cibernéticos. *La FM*. [En línea] 28 Mayo 2018. [Consultado 10 marzo de 2022]. Disponible en: https://www.lafm.com.co/tecnologia/el-67-de-los-colegios-en-latinoamerica-han-sido-victimas-de-ataques-ciberneticos

necesarios para la protección de su información, además muestra, que el 50% de las empresas encuestadas aceptaron que se han visto afectadas por infecciones de malware. Igualmente, muestra cifras alarmantes de las instituciones educativas evaluadas en Latinoamérica y que manifiestan que han sido víctimas en algún momento de ataques a sus bases de datos por ciberdelincuentes.

Parra y Yánez[49] llevaron a efecto un estudio con el propósito de hacer un análisis de vulnerabilidad tecnológica en un centro de educación superior, para dicho estudio se hizo necesario utilizar una herramienta de test de intrusión y haciendo uso de la metodología internacional OSSTMM se pudo encontrar que tenía ciertos puertos abiertos, y una cantidad de vulnerabilidades; el mismo estudio determinó de qué forma se puede acceder a unos de los puertos.

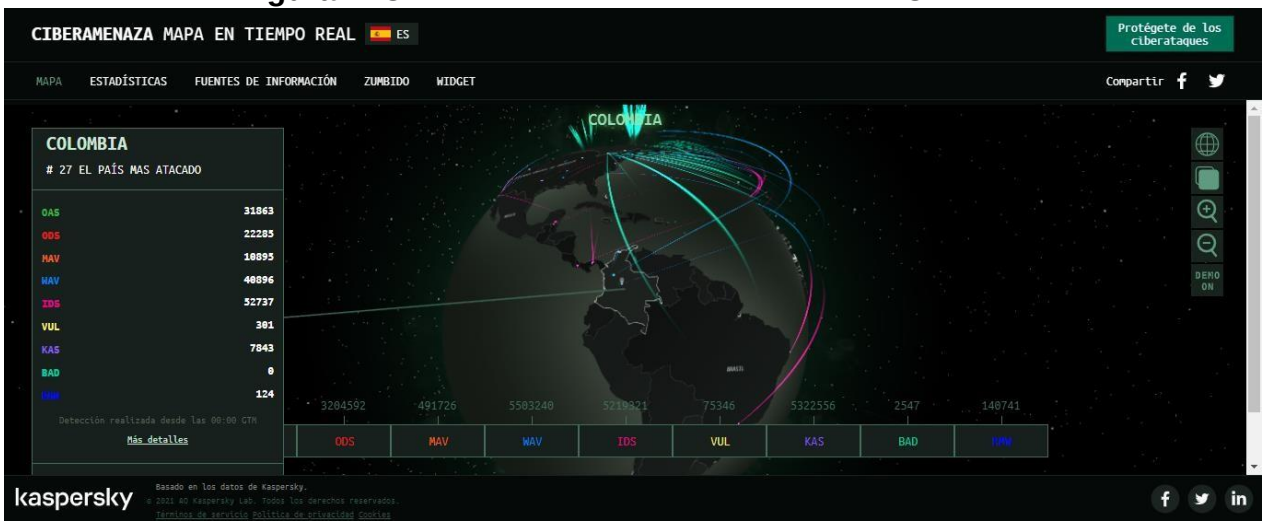
De acuerdo a Bertolín "la seguridad es una forma de protección contra los riesgos, es un conjunto de pasos o procedimientos en el que se toma en cuenta elementos como aspectos tecnológicos, de gestión organizacionales, de negocios, de tipo legal, de cumplimiento, entre otros"[50]. De aquí la importancia de ser conocedores de los distintos modelos y estándares para la seguridad de la información, algunos de estos análisis son elaborados por Ezquivel Triana[51] en el 2014 en su escrito titulado "Modelos de Seguridad", quien da a conocer que los modelos CMMI, MBOK, ITIL y COBIT, entre otros modelos y estándares, ayudan a hacer un análisis de cuan conveniente es su aplicación para mantener la seguridad de la información en los establecimientos educativos.

Se ha evidenciado que los establecimientos educativos no toman importancia en la protección de su información y desconocen cuál es la forma apropiada de llevar a efecto buenas prácticas de control de los contenidos o páginas visitadas por los empleados o estudiantes que hacen uso de internet. Los estudiantes de la Universidad Uniminuto,

[49] PARRA BARZOLA Liliana M.; YÁNEZ CEDEÑO Erick S. Análisis de vulnerabilidades en la Infraestructura tecnológica de una empresa, utilizando herramientas de test de Intrusión. Trabajo de investigación .Guayaquil: Universidad de Guayaquil. Facultad de Matemáticas y Física, 2017. 154p.
[50] BERTOLÍN, J. A. Seguridad de la información. Redes, informática y sistemas de información, Madrid. Editorial Paraninfo. 2008. 592p
[51] EZQUIVEL TRIANA, Ricardo. Modelos de seguridad. Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacional, Bogotá. 2014. 26p

Bermúdez Sanmiguel y Tafur Torres[52] realizaron un trabajo de grado donde hacen un análisis de esta problemática permitiendo hacer un estudio apropiado con el propósito de hacer correcciones a dicha situación, encuentran que el Colegio Cooperativo Espíritu Santo los equipos informáticos presentan continuos daños en el sistema operativo por la descarga excesiva de virus a través de la red de internet y proponen la instalación de un firewall en el servidor de la sala de sistemas, logrando que se proteja la red LAN de intrusos y accesos no autorizados, como también el bloqueo de páginas web inseguras.

Figura 2. CIBERAMENAZA MAPA EN TIEMPO REAL



Fuente: KASPERSKY. [En línea]. Rusia. Disponible en: https://cybermap.kaspersky.com/es

En internet se encuentra la página web de la empresa Kaspersky[53] en donde se muestra un mapa en tiempo real (Figura 2), sobre las ciberamenazas a nivel mundial, muestra estadísticas importantes para realizar diagnósticos y conocer el panorama mundial y nacional en estos aspectos. Con esta herramienta se puede ver como se encuentra Colombia en cuanto ataques perpetuados a los sistemas informáticos, dicha información

[52] BERMUDEZ SANMIGUEL, Edgar y TAFUR TORRES, Diego. Sistema de Seguridad Informático para el Colegio Cooperativo Espíritu Santo De Girardot. Trabajo de grado realizado para optar al título de tecnólogo en redes de computadores y seguridad informática. Girardot: Corporación Universitaria Minuto de Dios. Facultad de Ingeniería de Sistemas, 2011. 33p.

[53] KASPERSKY. Ciberamenaza Mapa en Tiempo Real. [Sitio web]. Rusia. [Consultado marzo 10 de 2022]. Disponible en: https://cybermap.kaspersky.com/es

es relevante para la presente monografía para saber en qué posición se encuentran según los ataques en cada continente y a nivel mundial.

En Colombia existe un grupo de líderes en consultoría denominado MARSH quienes son profesionales en la gestión de riesgos; en su blog "El Riesgo en Contexto" publican análisis y estudios en estos ámbitos y uno de ellos el Doctor Jhon Fraser[54] publica en abril de 2018, un análisis llamado "El sector educativo, un blanco perfecto para ciberataques", donde se hace un detallado del porqué cada día se ven más ataques a los establecimientos educativos. En este informe se indica que "el sector educativo se clasifica en uno de los más susceptibles al riesgo cibernético. ¿Por qué? En pocas palabras, las redes en las instituciones educativas albergan el tipo de información que codician los hackers y, dado el entorno académico abierto, esas redes tienden a ser más fáciles de penetrar"[55].

La Universidad del Rosario en Colombia llevó a efecto un estudio denominado "Colombia no está preparada ante un ciberataque"[56], en el que presenta un video donde se explica la situación actual del país en materia de seguridad de la información, los que aporta información valiosa al panorama nacional de la seguridad de la información en los establecimientos educativos. En este informe se indica que "el 81% de los funcionarios de empresas grandes y pequeñas tienen acceso a internet y sin embargo, según un reciente estudio, el presupuesto destinado a seguridad digital es de menos del 1% de las ventas o inversiones. Mientras tanto, los ataques cibernéticos aumentan en sofisticación e impacto, así que la única salida es anticiparse y ampliar el espectro a la hora de gestionar los riesgos"[57].

---

[54] FRASER, John. El sector educativo, un blanco perfecto para ciberataques. *BLOG: EL RIESGO EN CONTEXTO*. [En línea]. 2018, [consultado 15 octubre de 2020]. Disponible en: https://www.marsh.com/co/insights/risk-in-context/sector-educativo-ciberataques.html

[55] FRASER, John. El sector educativo, un blanco perfecto para ciberataques. *BLOG: EL RIESGO EN CONTEXTO*. [En línea]. 2018, [consultado 15 octubre de 2020]. Disponible en: https://www.marsh.com/co/insights/risk-in-context/sector-educativo-ciberataques.html .

[56] UNIVERSIDAD DEL ROSARIO. Colombia no está preparada ante un ciberataque. [En línea]. [consultado 11 marzo de 2022] disponible en: https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/

[57] Ibid.

La Universidad Santo Tomas con su informe “Los Ataques Informáticos en el Sector Educativo”[58], presenta un análisis sobre la seguridad de la información en los establecimientos educativos y redacta casos como el de la Universidad de los Andes cuando en el 2015 un estudiante de ingeniería de software, consiguió de forma no autorizada la contraseña de varios docentes para acceder a la plataforma de notas y poder posteriormente modificarlas; casos como estos se repiten en Colombia en grandes cantidades en periodos cortos de tiempo en el Sector de la Educación.

La Revista Dinero, en su informe “En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos”[59], suministra información detallada sobre estos ataques, como por ejemplo, indica que el Servicio de inteligencia de amenazas de la compañía Fortinet publicó un estudio en el último congreso Andicom que se lleva a cabo en Cartagena, revelando que entre los meses de abril y julio del 2019, en Colombia se presentaron más de 40 billones de intentos de ciberataques, denominados *exploits*, considerados programas o códigos que aprovechan las debilidades de las aplicaciones o de los sistemas para que estas sean controladas por los atacantes.

La universidad Libre de Colombia indica en el estudio “Crecen los ataques de Phishing en Colombia”[60], presenta detalladamente este tipo de ataque; igualmente indica que en Colombia al mes, se registran alrededor de 187 denuncias por robos informáticos, siendo el phishing el más común, delito perpetuado en su mayoría por medio de correos electrónicos, de esta forma se engaña a las personas para que suministren información bancaria, documentos de identidad, contraseñas, entre otros.

[58] UNIVERSIDAD SANTO TOMÁS. Los Ataques Informáticos en el Sector Educativo. [En línea]. [consultado 11 marzo de 2022] disponible en: https://auditoriainterna.usta.edu.co/index.php/120-los-ataques-de-hacking-en-el-sector-educativo

[59] DINERO. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [En línea]. [Consultado 11 marzo de 2022]. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

[60] UNIVERSIDAD LIBRE. Crecen los ataques de Phishing en Colombia. [En línea]. [Consultado 11 marzo de 2022] disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/424-crecen-los-ataques-de-phishing-en-colombia

La Universidad Tecnológica de Pereira en su artículo “Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico”[61] un análisis de riesgos con base en la norma ISO 27005 y hace una identificación de los activos críticos del área de secretaría académica de las instituciones educativas nivel básico y los riesgos asociados, con el propósito de crear el plan de tratamiento de riesgos, así mismo hace un análisis de la normatividad del Ministerio de Educación, del Ministerio de Tecnologías de la Información y las Comunicaciones 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 educativas.

El periódico el Tiempo publicó en junio de 2021, que la Universidad del Bosque recibió un ataque cibernético en donde se vio afectada la información personal de la comunidad educativa, indica el informe que en el ataque tomaron el control del perfil de Twitter de la universidad, en donde anunciaron que el equipo de seguridad de la universidad debería comunicarse con los atacante para poder recuperar la información secuestrada; también se vio afectado otros sistemas internos, página web y los correos institucionales[62].

La Universidad Javeriana en sus sedes de Bogotá y Cali también fue víctima de un ataque cibernético según informó “elcolombiano.com”, la Universidad fue afectada en su sistema tecnológico y mantuvo inactivo varios servicios por más de 30 horas[63].

Los ataques informáticos o robos de información a instituciones educativas oficiales de educación básica y media del país vienen en aumento, pero registros de los mismos casi no se evidencian y las Instituciones prefieren callar antes que denunciar o simplemente

[61] Benavides S. Alejandra, Blandón J. Carlos. Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. Scientia et Technica Año XXII, Vol. 23, No. 01, marzo de 2018. Universidad Tecnológica de Pereira. ISSN 0122-1701

[62] EL TIEMPO. Universidad El Bosque sufre ataque informático [En línea]. [Consultado 11 marzo de 2022]. Disponible en: https://www.eltiempo.com/vida/educacion/universidad-el-bosque-sufre-ataque-informatico-599303

[63] Elcolombiano.com. Cibersecuestradores: ahora le cayeron a la Javeriana. [En línea]. [Consultado 11 marzo de 2022]. Disponible en: https://www.elcolombiano.com/colombia/ataques-contra-javeriana-y-dane-alertan-de-mas-ciberataques-KB16069751

no le prestan la importancia que se le debe dar. A nivel Nacional no se encuentran estudios detallados sobre los ataques a establecimientos oficiales de secundaria y media.

5.3 PANORAMA ACTUAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN ESTABLECIMIENTOS EDUCATIVOS OFICIALES DE EDUCACIÓN BÁSICA SECUNDARIA Y MEDIA DE COLOMBIA

El avance tecnológico de los últimos años ha convertido a los jóvenes en una nueva generación dependiente de la tecnología, así lo indica también el Dr Bonilla[64] que para los jóvenes la tecnología se ha vuelto una obsesión. Los jóvenes están adquiriendo distintos hábitos en sus estilos de vida, mejorando en gran manera el acceso a información más variada y en tiempo real, pero ha generado una serie de problemas como la necesidad de adaptabilidad a los grupos sociales, una gran dependencia a los medios tecnológicos, genera afectaciones emocionales y permite en muchos casos interacción virtual con expendedores de drogas, pedófilos, redes de prostitución infantil, o en general delincuentes en búsqueda de víctimas en diferentes aspectos.

Las Instituciones Educativas en Colombia desempeñan un papel clave en la sociedad, no solo por capacitar, enseñar y orientar a los estudiantes, sino porque desde el Ministerio de Educación Nacional se les exige total exactitud en la calidad de la información que se reportan en las distintas plataformas de control como SIMAT[65] (Sistema de matrículas), SIGEP[66] (Sistema de Información y Gestión del Empleo Público), SIMPADE[67] (Sistema de Información para el Monitoreo, la Prevención y el Análisis de la Deserción Escolar), entre otras, de cada uno de los estudiantes, acudientes,

---

[64] BONILLA, Francisco. La adicción a las nuevas tecnologías en jóvenes y adolescentes. *BLOG: Psicología y salud*. [En línea]. 2022, [consultado 15 octubre de 2022]. Disponible en: https://www.quironsalud.es/blogs/es/psicologia-salud/adiccion-nuevas-tecnologias-jovenes-adolescentes

[65] SIMAT. Sistema de matrículas. [Plataforma web] Disponible en: https://www.sistemamatriculas.gov.co/

[66] SIGEP. Sistema de Información y Gestión del Empleo Público. [Plataforma web] Disponible en: https://www.funcionpublica.gov.co/web/sigep

[67] SIMPADE. Sistema de Información para el Monitoreo, la Prevención y el Análisis de la Deserción Escolar. [Plataforma web] Disponible en: https://simpade.mineducacion.gov.co/simpade/

administrativos y docentes; lo cual requiere gran nivel de seguridad en el tratamiento de la misma, es de aclarar que aunque las Instituciones Educativas están autorizadas por la Ley en cuanto el uso y tratamiento de esta información en el ejercicio de la función educativa, y las mismas deben salvaguardar esta información sensible y evitar rigurosamente al personal no autorizado su acceso o divulgación sin la autorización o consentimiento de los titulares, en especial porque la mayor parte de estos datos corresponden a datos de menores de edad.

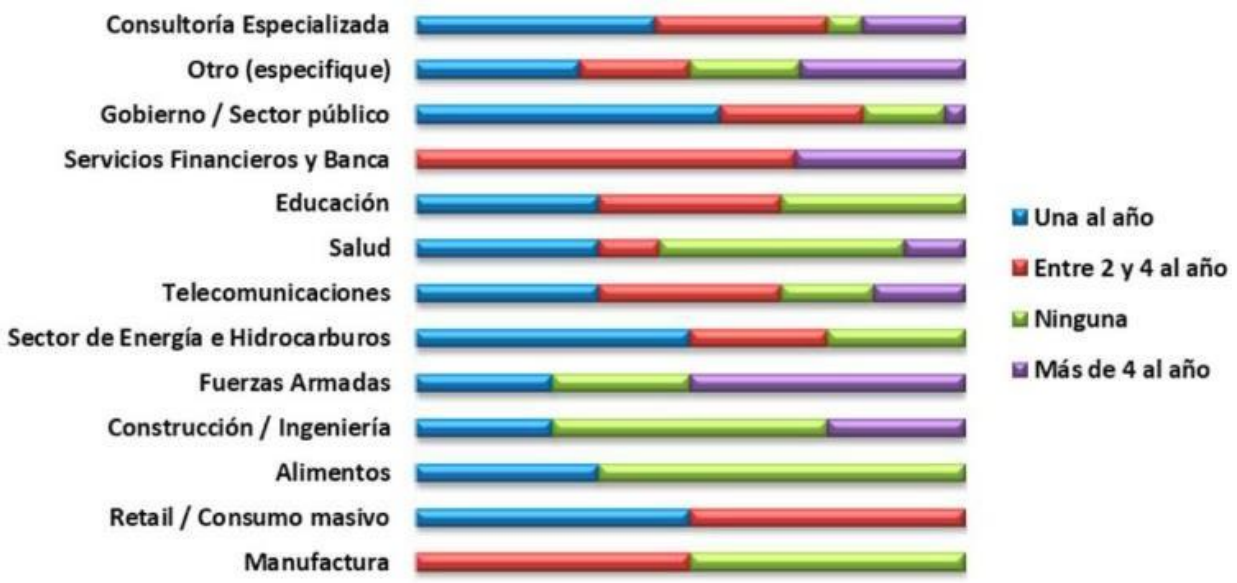
En los últimos años se han realizado algunos estudios con respecto a la seguridad de la información que manejan las Instituciones Educativas de Colombia, tanto en la educación Básica y Medía, como también en la educación Superior, sin embargo, se presenta a continuación el panorama actual sobre la seguridad de la información en establecimientos educativos oficiales de educación básica secundaria y media de Colombia. Uno de estos estudios es el de la empresa *Digiwere*[68] en el 2018, en el cual ubica a Colombia en el quinto puesto en Latinoamérica, entre los países más atacados por los ciberdelincuentes a los establecimientos educativos. Igualmente, expresa que el Laboratorio de Investigación de *ESET* Latinoamérica en cabeza de Camilo Gutiérrez, expresa que en Colombia es poca la cultura relacionada con la ciberseguridad y la necesidad de proteger su información del uso no autorizado. Pero en lo que concierne a las Instituciones educativas del país se indica que dichos establecimientos manifiestan que han sido víctimas en algún momento de ataques a sus bases de datos por ciberdelincuentes y en su gran mayoría se debe a la falta de controles básicos de protección, como lo es, la obtención y uso de Antivirus, falta de ***Backups*** de la información y aplicación de *Firewall*.

Es importante que el sector educativo haga evaluaciones periódicas sobre la seguridad de la información en sus establecimientos, pero esta conciencia parece no verse reflejada en el sector de la educación. La Asociación Colombiana de Ingenieros de Sistemas ACIS en su encuesta nacional elaborada en el 2021 sobre seguridad de la información muestra

[68] DIGIWERE - ¿A qué amenazas cibernéticas se enfrentará el sector educativo con la transformación digital?, [En línea]. [27 diciembre de 2019] disponible en: http://www.digiware.net/?q=es/blog/a-que-amenazas-ciberneticas-se-enfrentara-el-sector-educativo-con-la-transformacion-digital

en su revista “SISTEMAS”[69] que en sector educación la mayoría no realiza evaluaciones de seguridad durante el año, algunas hacen una sola y pocas entre dos y cuatro al año como se evidencia en la figura 3.

Figura 3. Evaluación de seguridad por sectores



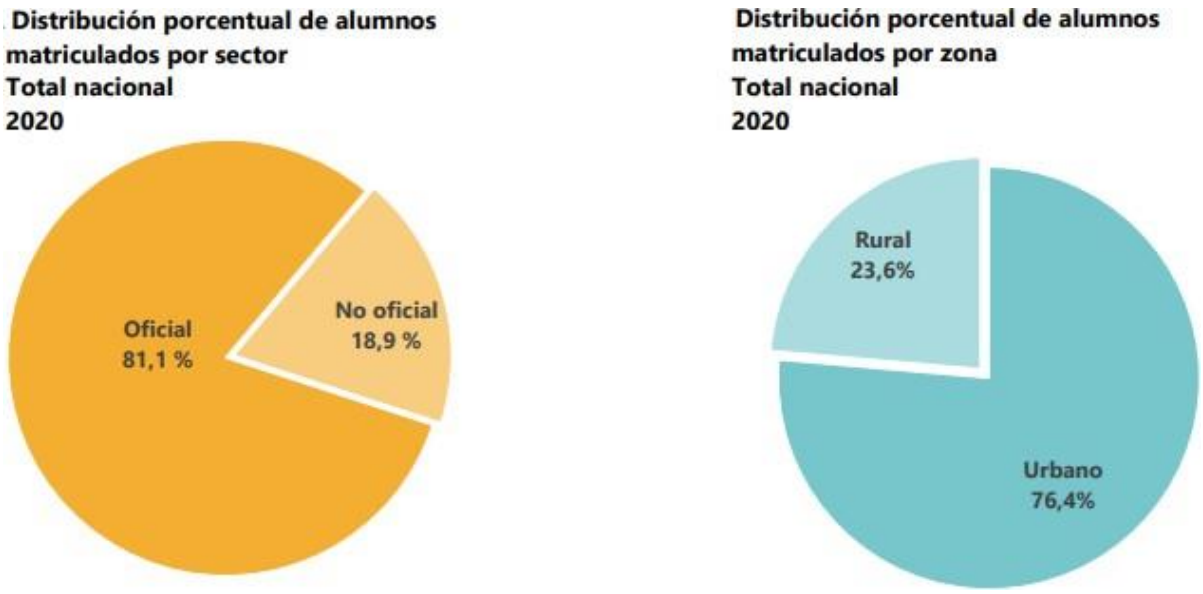
Fuente: ACIS, Revista SISTEMAS No. 159 (2021). Resiliencia Digital. La nueva frontera para las organizaciones del siglo XXI. DOI: 10.29236/sistemas

De acuerdo a estos estudios en Colombia no existe la conciencia suficiente de la protección de la información por parte de las Instituciones Educativas de básica y medía tanto públicas como privadas, o no cuentan con la capacitación necesaria; por ello las Instituciones educativas se han convertido en blanco fácil para los delincuentes informáticos, que ven con gran interés acceder a la gran cantidad de información que manejan estas Instituciones debido al gran número de estudiantes que se matriculan en el país.

[69] ACSI. Revista SISTEMAS No. 159 (2021). Resiliencia Digital. La nueva frontera para las organizaciones del siglo XXI. DOI: 10.29236/sistemas

Según el DANE[70] en Colombia para el año 2020 la matrícula nacional en el sector público fue de 8.018.501 alumnos. Siendo esta cifra el 81,1% del total de estudiantes matriculados en todo el país tal como se observa a continuación en la figura 4.

Figura 4: Distribución porcentual de alumnos matriculados por sector total nacional 2020



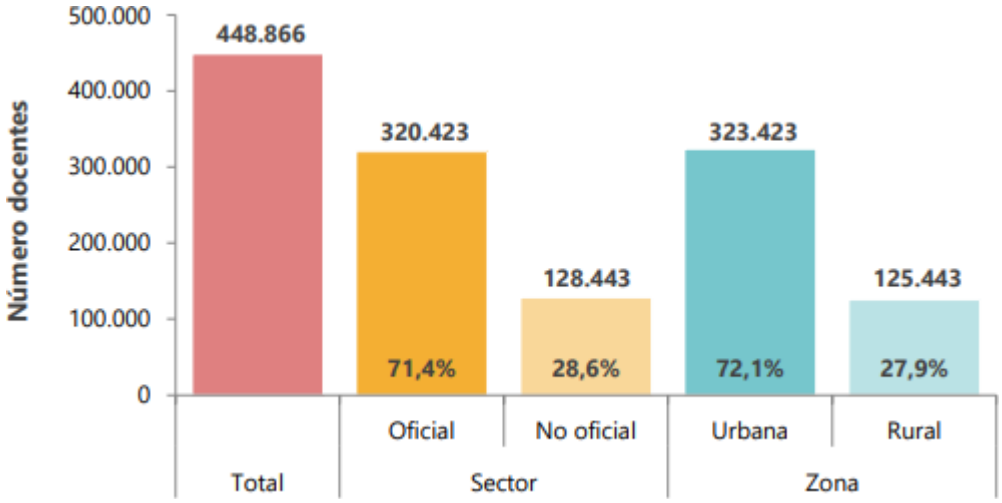
Fuente: DANE. Boletín Técnico Educación Formal (EDUC). Bogotá D.C. 2020. Disponible en: https://www.dane.gov.co/files/investigaciones/boletines/educacion/bol_EDUC_20.pdf

Estos gráficos reflejan la cantidad de estudiantes que hay matriculados en estos niveles de formación y por ende dan una idea de la cantidad de datos que se manejan en los establecimientos educativos del país. Sin embargo, el Gobierno Nacional a pesar de conocer a detalles estas estadísticas, no suministra los recursos, ni los medios que se requieren para la custodia apropiada de esta información recolectada año tras año de los estudiantes y acudientes con información sensible como lo es ubicación, identificación y otros que al caer en manos equivocadas pueden afectar la integridad de sus propietarios.

[70] DANE. Dirección Nacional de Estadística. [Sitio web] [Recuperado 12 abril de 2022]. Disponible en: https://www.dane.gov.co/

Pero no solo se manipula información de padres y estudiantes, también los establecimientos educativos manejan datos de los docentes y administrativos pertenecientes a las mismas y que para el año 2020 fue de fue de 448.866 docentes en el país según el DANE.

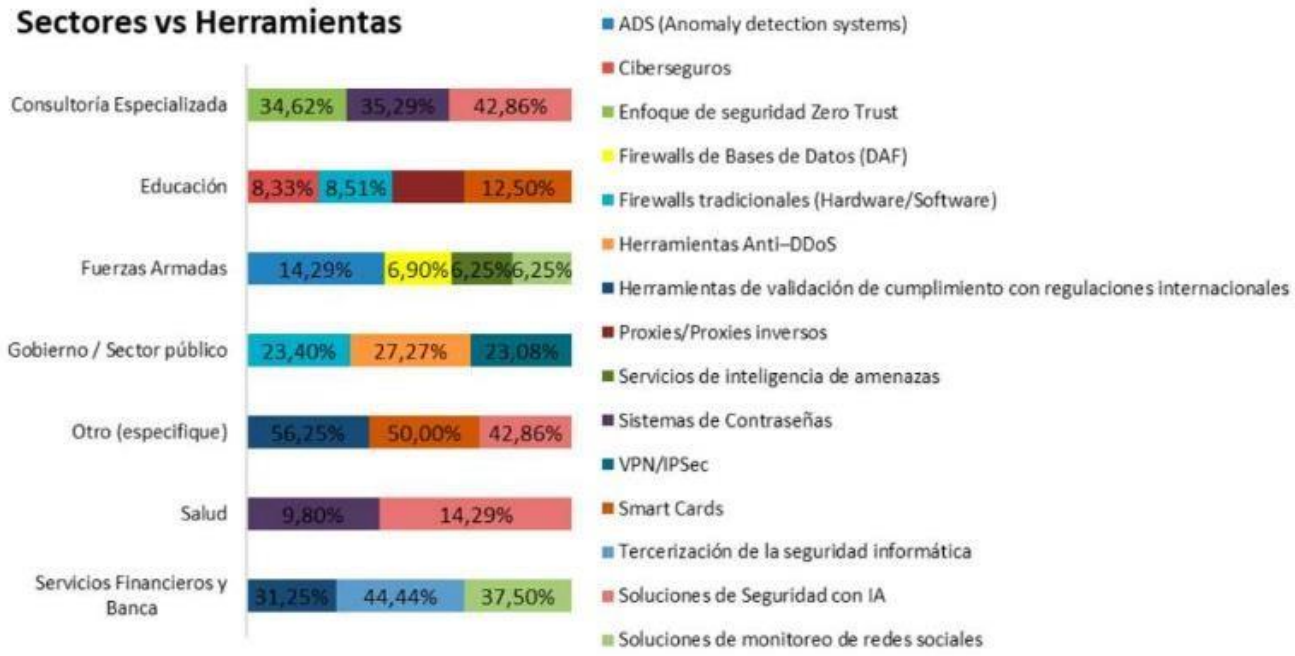
Figura 5: Número y distribución porcentual de docentes con asignación académica según sector y zona Total nacional 2020



Fuente: DANE. Boletín Técnico Educación Formal (EDUC). Bogotá D.C. 2020 [Recuperado 12 abril de 2022]. Disponible en: https://www.dane.gov.co/files/investigaciones/boletines/educacion/bol_EDUC_20.pdf

Cada miembro de la comunidad educativa confía en la capacidad del establecimiento educativo para proteger la información suministrada, pero la realidad muestra que el sector público de la educación Colombiana, no invierte en personal capacitado para la seguridad de la información, ni mucho menos invierten en recursos físicos o lógicos propios para la protección de la información como servidores, firewall entre otros, como tampoco cuentan con la implementación de Sistema de Gestión de Seguridad de la Información (S.G.S.I). Así se muestra en la figura 6 donde se puede ver que en el sector educativo encuestado solo el 8,33% cuenta con ciberseguros, el 8,51% tienen los *firewalls* tradicionales, un 8% *proxies* y 12,5 % cuentan con *Smart cards*.

Figura 6. Mecanismos de seguridad en sectores



Fuente: ACIS, Revista SISTEMAS No. 159 (2021). Resiliencia Digital. La nueva frontera para las organizaciones del siglo XXI. DOI: 10.29236/sistemas pág. 42

Es evidente que los establecimientos educativos no cuentan con herramientas robustas que permitan garantizar la confidencialidad, integridad y seguridad de la información que se maneja en dichos establecimientos.

Lo anterior se puede considerar por la falta de recursos propios que permitan la adquisición de los elementos mínimos necesarios para garantizar la seguridad de la información en los establecimientos educativos públicos de educación básica y media del país. Sin embargo, debido a las condiciones actuales, la necesidad de acceder a la información de internet y también debido a la pandemia presentada, el uso diario de computadores y demás herramientas TIC se viene implementado en mayor proporción, en todas las instituciones públicas y privadas de educación básica y media del país.

Tabla 1. Distribución porcentual de la frecuencia de uso de los bienes TIC, por nivel educativo Total nacional 2020

Frecuencia de uso	Nivel educativo				
	Preescolar	Básica primaria	Básica secundaria	Media	CLEI
Ningún día de la semana	9,4	3,1	2,3	2,0	6,4
Todos los días de la semana	10,7	15,5	30,7	34,4	12,1
Al menos una vez a la semana	68,0	73,9	63,3	59,5	63,5
Al menos una vez al mes	8,1	5,0	2,4	2,9	13,3
Una vez al mes pero no todos los meses del año	3,7	2,4	1,3	1,3	4,7

Fuente: ACIS, Revista SISTEMAS No. 159 (2021). Resiliencia Digital. La nueva frontera para las organizaciones del siglo XXI. DOI: 10.29236/sistemas pág. 42.

En la tabla 1 se observa que el uso de las TIC viene en aumento en todos los niveles de educación y si no se cuenta con la seguridad apropiada, las instituciones estarán cada día más expuestas a ataques cibernéticos internos y externos.

Otro aspecto importante en cuanto al cuidado de la información en físico que se maneja en las instituciones educativas públicas del país viene tomando gran importancia y es por eso que hoy en día los Establecimientos educativos oficiales de educación básica y media vienen implementando la aplicación de la Ley General de Archivo[71] (Ley 594 del año 2000), la cual estipula y regula las normas y procedimientos para el manejo de los archivos tanto físicos como digitales. Por este motivo las Instituciones educativas se encuentran implementando los procesos de digitalización de los archivos físicos como hojas de vida de los docentes y administrativos, matrículas de estudiantes de años anteriores, libros finales de calificaciones y los observadores de los estudiantes, almacenando dichos archivos en equipos de cómputo conectados a las redes LAN institucionales.

Esta información digital es manejada por personal administrativo de las instituciones educativas como las secretarias, pagadores y auxiliares de oficina, quienes en su gran mayoría o casi en su totalidad no tienen preparación en cuanto a la seguridad de la

[71] COLOMBIA. ARCHIVO GENERAL DE LA NACION. Ley 594; 14, 07, 2000; Ley General de Archivo.

información, conllevando esto a que el personal encargado de la información institucional, no se preocupe por tener los controles apropiados en sus dispositivos de conexión, ni crean sistemas de encriptación o de mensajería codificada, ni asignan los roles apropiados a los distintos usuarios que manejan la información.

Los recursos que manejan las Instituciones educativas oficiales de la educación básica y media del país, no hacen cobros por costos de matrículas ni pensiones, por consiguiente todo el personal que labora en una Institución educativa son pagados por el Estado Colombiano y los únicos recursos que manejan son los enviados por el Gobierno para ser utilizados en labores de mantenimiento locativo y de infraestructura o para compra de material educativo necesario para el normal funcionamiento de la labor educativa. Por este motivo, los pocos recursos que utilizan las Instituciones Educativas no son suficientes para invertir en personal capacitado en seguridad informática, ni mucho menos en dispositivos para protección de la información.

El Gobierno Nacional, mediante el Ministerio de las TIC, desde hace algunos años viene generando una serie de guías y metodologías para garantizar la seguridad de la información, ellas son “La Política General MSPI”, “Controles de Seguridad y Privacidad de la Información”, “Guía de indicadores de gestión para la seguridad de la información”, y CONPES 3854 Política Nacional de Seguridad Digital.

En vista del incremento del uso de herramientas tecnológicas y del uso del Internet debido a situación de emergencia sanitaria por el COVID19, en Colombia se creó un documento denominado CONPES 3995 de 2020, diseñado por el CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL (CONPES) dicho documento indica textualmente que el CONPES “formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital”[72], dicho documento está programado para ser ejecutado durante el período 2020-2022, sin embargo este no es el primero de esta clase que se ha creado en Colombia, a este, lo

[72] Consejo Nacional de Política Económica y Social. Política Nacional de Confianza y Seguridad Digital. CONPES 3854, Bogotá D.C. 2020, p 3.

han antecedido en el año 2011 el CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa y luego en el año 2016 el Documento CONPES 3854 “Política Nacional de Seguridad Digital” los cuales fueron creados para fortalecer y generar capacidades en el Gobierno Nacional con un enfoque de gestión de riesgos, con el propósito de brindar seguridad y defensa a los colombianos y a las Instituciones oficiales en el ciberespacio; sin embargo, ese propósito no logró conseguir un avance mínimo esperado, ya que no se difundió de forma apropiada, ni se involucró personal relacionado con la seguridad de la información a todos los estamentos del Estado y en caso particular no se implementó en las entidades territoriales certificadas para el manejo de la educación en Colombia y a su vez las Instituciones Educativas oficiales de educación básica y media.

En Colombia se han implementado las políticas y estrategias desde el Gobierno nacional para brindar seguridad y defensa en el ciberespacio, con un enfoque de gestión de riesgos (Figura 8), la cual estará vigente entre los años 2020 y 2022. Sin embargo, la transformación digital da pasos gigantes en actualizaciones, estas estrategias actualmente se están quedando cortas para generar confianza y seguridad digital en los colombianos.

Es así como en el papel existen buenas recomendaciones y prácticas para la prevención e implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I) pero en la realidad muy escasas intensiones y recursos para ello.

Los Establecimientos educativos solo se interesan por tener conectividad y poder diligenciar en las fechas programadas la información que les solicitan, pero no cuentan con los requerimientos mínimos para garantizar la seguridad e integridad de la información que manejan.

Figura 8: Implementación de Políticas y estrategias desde el Gobierno nacional para brindar seguridad y defensa en el ciberespacio.

Fuente: CONPES 3995 POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL. Bogotá 2020. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Por todo lo anterior se puede ver que en Colombia las Instituciones Educativas Oficiales de Educación básica y media son uno de los sectores más susceptibles al riesgo cibernético debido a que en sus redes informáticas tienden a ser más fáciles de penetrar, volviéndose motivante para los hackers ya que allí reposa la información sensible que son codiciadas por ellos. Algunos factores que evidencian esta vulnerabilidad a los ciberataques son los siguientes:

5.3.1. Datos personales. Las Instituciones Educativas manejan información como nombres completos, fechas de nacimiento, números de identificación, direcciones de residencia, números de contacto, correos electrónicos, datos de familiares y padres de familia, todo esto de estudiantes, docentes y personal administrativo actuales y antiguos.

5.3.2. Múltiples puntos de entrada. Una de las metodologías más utilizadas hoy en día es el intercambio de conocimiento a través de redes sociales y encuentros sincrónicos entre grupos de trabajo y docentes. Las redes informáticas de las Instituciones educativas atienden a una variada cantidad de usuarios entre los que se encuentran docentes, estudiantes, administrativos, padres de familia, proveedores externos, entre otros. Estos

usuarios tienen acceso a las redes instituciones las 24 horas del día, durante todo el año y lo hacen desde dispositivos que pueden no ser monitoreados o que se encuentren infectados por virus informáticos.

5.3.3. Inseguridad social. En Colombia muchos establecimientos educativos de básica y media, permiten que sus estudiantes y docentes accedan a las redes sociales desde sus dispositivos móviles o teléfonos inteligentes. A pesar de que algunas Instituciones educativas cuentan con seguridad perimetral, son más las que no cuentan con políticas de seguridad para el acceso a redes sociales o que establezcan estándares aceptados para el intercambio de información patentada y propiedad intelectual.

5.3.4. Hardware de seguridad insuficiente. La mayoría de las instituciones educativas oficiales de educación básica y media no cuentan con recursos suficientes para la adquisición de dispositivos que aseguren y garanticen la integridad de la información que almacenan en sus equipos de cómputo.

El acceso a la información manejada por las Instituciones educativas de forma no autorizada, puede traer grandes perjuicios a cualquiera de los miembros de la comunidad educativa; algunos ejemplos de estas dificultades son los robos de identidad, acoso electrónico, *bullying, ciberbullying*, ataques físicos, violaciones a la propiedad intelectual, entre otros.

Es claro que, en Colombia las Instituciones Educativas oficiales de educación básica y media, casi en su totalidad carecen de sistemas de gestión de seguridad de la información, ni cuentan con los conocimientos apropiados para garantizar la seguridad e integridad de la información que administran y mucho menos cuentan con personal capacitado que se encarguen exclusivamente de este aspecto. Es por ello por lo que se requiere que las Instituciones educativas tomen más en serio el aspecto de la seguridad informática y gestionen recursos para poder garantizar la preservación y seguridad de la información que manejan. Igualmente se deben asumir estándares y políticas de seguridad de la información.

5.4 RECOMENDACIONES DE ACUERDO CON EL PANORAMA DESCRITO PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN EN LOS ESTABLECIMIENTOS EDUCATIVOS

La intención de este objetivo es proporcionar a las Instituciones educativas oficiales de educación básica y media de Colombia, una guía básica y atemporal para los encargados de tomar decisiones mediante la identificación de factores que deben tenerse en cuenta cuando desarrollan estrategias y políticas de seguridad o no desarrollan por carecer de ellas, para cumplir con las condiciones particulares y circunstancias locales de cada establecimiento educativo. Estás recomendaciones están diseñadas para ayudar al personal educativo en su esfuerzo por caminar por la delgada línea entre mantener seguros los datos educativos y, al mismo tiempo, estar disponibles para personas autorizadas con fines legítimos. De acuerdo a toda la bibliografía estudiada y en especial el documento publicado por el Foro Nacional de Estadísticas Educativas de los Estados Unidos[73], se diseñaron las recomendaciones técnicas para proteger los datos digitales que se manejan en las Instituciones educativas; como en su mayoría el personal administrativo de estas instituciones no cuentan con la suficiente capacitación y experiencia en el campo de la seguridad de la información, estas recomendaciones están escritas en un lenguaje no técnico que se adapta específicamente a los administrativos, directivos docentes y docentes.

Se inicia recomendándole a los rectores de los establecimientos educativos que deben desarrollar una comprensión suficiente de la seguridad de la información y sus problemas relacionados: para que puedan juzgar si sus subordinados están actuando de manera competente y completa y, posteriormente, puedan determinar si las recomendaciones y procedimientos propuestos sean adecuados y efectivos.

La seguridad implica más que mantener a los intrusos fuera de los archivos confidenciales. Si bien una organización ciertamente debe estar al tanto de los piratas

[73] The National Forum on Education Statistics (NFES). Protecting the Privacy of Student Education Records. U.S. Department of Education. 1997. p. 41-54.

informáticos del sistema, debe lidiar con más regularidad con amenazas como discos duros dañados, café derramado u otro percance físico que pueda afectar la información.

Dentro de las recomendaciones iniciales para las directivas de una Institución educativa oficial de educación básica y media, es el de mantener un fuerte apoyo externo capacitado, asignar o contratar personal capacitado quien debe ser específicamente responsable de las actividades de seguridad con el tiempo necesario para las pruebas, el monitoreo y otras actividades diseñadas para proporcionar retroalimentación sobre el sistema informático. Igualmente, que los empleados deben recibir formación mediante programas de formación bien concebidos.

De acuerdo con el NFES[74] el primer punto de partida es el responder las siguientes preguntas:

- ¿Están los principales responsables de la toma de decisiones conscientes de que toda la información que es esencial para la prestación de servicios educativos debe mantenerse de manera segura?
- ¿El personal ha considerado las implicaciones de las leyes y regulaciones municipales, departamentales y nacionales que requieren que ciertos tipos de información educativa estén protegidos de la divulgación indebida?
- ¿Se ha convertido la seguridad de la información en una prioridad en la Institución educativa, como lo demuestra el compromiso del rector de leer estas recomendaciones y consultar estas pautas al planificar la seguridad del sistema de información de la Institución?
- ¿Se ha designado a un solo miembro del personal capacitado para administrar la operación de seguridad de la Institución?
- ¿La persona de seguridad designada tiene la autoridad adecuada y el tiempo necesario para realizar el trabajo correctamente?

[74] The National Forum on Education Statistics (NFES). Protecting the Privacy of Student Education Records. U.S. Department of Education. 1997.

- ¿Están los responsables de la toma de decisiones preparados para invertir los recursos necesarios en la formación de seguridad del personal?
- ¿Se espera que todos los empleados participen en iniciativas de seguridad en todo momento según corresponda?

Posterior a esta encuesta, se requiere que la Institución educativa inicie la primera fase con una evaluación de riesgos. En pocas palabras, la evaluación de riesgos implica identificar:

- Activos que posee la Institución educativa.
- Amenazas potenciales a esos activos.
- Puntos en la Institución educativa donde puede tener vulnerabilidades a esas amenazas.
- Probabilidades de amenazas que golpean una vulnerabilidad organizacional
- Estimaciones de costos de pérdidas en caso de que se materialice una amenaza potencial.

Pareciera algo complicado, pero no lo es, la evaluación de riesgos es un proceso sencillo y un paso muy necesario en la toma de decisiones. Al evaluar el riesgo**,** está determinando sus necesidades para no gastar recursos valiosos en salvaguardas innecesarias y, al mismo tiempo, no quedar expuesto a pérdidas desprotegidas. Ignorar el riesgo no es una estrategia aceptable. Los riesgos están en todas partes. Si se elige no realizar una evaluación de riesgos y, en cambio, simplemente se elige ignorar sus riesgos, seguirán existiendo de todos modos, simplemente no estará preparado para ellos.

El proceso de evaluación de riesgos debe ser iniciado y dirigido por los rectores de las Instituciones educativas. Pero, aunque lo inicia el rector, se requiere la retroalimentación de todas las dependencias y cargos. Entre más personas participen en el proceso de evaluación del riesgo, mejor serán los resultados. Se debe ser inclusivo, exhaustivo y realista al documentar los activos. A continuación, se proponen 8 pasos a seguir para la

construcción del proceso de evaluación de riesgos de la Información para las Instituciones educativas oficiales de educación básica y media del país:

Paso 1 - Identificar información sensible: el objetivo aquí es hacer una distinción entre información general y la información que maneja los datos personales de estudiantes, administrativos y docentes.

Paso 2 - Estimar el valor de los componentes del sistema: En este paso se busca identificar todos los sistemas que manejan en los distintos equipos y asignarle un valor monetario. Ejemplo de ellos sistemas operativos, antivirus, *software* de aplicación, calificación de notas, etc.

Paso 3 - Identificar las amenazas: ¿Qué actores, acciones o eventos amenazan los sistemas? En este paso se debe considerar los siguientes tipos de amenazas:

- Natural (por ejemplo, fuego, inundación, rayos y humedad)
- Hecho por el hombre no intencional (por ejemplo, negligencia y accidentes)
- Hecho por el hombre intencional (p. Ej., Piratas informáticos y virus)

Paso 4 - Identificar las vulnerabilidades: ¿Dónde es susceptible el sistema? Considerar las vulnerabilidades a las amenazas naturales y las amenazas provocadas por el hombre; tanto intencionales como no intencionales, como se identificó en el Paso 3. Ejemplo:

- Problemas físicos (por ejemplo, acceso a la habitación, construcción de edificios y clima)
- Problemas relacionados con el hardware y el software (p. Ej., Equipos, programas y compatibilidad)
- Responsabilidades de los medios (por ejemplo, discos, cintas, discos duros y copias impresas)
- Comunicaciones (p. Ej., Puntos de acceso y cifrado)
- Problemas humanos (p. Ej., Comportamiento del personal y de la oficina)

Paso 5 - Estimar la probabilidad de que una amenaza potencial se convierta en una amenaza real: ¿Cuál es la probabilidad de que una amenaza se vuelva una vulnerabilidad? Por ejemplo, para una institución ubicada cerca de un río, los terremotos y las inundaciones son amenazas que están dentro de las posibilidades, pero la lógica dirá que el sitio probablemente sea mucho más susceptible a las inundaciones. Usando historiales de inundaciones, se puede estimar la probabilidad de la próxima inundación. De manera similar, al investigar los datos de terremotos, también se puede estimar la probabilidad de terremotos.

Paso 6 - Identificar las acciones contra las amenazas y vulnerabilidades detectadas: Este paso es paralelo a los pasos 3 y 4 en el sentido de que su propósito es generar una lista exhaustiva de ideas, esta vez posibles soluciones a las preocupaciones causadas por las amenazas y vulnerabilidades identificadas. Al considerar las opciones, asegurarse de tener en cuenta que muchas amenazas y vulnerabilidades se pueden abordar con más de una contramedida. Un ladrón potencial, por ejemplo, podría verse frustrado por mejores cerraduras, cámaras de video y otra vigilancia electrónica, o incluso celadores capacitados. Los aspectos a tener en cuenta al realizar una lluvia de ideas sobre posibles contramedidas incluyen:

- Equipo y procedimientos de seguridad física: ubicación, especificaciones de construcción requeridas y regulaciones que rigen el acceso a las oficinas y el uso de alimentos y bebidas.
- Prácticas de seguridad de la información: regulaciones de almacenamiento y uso, como etiquetado y protección de archivos contra escritura.
- Técnicas de seguridad de *software*: problemas de compra y programación, como infracciones de derechos de autor y documentación adecuada.
- Controles de acceso de usuario: problemas de acceso a datos y al sistema, incluido el inicio de sesión y la protección con contraseña.
- Iniciativas de seguridad de redes: problemas de conectividad como *firewalls* y estrategias de cifrado.

Paso 7 - Estimar los costos de implementar las contramedidas: Este paso implica determinar los costos asociados con las contramedidas identificadas en el Paso 6. Recordar que la gran mayoría de los costos son dobles: iniciales y continuos. Asegúrese de considerar todos los siguientes factores:

- Dinero y tiempo para investigación, desarrollo, adquisición, instalación y mantenimiento de funciones de seguridad.
- Tiempo de formación del personal: los costos reales y absolutamente necesarios.
- La productividad alterada (por ejemplo, hacer que cada empleado pase un minuto usando un escáner de virus tres veces al día puede equivaler a solo tres minutos de tiempo de trabajo por día, pero cuando se calcula para toda la Institución y se suma a una serie de otras posibles actividades de seguridad, como costos aparentemente insignificantes pueden sumar).
- Las contramedidas ya están disponibles para la organización que pueden requerir una menor inversión para implementarlas (por ejemplo, si la oficina de secretaría académica usa actualmente ciertos procedimientos de seguridad, puede haber menos costos de capacitación porque ya tiene un núcleo de personas que pueden compartir su experiencia).

Paso 8 - Seleccionar las contramedidas adecuadas para la implementación: este paso, finalmente es el momento de decidir qué contramedidas tienen más sentido implementar. Recordar que probablemente habrá más de una contramedida que pueda proteger los sistemas o los datos de cualquier amenaza o vulnerabilidad dada. Se debe determinar qué estrategia tiene más sentido desde el punto de vista del costo / beneficio. Esto se puede lograr comparando sus costos estimados de pérdidas potenciales durante un período de tiempo determinado (Pasos 2-5) con los costos de seguridad reales en los que se incurriría al evitar dicha pérdida durante el mismo período de tiempo (Paso 7).

Una vez que se determine las necesidades y prioridades a través de los ocho pasos anteriores, se podrá tomar decisiones de seguridad basadas en información concreta.

No solo los administrativos o docentes son responsables de la seguridad de la información confidencial, sino también la propia institución educativa. Por lo tanto, corresponde a las directivas, garantizar que se desarrolle y se ponga en práctica una política de seguridad adecuada y eficaz en toda la Institución.

La política de seguridad de la información debe basarse en los resultados de la evaluación de riesgos. Los hallazgos de una evaluación de riesgos brindan a los responsables de la seguridad de la información grandes ventajas frente a las amenazas. Se recomienda tener en cuenta lo siguiente:

- Identificar información sensible y sistemas críticos.
- Incorporar la legislación colombiana sobre seguridad de la información y delitos informáticos, así como estándares éticos relevantes.
- Definir metas y objetivos de seguridad de la información.
- Establecer un rumbo para lograr esas metas y objetivos.
- Asegurar que los mecanismos necesarios para lograr las metas y objetivos estén en su lugar.

El increíble ritmo de las innovaciones tecnológicas requiere que todas las políticas de seguridad se revisen con frecuencia. En términos generales, cada nuevo cambio tecnológico tiene el potencial de requerir un cambio de política correspondiente, por lo que es una buena regla revisar todas las políticas de la Institución anualmente como mínimo.

La seguridad eficaz de los sistemas de información depende de la creación de un entorno de trabajo y una estructura organizativa donde las directivas comprendan y apoyen plenamente los esfuerzos de seguridad, y se anime a los usuarios a actuar con cautela. El gerente de seguridad lidera este esfuerzo.

Un gerente de seguridad debe:

- Comunicar al personal que proteger el sistema no solo redunda en el interés de la Institución, sino también en el mejor interés de los usuarios.

- Aumentar la conciencia del personal sobre los problemas de seguridad.
- Proporcionar al personal una formación adecuada en materia de seguridad.
- Supervisar la actividad de los usuarios para evaluar la implementación de la seguridad.

La seguridad informática tradicional con frecuencia depende en gran medida de proteger los sistemas de ataques y minimizar la probabilidad de fallas de software y equipos, pero generalmente se presta poca atención a cómo manejar un ataque o falla una vez que realmente ocurre. El resultado es que cuando ocurre un problema, muchas decisiones se toman apresuradamente. A menudo, tales decisiones reflejan esta falta de previsión y no contribuyen a rastrear la fuente del incidente, recolectar evidencia para ser utilizada en los esfuerzos de enjuiciamiento, proteger la información valiosa contenida en el sistema o prepararse para la recuperación del sistema.

Una buena política de seguridad, siempre que la seguridad se vea amenazada, ya sea una falla del disco, un ataque de intrusos externos o un desastre natural, es haber planificado con anticipación posibles eventos adversos. Podría suceder en un año, un mes o más antes. La planificación para emergencias de antemano va más allá de una "buena política".

La seguridad es más que mantener a los piratas informáticos y otras personas infractoras de las normas y leyes informáticas, fuera del acceso a los equipos de la institución. Implica una serie de prácticas internas que sirven para proteger la información en caso de falla del sistema o del disco. Algunas de las principales actividades que realizan los gerentes de seguridad en el día a día incluyen la administración de mecanismos de respaldo y protección contra virus, mantenerse al tanto de las actualizaciones de *software*, administrar las cuentas de los usuarios y monitorear la actividad del sistema.

Se enfatiza bastante en la necesidad de una buena estrategia de respaldo. Las copias de seguridad del sistema no solo protegen a la Institución en caso de fallas de hardware o eliminaciones accidentales, sino que también protegen al personal contra cambios

accidentales o no autorizados realizados en el contenido del archivo. Los archivos de respaldo deben crearse a intervalos apropiados y ellos mismos deben estar bien protegidos contra daños y destrucción.

De acuerdo ESET[75] a través de su página web indica que según la ITIL (*Information Technology Infrastructure Library*), existen tres tipos de estrategias de respaldo que se deben implementar:

- Una copia de seguridad completa: copia de seguridad de todo el disco duro. La ventaja de esta estrategia es la integridad; se obtiene una copia exacta de todo el contenido de su disco duro.
- Una copia de seguridad parcial: solo realiza una copia de seguridad de los directorios o archivos seleccionados.
- Una copia de seguridad incremental: solo hace una copia de seguridad de los archivos que se han modificado desde la última copia de seguridad. Significa usar un *software* de respaldo para escanear los archivos y ver si se han modificado desde el último ciclo de respaldo. Si es así, el archivo se guarda; de lo contrario, se mantiene la copia de seguridad anterior.

Cualquier máquina que esté conectada a una red o que interactúe con otras a través de pendrives o una red LAN con internet, es vulnerable a programas fraudulentos: virus informáticos, gusanos, caballos de Troya y similares. Es deber del gerente de seguridad desarrollar y monitorear procedimientos para prevenir que virus y otros programas fraudulentos se infiltren en el sistema. Como regla general, ningún dispositivo USB externo al sistema debe usarse en una máquina del sistema sin haber sido escaneado primero por un programa antivirus actualizado.

No hace falta decir que los sistemas informáticos tienen errores. Incluso los sistemas operativos, que dependen en gran parte para la protección de la información, tienen

[75] WELIVESECURITY- ESET. Backup en empresas: enfoque normativo de los respaldos de información. [Recuperado 18 abril de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2015/04/09/backup-empresas-enfoque-normativo/

errores. Debido a esto, los editores de *software* publican actualizaciones con frecuencia. A menudo, estas actualizaciones son, de hecho, tapones de agujeros en la seguridad del *software* que se han descubierto. Es importante que siempre que se identifiquen estos errores, el administrador del sistema tome todas las medidas posibles para remediarlos lo antes posible a fin de minimizar la exposición.

Como se indica en las recomendaciones anteriores, una sola persona debe tener la responsabilidad principal de un sistema de información. Para que esta persona, el gerente de seguridad o el administrador de sistemas, pueda supervisar el sistema de manera efectiva, él o ella necesitan tener acceso a todos los componentes del sistema y acceso a los archivos que comúnmente se conoce como "privilegios de administrador del sistema". Por lo general, se considera una buena práctica compartir los privilegios de acceso del administrador del sistema con alguien que no sea el administrador del sistema, aunque solo sea para tener acceso de emergencia al sistema en caso de que el administrador no esté disponible. Pero, se requiere una responsabilidad total, y debe limitarse al menor número de personal que sea necesario para mantener el sistema seguro.

Los usuarios que no sean el administrador del sistema deben tener acceso al sistema basándose únicamente en sus necesidades laborales. Restringir el acceso de los usuarios minimiza las oportunidades de accidentes y otras acciones posiblemente inapropiadas. Mediante el uso de cuentas de usuario, cada usuario autorizado se identifica antes de acceder al sistema, y cualquier acción que realice ese usuario se clasifica como tal. Los usuarios deben tener acceso solo a los archivos y sistemas que necesitan para hacer su trabajo, y nada más.

De acuerdo a la Ley 594 de 2000, Ley General de Archivos[76], la seguridad física se refiere a la protección de los sitios y equipos informáticos, de robo, vandalismo, desastres naturales, catástrofes provocadas por el hombre y daños accidentales. Requiere una

[76] COLOMBIA. ARCHIVO GENERAL DE LA NACION. Ley 594; 14, 07, 2000; Ley General de Archivo.

construcción sólida, preparación adecuada para emergencias, fuentes de alimentación confiables, control climático adecuado y protección adecuada contra intrusos.

La seguridad física requiere que los sitios de construcción estén protegidos de una manera que minimice el riesgo de robo y destrucción de recursos. La planta física debe estar asegurada satisfactoriamente para evitar que las personas que no están autorizadas a ingresar al sitio y utilizar equipos lo hagan.

Si bien la confidencialidad de la información a veces es obligatoria por ley, el sentido común y las buenas prácticas sugieren que incluso la información no confidencial en un sistema debe protegerse también, no necesariamente de la divulgación no autorizada, sino de modificaciones no autorizadas e influencias inaceptables en su accesibilidad.

De acuerdo al Manual de Políticas de Seguridad de la Información del gobierno Nacional[77] Las siguientes contramedidas abordan los problemas de seguridad de la información que podrían afectar las Instituciones educativas. Estas estrategias se recomiendan cuando la evaluación de riesgos identifica o confirma la necesidad de contrarrestar posibles brechas en la seguridad de la información del sistema.

Transmitir información de forma segura (incluido el correo electrónico):

- Utilizar el correo electrónico solo para las comunicaciones habituales en la oficina: nunca enviar información confidencial como correo electrónico. Si es absolutamente necesario utilizar el correo electrónico, se debe cifrar el archivo y enviarlo como un archivo adjunto en lugar de en el texto del mensaje de correo electrónico.
- Cifrar todo antes de que salga de la oficina de trabajo: incluso la contraseña debe estar cifrada antes de dejar la estación de trabajo en el camino hacia el servidor de red; de lo contrario, podría ser interceptada mientras viaja por las conexiones de red.

[77] Presidencia de la Republica. Manual de Políticas de Seguridad de la Información. Bogotá (octubre de 2021).

- Proteger físicamente los dispositivos y claves de cifrado de datos: guardarlos lejos de la computadora recordando donde los deja. Utilizar los mismos principios de protección de sentido común que se debe con el PIN de las tarjetas bancarias.
- Informar al personal que todos los mensajes enviados con o sobre las computadoras de la Institución pertenecen a la Institución: esta es una buena forma de decir que todo en la oficina está sujeto a monitoreo.
- Verificar la autenticidad del receptor antes de enviar información a cualquier lugar: asegurarse de que los usuarios en el extremo receptor sean quienes representan a sí mismos verificando:
- Mantener la seguridad al enviar y recibir información: cuando se envíe información confidencial por correo, mensajero o mensajería, exigir que todos los proveedores de servicios externos que cumplan o superen los requisitos de seguridad.

Almacenar la información correctamente:

- Aplicar los principios de almacenamiento recomendados tanto a los archivos originales como a los de respaldo: los archivos de respaldo requieren los mismos niveles de seguridad que los archivos originales.
- Etiquetar claramente los discos, cintas, contenedores, gabinetes y otros dispositivos de almacenamiento: el contenido y la sensibilidad deben estar marcados de manera apropiada para que haya menos posibilidades de errores de identidad.
- Separar la información confidencial: nunca almacenar información confidencial de forma que se mezcle con otros datos en discos u otros medios de almacenamiento de datos extraíbles.
- Restringir el manejo de información sensible al personal autorizado: La información, los programas y otros datos deben ingresarse o exportarse desde el sistema solo a través de canales aceptables y por personal con la autorización adecuada.

Eliminar la información de manera oportuna y completa:

- Establecer una política específica de retención y eliminación de información según lo determinen las necesidades de la Institución y los requisitos legales: Todos los datos tienen un ciclo de vida finito.
- Marcar los archivos para indicar el contenido, su ciclo de vida esperado y las fechas de destrucción adecuadas.
- No limitarse a borrar o reformatear los medios, sino sobrescribirlos con código binario aleatorio. Los usuarios sofisticados aún pueden acceder a la información incluso después de que se haya borrado o reformateado, mientras que la sobreescritura reemplaza la información descartada.

Considerar la desmagnetización como una opción de borrado.

- Quemar, triturar o destruir físicamente los medios de almacenamiento (por ejemplo, papel) que no se puedan sobrescribir o desmagnetizar de manera eficaz.
- Limpiar pendrives, discos y discos duros que hayan almacenado datos confidenciales antes de reasignarlos: nunca compartir discos que hayan almacenado datos confidenciales a menos que se hayan limpiado adecuadamente. También recordar limpiar los medios de almacenamiento magnéticos antes de devolverlos a un proveedor para su intercambio o eliminación.

Implementar un programa en el que cada usuario acceda al sistema a través de una cuenta individual:

- Limitar el acceso de los usuarios a solo aquellos archivos que necesitan para hacer su trabajo: proporcionar un acceso que no es necesario contribuye en gran medida al riesgo sin el correspondiente aumento en el beneficio.
- Evite las cuentas compartidas: la actividad individual no se puede diferenciar a menos que haya cuentas individuales.

- Proteger la lista de nombres de cuentas de usuario: debido a su importancia para la seguridad del sistema, la lista de cuentas de usuario debe considerarse confidencial y nunca debe hacerse pública.
- Supervisar las actividades de la cuenta: mantener un registro de todo el uso del sistema.
- Terminar las cuentas inactivas después de un período predeterminado de inactividad (por ejemplo, 30 días): Los usuarios legítimos siempre puede volver a aplicar y restablecer sus cuentas.

Dado que las contraseñas son el método más común de autenticación de usuarios, merecen una atención especial.

Selección de contraseña:

- Exigir que las contraseñas tengan al menos seis caracteres (aunque es preferible que tengan entre ocho y diez).
- Prohibir el uso de contraseñas que sean palabras, nombres, fechas u otros formatos comúnmente esperados.
- Prohibir el uso de contraseñas que reflejen o identifiquen al propietario de la cuenta (por ejemplo, sin fechas de nacimiento, iniciales o nombres de mascotas).
- Exigir una combinación de caracteres (es decir, letras / números y mayúsculas / minúsculas si el sistema distingue entre mayúsculas y minúsculas).

Proteger la red de personal ajeno a la Institución:

- Implementar las recomendaciones de seguridad aplicables como se planteó en los puntos anteriores: La defensa sólida contra las amenazas externas de Internet incluye la implementación adecuada de medidas de seguridad relativamente sencillas como *software* de cifrado, escáneres de virus, regulaciones de acceso remoto y contraseñas.
- Aislar la red mediante el uso de un *firewall*: la instalación de un *firewall* permite a la Institución decidir qué tipos de mensajes deben permitirse en el sistema desde

fuentes externas (por ejemplo, "nada con codificación de virus identificable" y "nada con estructuras de codificación de descifrado").

- Ubicar el equipo y la información destinados a usuarios externos fuera del *firewall*: si el servidor web de una Institución está destinado a proporcionar información y servicios al público, no debe ubicarse en el lado privado del *firewall*. Tampoco debería poder acceder a información confidencial que reside dentro del firewall. De esta forma, si el servidor web público llegara a verse comprometido, la información confidencial seguirá estando protegida.

Proteger las transmisiones enviadas por Internet:

- Utilizar los servidores *Secure Sockets Layer (SSL)* para proteger las transacciones financieras y de información realizadas con un navegador web: en una sesión web segura, el navegador web genera una clave de cifrado aleatoria y la envía al host del sitio web para que coincida con su clave de cifrado pública. El navegador y el sitio web luego cifran y descifran todas las transmisiones.
- Autenticar mensajes mediante el uso de firmas digitales: una firma digital equivale a una "huella digital" de un mensaje. Representa el mensaje de tal manera que, si el mensaje se modificara de alguna manera, la "huella digital" lo reflejaría, lo que haría posible la detección de falsificaciones. Lo contrario, por supuesto, es que, si la "huella digital" no cambia durante la transmisión, puede estar seguro de que el mensaje no se modificó.
- Autenticar los "receptores" de mensajes mediante el uso de certificados digitales: al requerir un agente de autenticación o un certificado digital, obliga a la persona en el otro extremo de la transmisión a probar su identidad.
- Cifrar todos los mensajes enviados a través de Internet: a medida que se envían más y más mensajes a través de redes cada vez más grandes, la información se vuelve cada vez más vulnerable a los ataques. El cifrado se ha convertido en una herramienta líder para combatir esta vulnerabilidad. Al igual que otras contramedidas, puede ser muy eficaz si se usa de manera adecuada y regular.

En sí el seguir los estándares internacionales, guías y manuales de buenas prácticas es la mejor forma de mantener la confidencialidad, integralidad y disponibilidad de la información que se maneja en las Instituciones educativas oficiales de educación básica y media del país y en general en cualquier organización.

6 CONCLUSIONES

En Colombia es evidente que últimamente se vienen diseñando nuevas recomendaciones, guías, normatividad y en general estrategias para garantizar la seguridad de la información que se maneja en las entidades del Estado, en las que se incluyen las Instituciones Educativas oficiales de educación básica y media del país; pero en la mayoría de estos establecimientos no se observa la aplicación de estas recomendaciones o normatividad.

Se pudo observar que los estudios realizados a la seguridad de la información de establecimientos educativos oficiales de educación básica y media no solo de Colombia, sino de otros países, muestran los grandes riesgos que pueden tener los establecimientos educativos en el tema de la seguridad de la información; ya que no cuentan con sistemas de seguridad que garanticen la integralidad, disponibilidad y privacidad de la información sensible que manejan, sin embargo, casi nulos los estudios sobre la seguridad de la información en establecimientos educativos oficiales de educación básica y media del país.

En cuanto al panorama actual de la seguridad de la información en los establecimientos educativos oficiales de educación básica secundaria y media de Colombia se evidencia que está en riesgo constante, más ahora donde el uso de redes sociales se ha incrementado enormemente en los miembros de las comunidades educativas. Los establecimientos educativos no están poniendo en práctica las indicaciones redactadas en los diferentes documentos que invitan a la puesta en marcha de guías y manuales de buenas prácticas para garantizar la seguridad de la información.

Las recomendaciones dadas en la presente monografía a las instituciones educativas oficiales de educación básica y media del país, se encuentran basadas en las recomendaciones dadas por *The National Forum on Education Statistics (NFES)* de los Estados Unidos. Las buenas prácticas dadas por el ITIL, ISO27001, COBIT y NIST, permitirán en gran porcentaje proteger la información sensible que manejan dichos

establecimientos de cada uno de los miembros de comunidad educativa como lo son estudiantes, egresados, padres de familia, docentes, directivos docentes y administrativos en general.

7 RECOMENDACIONES

Se hace indispensable que todos los miembros de las comunidades educativas tomen conciencia de los riesgos que se corren con el manejo de información a través de los sistemas informáticos, redes LAN y redes sociales y acaten las recomendaciones plasmadas en el presente documento, diseñadas de acuerdo con el panorama descrito para garantizar la seguridad de la información en las Instituciones educativas oficiales de educación básica secundaria y media de Colombia, las cuales se encuentran de una forma clara y concisa para que fueran del entender de todos los lectores de la monografía.

Se requiere que los establecimientos educativos oficiales del país asignen dentro de sus presupuestos, rubros destinados a garantizar los mecanismos que se requieren implementar en su interior, para mejorar la seguridad de la información que manejan y puedan capacitar a todo el personal administrativo, docente y estudiantes, asignando o contratando una persona encargada del sistema de gestión de la seguridad de la información y solo desempeñe dichas funciones.

Dado que muchos estudiantes y educadores se están alejando a largo plazo el próximo año escolar, es aún más importante para ellos comprender las implicaciones de seguridad cibernética de tener un aula virtual. Por ellos se recomienda que se fortalezcan también los sistemas informáticos de los establecimientos y los puntos finales utilizados por docentes y estudiantes, con el ánimo de prevenir tácticas como el phishing y la ingeniería social. Además, las directivas deben enviar recordatorios mensuales al personal sobre varios temas y medidas de seguridad para ayudarlos a mantenerse alerta e informados.

Es imperativo que los establecimientos educativos identifiquen las amenazas y las mitiguen rápidamente, además de ejecutar evaluaciones de vulnerabilidad en sistemas públicos y dispositivos internos en un cronograma mensual para mantener la misión principal de enseñanza y aprendizaje

BIBLIOGRAFÍA

27001ACADEMY - How to integrate ISO 27001, COBIT and NIST, [En línea]. [Consultado 27 noviembre de 2021]. Disponible en: https://info.advisera.com/27001academy/free-download/how-to-integrate-iso-27001-cobit-and-nist

ACSI. Revista SISTEMAS No. 159 (2021). Resiliencia Digital. La nueva frontera para las organizaciones del siglo XXI. DOI: 10.29236/sistemas

AGUIRRE, Jhon. El 67% de los colegios en Latinoamérica han sido víctimas de ataques cibernéticos. *La FM*. [En línea] 28 Mayo 2018. [Consultado 27 diciembre de 2021]. Disponible en: https://www.lafm.com.co/tecnologia/el-67-de-los-colegios-en-latinoamerica-han-sido-victimas-de-ataques-ciberneticos

BENAVIDES S. Alejandra, BLANDÓN J. Carlos. Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. Scientia et Technica Año XXII, Vol. 23, No. 01, marzo de 2018. Universidad Tecnológica de Pereira. ISSN 0122-1701

BERMUDEZ SANMIGUEL, Edgar y TAFUR TORRES, Diego. Sistema de Seguridad Informático para el Colegio Cooperativo Espíritu Santo De Girardot. Trabajo de grado realizado para optar al título de tecnólogo en redes de computadores y seguridad informática. Girardot: Corporación Universitaria Minuto de Dios. Facultad de Ingeniería de Sistemas, 2011. 33p.

BERTOLÍN, J. A. Seguridad de la información. Redes, informática y sistemas de información, Madrid. Editorial Paraninfo. 2008. 592p

BONILLA, Francisco. La adicción a las nuevas tecnologías en jóvenes y adolescentes. *BLOG: Psicología y salud*. [En línea]. 2022, [consultado 15 octubre de 2022]. Disponible en: https://www.quironsalud.es/blogs/es/psicologia-salud/adiccion-nuevas-tecnologias-jovenes-adolescentes

CCIT. Informe SAFE - Tendencias del Cibercrimen 2021 – 2022. [En línea]. [Consultado 15 diciembre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Ley 594; 14, 07, 2000; Ley General de Archivo. [En línea]. [27 diciembre de 2021] disponible en: https://normativa.archivogeneral.gov.co/ley-594-de-2000/?pdf=41

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Seguridad en la Nube, Guía 12, [En línea]. [27 diciembre de 2021] disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Plan de Seguridad y Privacidad de la Información del MINTIC 2020, [En línea]. [Consultada 10 diciembre de 2021] disponible en: https://www.mintic.gov.co/portal/715/articles-135830_plan_seguridad_privacidad_informacion_2020_u20201228.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, [En línea]. [Consultada 10 diciembre de 2021] disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Controles de Seguridad y Privacidad de la Información. Guía 8, [En línea]. [27 diciembre de 2021] disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía de indicadores de gestión para la seguridad de la información. Guía 9, [En línea]. [27 diciembre de 2021] disponible en:

https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Resolución 500 de 2021. [12 diciembre de 2021] disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. MinTIC expide la resolución que establece los lineamientos y estándares para la estrategia de seguridad digital. [12 diciembre de 2021] disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/162626:MinTIC-expide-la-resolucion-que-establece-los-lineamientos-y-estandares-para-la-estrategia-de-seguridad-digital

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Decreto 1377 del 27 de junio de 2013. [En línea]. [10 diciembre de 2021] disponible en: https://www.mintic.gov.co/arquitecturati/630/articles-9011_documento.pdf

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1266 de 2008. [En línea]. [12 diciembre de 2021] disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=34488

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 del 5 de enero de 2009. [En línea]. [10 diciembre de 2021] disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581 del 17 de octubre de 2012. [En línea]. [10 diciembre de 2021] disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CONPES 3995. POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL. Bogotá D.C. 2021 [Recuperado 12 noviembre de 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política Nacional de Seguridad Digital. CONPES 3854, [En línea]. [10 diciembre de 2021] disponible en: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política Nacional de Confianza y Seguridad Digital. CONPES 3995, Bogotá D.C. 2021.

CONSTITUCIÓN POLÍTICA DE COLOMBIA. Art. 42. 7 de julio de 1991 (Colombia).

DANE. Boletín Técnico Educación Formal (EDUC). Bogotá D.C. 2021 [Recuperado 12 abril de 2022]. Disponible en: https://www.dane.gov.co/files/investigaciones/boletines/educacion/bol_EDUC_20.pdf

DE HAES Steven, VAN GREMBERGEN Wim y DEBRECENY Roger S. COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. En: Journal of Information Systems Vol. 27 No 1. (Mar-May.2013); p. 307-324. DOI: 10.2308/isys-50422.

DIGIWERE - ¿A qué amenazas cibernéticas se enfrentará el sector educativo con la transformación digital?, [En línea]. [27 diciembre de 2021] disponible en: http://www.digiware.net/?q=es/blog/a-que-amenazas-ciberneticas-se-enfrentara-el-sector-educativo-con-la-transformacion-digital

DIGIWERE - Ciberseguridad en la educación: conozca los nuevos retos cibernéticos del sector educativo, [En línea]. [10 marzo de 2022] disponible en: https://www.digiware.net/post/ciberseguridad-en-la-educaci%C3%B3n-conozca-los-nuevos-retos-cibern%C3%A9ticos-del-sector-educativo

DINERO. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [En línea]. [Consultado 10 enero de 2021]. Disponible en:

https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

EL TIEMPO. Universidad El Bosque sufre ataque informático [En línea]. [Consultado 11 marzo de 2022]. Disponible en: https://www.eltiempo.com/vida/educacion/universidad-el-bosque-sufre-ataque-informatico-599303

ELCOLOMBIANO.COM. Cibersecuestradores: ahora le cayeron a la Javeriana. [En línea]. [Consultado 11 marzo de 2022]. Disponible en: https://www.elcolombiano.com/colombia/ataques-contra-javeriana-y-dane-alertan-de-mas-ciberataques-KB16069751

EZQUIVEL TRIANA, Ricardo. Modelos de seguridad. Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacional, Bogotá. 2014.

FRASER, John. El sector educativo, un blanco perfecto para ciberataques. *BLOG: EL RIESGO EN CONTEXTO*. [En línea]. 2018, [consultado 15 octubre de 2021]. Disponible en: https://www.marsh.com/co/insights/risk-in-context/sector-educativo-ciberataques.html

HERZOG Pete. OSSTMM 3. The Open Source Security Testing Methodology [Manual]. Isecom.org. USA. 2010. 211p

ISOTOOLS. Sistemas de Gestión de Riesgos y Seguridad. [En línea]. [Consultado 27 noviembre de 2021]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/#

KASPERSKY. Ciberamenaza Mapa en Tiempo Real. [Sitio web]. Rusia. [Consultado marzo 10 de 2022]. Disponible en: https://cybermap.kaspersky.com/es

LA REPÚBLICA. Colombia fue uno de los países con más ataques cibernéticos el año pasado. [En línea]. [Consultado 27 diciembre de 2021]. Disponible en:

https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

LARA Elva G, CORELLA Flavio A. Comparación de modelos tradicionales de seguridad de la información para centros de educación. Revista Tierra Infinita N° 4. Jun-Ago.2018.

LEIVA, Eduardo. 2015. Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingeniería de Software, 3(4): 161-176, ISSN 2314-2642.

PARRA BARZOLA Liliana M.; YÁNEZ CEDEÑO Erick S. Análisis de vulnerabilidades en la Infraestructura tecnológica de una empresa, utilizando herramientas de test de Intrusión. Trabajo de investigación .Guayaquil: Universidad de Guayaquil. Facultad de Matemáticas y Física, 2017.

PMOGuide. Comparativa – PMBOK, CMMI, COBIT, ITIL, [Sitio web]. Mexico. [Consultado 12 noviembre de 2021]. Disponible en: https://ipmoguide.com/comparativa-pmbok-cmmi-cobit-itil/

POLICÍA NACIONAL, CCIT. Informe de las Tendencias del cibercrimen en Colombia (2019-2020). [En línea]. [Consultado 15 diciembre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

PORTAFOLIO. Las entidades que reportan mayores suplantaciones por cibercriminales. [En línea]. [Consultado 15 diciembre de 2021]. Disponible en: https://www.portafolio.co/innovacion/entidades-colombianas-que-reportan-mayor-suplantaciones-por-cibercriminales-559465

PRESIDENCIA DE LA REPÚBLICA. Decreto 1081 del 26 de mayo de 2013. [En línea]. [12 diciembre de 2021] disponible en: http://es.presidencia.gov.co/normativa/normativa/Decreto-1081-2015.pdf

PRESIDENCIA DE LA REPUBLICA. Manual de Políticas de Seguridad de la Información. Bogotá (octubre de 2021).

SIGEP. Sistema de Información y Gestión del Empleo Público. [Plataforma web] Disponible en: https://www.funcionpublica.gov.co/web/sigep

SIMAT. Sistema de matrículas. [Plataforma web] Disponible en: https://www.sistemamatriculas.gov.co/

SIMPADE. Sistema de Información para el Monitoreo, la Prevención y el Análisis de la Deserción Escolar. [Plataforma web] Disponible en: https://simpade.mineducacion.gov.co/simpade/

SOLARTE SOLARTE, Francisco, ENRIQUEZ ROSERO, Edgar y BENAVIDES RUANO, Mirian. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnologica Espol – RTE*. 2015, vol. 28, nro. 5.

STONEBURNER, Gary, GOGUEN Alice y FERINGA Alexis. Risk management guide for information technology systems: recommendations of the National Institute of Standards and Technology. [Manual]. *National Institute of Standards and Technology*. USA. 2012.

THE NATIONAL FORUM ON EDUCATION STATISTICS (NFES). Protecting the Privacy of Student Education Records. U.S. Department of Education. 1997. p. 41-54.

UNIVERSIDAD DEL ROSARIO. Colombia no está preparada ante un ciberataque. [En línea]. [consultado 30 diciembre de 2021] disponible en: https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/

UNIVERSIDAD LIBRE. Crecen los ataques de Phishing en Colombia. [En línea]. [05 enero de 2021] disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/424-crecen-los-ataques-de-phishing-en-colombia

UNIVERSIDAD SANTO TOMÁS. Los Ataques Informáticos en el Sector Educativo. [En línea]. [consultado 05 enero de 2021] disponible en: https://auditoriainterna.usta.edu.co/index.php/120-los-ataques-de-hacking-en-el-sector-educativo

VALDEZ ALVARADO, Aldo. OSSTMM 3. *Revista de Información, Tecnología y Sociedad*. [En línea]. 2013, junio No 8. [consultado 15 octubre de 2021] ISSN 1997-4044. Disponible en: http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100013&script=sci_arttext

WELIVESECURITY- ESET. Backup en empresas: enfoque normativo de los respaldos de información. [Recuperado 18 abril de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2015/04/09/backup-empresas-enfoque-normativo/

WORLD ECONOMIC FORUM. Global Cybersecurity Outlook 2022. [Consultado 27 diciembre de 2021]. Disponible en: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf