Análisis de los Componentes de la seguridad informática en las IES desde una Perspectiva de dinámica de sistemas.

Modalidad:

Proyecto de Investigación

Luis Angel Florez Homeara.

CC. 1.095.841.366

UNIDADES TECNOLÓGICAS DE SANTANDER

Facultad de Ciencias Naturales e Ingenierías

Bucaramanga 08-05-2023

Análisis de los Componentes de la seguridad informática en las IES desde una Perspectiva de dinámica de sistemas.

Modalidad:

Proyecto de Investigación

Luis Angel Florez Homeara.
CC. 1.095.841.366

Trabajo de Grado para optar al título de
Tecnólogo en desarrollo de sistemas informáticos

DIRECTOR
Martha Lizette Massey Galvis
Grupo de investigación – GRIIS

UNIDADES TECNOLÓGICAS DE SANTANDER
Facultad de Ciencias Naturales e Ingenierías
Bucaramanga 08-05-2023

Nota de Aceptación

ACTA #37
FECHA: 26/09/2023

La tesis "Análisis de los Componentes de la seguridad informática en las IES desde una Perspectiva de dinámica de sistemas" fue APROBADA para el programa de Tecnología en Desarrollo de Sistemas Informáticos

LEYDI JOHANA POLO A.

_____

Firma del Evaluador

Lizette Massey Galvis

_____

Firma del Director

DEDICATORIA

Dedico mi trabajo principalmente a mi madre Albis y a mi abuela Fanny, principales fortalezas para seguir adelante, son mi inspiración.

AGRADECIMIENTOS

Expreso mi agradecimiento a la ingeniera de sistemas y directora de mi proyecto Martha Lizette Massey Galvis por brindarme su apoyo para realizar dicho trabajo.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN EJECUTIVO

El presente trabajo de investigación tiene como objetivo analizar los componentes de seguridad informática en las Instituciones de Educación Superior (IES), teniendo en cuenta que, es un tema importante que requiere de políticas de seguridad informática para garantizar la protección de la información. Por otro lado, Las políticas de seguridad informática tienen como objetivo establecer medidas técnicas y de organización necesarias para garantizar la seguridad de la información en las IES. Algunas de las políticas que se pueden implementar son la gestión de riesgos; la cooperación y colaboración; la educación y concienciación; realización de auditorías de seguridad periódicas; la implementación de mecanismos de seguridad activa para proteger los sistemas informáticos; por último, la privacidad de la información y el establecimiento de objetivos alineados a los objetivos de la institución.

Es importante que las políticas de seguridad informática se alineen con los objetivos de las IES, para que de esta forma sea posible garantizar su eficacia. Además, es importante que se realicen auditorías de seguridad periódicas para evaluar la eficacia de las políticas implementadas y realizar mejoras si es necesario. Por otra parte, la seguridad de las IES involucra a múltiples actores, factores y relaciones. La dinámica de sistemas es una herramienta que permite analizar la

seguridad de forma holística, teniendo en cuenta las interacciones entre los diferentes componentes del sistema. Estos modelos se construyen a partir de un conjunto de variables que interactúan entre sí a través de relaciones de causa-efecto.

De esta manera, las variables clave que pueden ser modeladas desde una perspectiva de dinámica de sistemas incluyen a los activos de la organización, ya sean tangibles o no; también los riesgos que, en este caso, son los que pueden dañar o destruir los activos y, por último, las medidas de seguridad que se toman para reducir las vulnerabilidades y las amenazas

La dinámica de sistemas permite analizar la seguridad de forma integral, teniendo en cuenta las interacciones entre los diferentes componentes del sistema. Esto puede ser útil para identificar riesgos potenciales, evaluar el impacto de las medidas de seguridad y desarrollar estrategias de seguridad más efectivas. En conclusión, la dinámica de sistemas en la seguridad informática sirve para modelar la evolución de las amenazas cibernéticas, evaluar el impacto de las medidas de seguridad y desarrollar estrategias de seguridad más efectiva, por lo tanto, es una herramienta útil que aporta una perspectiva integral para la seguridad informática hoy en día.

Palabras clave: Seguridad Informática; Instituciones de Educación Superior; Universidades; Dinámica de sistemas; Sistemas informáticos.

INTRODUCCIÓN

La seguridad informática en las IES es un desafío complejo y en constante evolución. Desde una perspectiva de dinámica de sistemas, podemos abordar este tema como un sistema interconectado, donde múltiples componentes interactúan de manera dinámica para influir en la seguridad general. Esta perspectiva nos permite comprender que la seguridad no es estática, sino que evoluciona con el tiempo y está influenciada por una serie de factores interrelacionados. En esta introducción, exploraremos cómo el análisis de los componentes de la seguridad informática en las IES desde una perspectiva de dinámica de sistemas nos proporciona una visión más completa y efectiva para abordar los desafíos en este ámbito, destacando la importancia de considerar la interconexión, la adaptación continua y la resiliencia en la protección de la información y los recursos en el entorno educativo.

Para el desarrollo del siguiente trabajo, se tuvo como tema referencial la seguridad de la información con la ayuda de un sistema dinámico causal, el cual fue de mucha ayuda para la elaboración de dicho modelo dinámico. La mayor referencia bibliográfica que sirvió como base para la elaboración fue Parada et al., (2018) con su investigación *Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas.* Con esta cita bibliográfica se

obtuvieron las bases de mayor impacto y que ayudaron a desarrollar la investigación.

En el presente trabajo se abordarán los principales componentes de la seguridad informática en las IES desde una perspectiva de dinámica de sistemas. Se discutirán las interacciones entre estos componentes y se mostrará cómo la dinámica de sistemas puede ayudar a las IES a mejorar su seguridad informática.

1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

Desde hace varias décadas se presenta casi que a diario una innovación tecnológica que permite la inclusión de esta en la vida cotidiana de las personas, además de ello, la tecnología ha permitido que diferentes sectores integren sus datos en un solo sistema, es allí, donde la seguridad informática toma relevancia, pues al tener las personas acceso a diferentes medios tecnológicos, se hace importante restringir información personal o privada ya sea de una persona, empresa, universidad, para proteger a los individuos. Es decir, la seguridad informática

> "Trata sobre la protección de información de índole personal, empresarial o gubernamental contenida no solo en la red, sino también en los dispositivos de uso diario como teléfonos celulares, tabletas, computadoras de escritorio, laptop o cualquier dispositivo digital, de amenazas que puedan poner en riesgo la información almacenada o transportada en alguno de los dispositivos antes mencionados" (Gamboa, J. 2020).

No obstante, existen constantes ataques a dicha seguridad informática, “Estos atacantes cibernéticos irrumpen sistemas y redes con fines maliciosos, tales como propagar malware, robar datos, o espiar sistemas. Su motivación destructiva es casi siempre económica o activista” (Gutiérrez, 2022).

Estos ataques, se empezaron a presentar con mayor frecuencia y en la actualidad, a pesar de, los grandes avances en materia tecnológica, aún se siguen presentando problemáticas en la ciberseguridad de diferentes organizaciones a nivel mundial, tanto así que, las cifras cada día van en aumento, destacando que, “El delito cibernético aumentó en un 600 % como resultado de la pandemia de COVID 19, desde robo y malversación hasta piratería y corrupción de datos.” (Gutiérrez, 2022).

En lo que concierne a Colombia, en el año 2022, según las denuncias presentadas, los ciberataques se presentaron con mayor frecuencia, donde se resalta que “el acceso abusivo al sistema informático que presentó 6.407 casos, es decir 46% más que en el mismo periodo del año anterior, y el hurto por medios informáticos que mostró un alza del 15% con 11.078 casos denunciados.” (Portafolio, 2022). Adicional a ello, según el informe de amenazas globales de Fortinet, Colombia “recibió 20.000 millones de intentos de ciberataques en 2022, lo cual representa un crecimiento del 80 por ciento frente a 2021.” (Lesmes, 2023).

Sin embargo, a raíz de esta creciente de ciberataques desde hace varios años se han implementado leyes y políticas en cada país para la protección de datos de la población en general; específicamente en Colombia, el Ministerio de las TIC ha buscado brindar lineamentos para que empresas o corporaciones cuenten con un modelo de gestión de seguridad informática.

En lo que concierne a las IES, estas también deben preocuparse por no tener ciberataques en sus sistemas, ya que la mayoría de estas, cuentan con un modelo de gestión de seguridad de la información que tiene el fin de minimizar los riesgos de divulgación de datos personales e institucionales, esto a través de diferentes estrategias que deben ser analizadas para lograr determinar la efectividad de seguridad que se le está brindando a la información personal, de estudiantes, docentes y directivas.

A pesar de esto, las IES al igual que otras empresas o corporaciones debe realizar un análisis periódico de su seguridad informática, para determinar si esta funciona bien o para poder determinar los puntos débiles que pueden ser corregidos. Es por ello, que en el presente trabajo pretende determinar ¿Cuál es la eficacia de los componentes de la seguridad informática en las IES desde una perspectiva dinámica sistemática?

2. JUSTIFICACIÓN

El presente proyecto tiene la finalidad de analizar los componentes de la seguridad informática en las IES desde una Perspectiva de dinámica de sistemas, puesto que, desde hace varios años se ha venido avanzando en el tema de la protección a los datos personales que se tienen en base de datos o en diferentes programas.

Debido a que, desde hace varios años la tecnología se ha vuelto parte indispensable en las organizaciones y en la vida de las personas, por ello, cada día se implementan diferentes modelos de protección en diferentes empresas que buscan asegurar sus datos para que no sean divulgados y así asegurar también el derecho a la intimidad de cada persona. Pues, en el desarrollo de funciones las IES se apoyan en la tecnología para el desarrollo de sus funciones, lo que deja datos importantes en el sistema, es allí, donde toma relevancia la seguridad informática, pues se debe buscar la protección a esos datos privados

No obstante, no basta con poner en función métodos de protección, sino que, constantemente se debe analizar los métodos o sistema utilizados por las IES, pues cada día se crean nuevos métodos de vulneración al sistema lo que permite una divulgación de datos personales de forma masiva. Es decir, las IES tienen el deber de brindar protección de datos a estudiantes, docentes y directivas, lo cual solo se

logra analizando los componentes de la seguridad informática. Todo esto, con la finalidad de mostrar la eficacia de la protección que se le está bridando a nuestros datos personales y aportar al buen funcionamiento de estos, pues la demostrar la seguridad de la información permite una confiabilidad en la organización.

3. OBJETIVOS

3.1.1. OBJETIVO GENERAL

Analizar los componentes de la seguridad informática en las IES desde una perspectiva dinámica de sistemas, a través de referencias documentales.

3.1.2. OBJETIVOS ESPECÍFICOS

- Determinar cuáles son los componentes de la seguridad informática en las IES en Colombia.

- Diseñar una hipótesis dinámica que explique el comportamiento de los componentes de seguridad informática en las IES en Colombia.

- Proponer una política que ayude al mejoramiento de la eficacia de los componentes de la seguridad informática utilizados por las IES Colombia.

4. ESTADO DEL ARTE

La introducción de la tecnología en el diario vivir de las personas ha ocasionado una mayor investigación por parte de los profesionales y de futuros profesionales sobre los temas relacionados, puesto que cada vez se hace más necesario conocer de seguridad informática en los diferentes ámbitos de la cotidianidad. Lo anterior, como lo mencionan Guzmán y Angarita (2017) en su trabajo de grado

> "En la actualidad, dado el crecimiento y adquisición de componentes con acceso a internet, la tecnología ha presentado un auge rápido y continúo debido a la demanda focalizada en la compra de artículos o uso de servicios en la Internet lo que genera a su vez un aumento en la demanda del mercado tecnológico".

Internacionalmente se ha indagado sobre diferentes modelos que garanticen la seguridad informática. En el Ecuador, según Vaca (2019) las instituciones no han dado el paso a nuevos modelos de implementación de la seguridad informática, lo cual representa un riesgo porque no garantizan la protección de los datos sensibles de los usuarios exponiéndolos a ataques cibernéticos. En sus resultados, refiere que el 85% de los jefes administrativos no tienen un protocolo para actuar frente a un ataque de pishing (Vaca, 2019). Lo anterior, es importante para la prevención y la protección de la información concordando por la investigación realizada por

Cáceda (2021) cuando menciona que en Perú “las organizaciones no cuentan con un modelo definido para la gestión de seguridad de la infraestructura de las TIC”, lo cual representa un riesgo significativo.

En las conclusiones del trabajo de Cáceda (2021) se hace referencia a que los modelos dinámicos para la seguridad informática contribuyen en el mejoramiento de la toma de decisiones, para disminuir los riesgos de ataques cibernéticos y las vulnerabilidades. Junto a esto, Romero (2018) revela cifras de la inseguridad informática en Perú, refiriendo que en un 60% incrementaron los ataques cibernéticos en el 2018 y, además, menciona que diariamente hubo registro de 746,000 ataques de malware en promedio; por otra parte, en los resultados de su investigación, destaca que actualmente “falta de capacitación sobre las buenas prácticas de seguridad informática” (Romero, 2018).

De esta manera, es importante mencionar que se hace necesaria el fomento de modelos de seguridad informática, no solo a nivel cibernético, sino que además, debe incluirse a los miembros de las organizaciones, incluyendo empresas y centros educativos. Por otra parte, Mayordomo (2016) propone un modelo para la seguridad informática, mediante la herramienta Honeypot la cual, crea una simulación de sistemas vulnerables y, de igual forma, estrategias de ataques, para que de esta manera, puedan ser detectadas a futuro; en esta investigación, crean reglas para

Iptables que se incorporan a los sistemas de forma automática, previniéndose así los ataques a la infraestructura.

En relación con lo anterior, Arroyo (2018) coincidiendo con Cairo et al., (2016) refiere que “no existe la seguridad absoluta”, por lo tanto, sugiere que la seguridad informática minimiza los riesgos, las amenazas y evita los daños; en consecuencia, como conclusión de su investigación menciona que se deben tomar medidas básicas para prevenir los riesgo, teniendo en cuenta que “tener una seguridad absoluta no es viable, siempre hay una nueva forma de vulnerar el sistema” (Arroyo, 2018), por lo que es necesario implementar esquemas de protección constantemente.

En contraste, Bermejo (2007) en su investigación sobre la seguridad informática en la Universidad de Sotavento, expresa que no contaban con un sistema de control interno por lo que se representa en falta de seguridad poniendo en riesgo a los alumnos, docentes y directivos, por lo que deben implementar estándares de los procesos informáticos siguiendo lineamientos internacionales y nacionales; así como la creación de una cultura informática basada en la prevención.

En la investigación realizada por Castillo (2013) hace referencia a la necesidad de la protección de los recursos informáticos en el comercio electrónico,

teniendo en cuenta que, que las prácticas que ahí se presentan involucran transacciones de dinero online, así como información de tarjetas de crédito, por lo que al realizar una encuesta el 60% de las personas mencionaron desconocer la confiablidad de las páginas; el 72% en algún momento ha comprado por internet. Es por esto, por lo que debe existir una cultura de protección de los datos mediante la seguridad informática.

Y es que, con el crecimiento de exponencial de la tecnología, también crecieron los ataques a los sistemas, es allí, donde se empezó a desarrollar el tema de la ciberseguridad, tema que, en la actualidad representa una gran relevancia nivel global, pues en el año 2022 se registró que “el 73% de las empresas en el mundo ha sufrido un ataque cibernético y muchas ni siquiera han sido conscientes de ello” (Portafolio, 2022) y además de ello, esta noticia informa que:

> Dado el continuo aumento del ransomware y el creciente panorama de amenazas actual, no sorprende que muchas organizaciones no se sientan más seguras de su capacidad para responder a los riesgos cibernéticos ahora que en 2019”, dijo Edson Villar, líder de Consultoría en Riesgo Cibernético en Marsh para Latinoamérica.

En el contexto colombiano, Pantoja (2017) realiza su investigación proponiendo un protocolo de buenas prácticas de seguridad informática en la Universidad del

Valle sede Cali, destacando que no tiene un protocolo que proteja la información almacenada; además plantea que otras instituciones como la University Collage London, reconocida por su investigación cibernética fue víctima de un ransomware, por lo que es necesario educación en seguridad informática en estos centros educativos del país. En relación con lo anterior, Villamil y Sarmiento (2021) realizaron una investigación similar en una empresa de biocombustibles también se establecieron lineamientos para estos sistemas de gestión de seguridad de la información fomentando la concientización hacia una cultura de la información.

Por otra parte, en la investigación de López (2018) encontró que en una unidad táctica de la Armada Nacional Colombiana, en el municipio de Turbo, Antioquia, el personal no estaba capacitado en una cultura de seguridad informática y realizaban prácticas que no eran seguras para la información que estaba en sus sistemas; de esta forma, se usó la metodología Magerit para visibilizar la importancia de una gestión adecuada de la infraestructura.

En otro contexto, se encontró que en el Hospital San Francisco de Gacheta, se presentaba perdida de datos sobre historias clínicas y de balances financieros en la entidad y no contaban con un protocolo de seguridad informática por lo que, al usar la misma metodología del artículo anterior, encontrando diferentes vulnerabilidades y amenazas que provocaban esta pérdida de información.

Por lo anterior, específicamente autores como Arias y Celis (2015) en Colombia es importante “un modelo de Ciberseguridad y Ciberdefensa como resultado del proceso de planeación estratégica para construir un verdadero escudo de protección para el país”, de esta forma, el país garantiza la prevención de ataques. De esta plantean que estos modelos deben estar fundamentados en “la significancia de la administración moderna (P=planeación, O=organización, D=dirección, E=ejecución, R=revisión o control)” (Arias y Celis, 2015). Lo anterior, se relaciona con que en el 2013 se reportaron 6 millones de víctimas de crimen digital en Colombia, según Mejía (2020), por lo que llevo a cabo una investigación en una empresa víctima de estos ataques, implementando un sistema de gestión de seguridad informática mediante la herramienta pentesting que resulto siendo útil para conocer las vulnerabilidades de los sistemas.

De esta manera, es necesario ver el escenario de la seguridad informática en un contexto local como el departamento de Santander y Norte de Santander; Bolaño (2015) plantea que ahora las empresas deben manejar su información en múltiples dispositivos, lo cual representan riesgos y amenazas, por lo que es necesario garantizar la protección de los usuarios por medio de redes seguras, para esto, uso la herramienta PacketFence que permite observar las anomalías en la red, ademas, mediante políticas de tipo BYOD facilita que la administración de los dispositivos y su información quede segura. Por otra parte, Corredor (2012) en su investigación menciona que son pocos los sistemas de detección de intrusos que cuentan con las

características que requiere el sector educativo en la región, por lo que concluye que Snort un sistema complejo para las organizaciones que aporta la detección de intrusiones en las redes telemáticas de área local.

En contraste, Duran (2017) en su estudio tenía como objetivo minimizar el impacto de las vulnerabilidades, amenazar y riesgos de seguridad informática, en instituciones gubernamentales y otras organizaciones en el Norte de Santander mediante el análisis de metadatos. Los hallazgos de esta investigación se centran en que existe un riesgo en estas entidades ya que “no están siendo cuidadosas con la información que publican en sus respectivos portales web” (Duran, 2017), por lo que, incluso en entidades estatales, no se toman las medidas de protección de la información. De igual forma, Ramirez (2015) realizó un análisis de los riesgos en las redes y sistemas de la Alcaldía de Pamplona donde manifiesta que no se toman en cuenta las normas del Sistema de Gestión de la Seguridad Informática, aumentando las probabilidades de delitos informáticos; gracias a este análisis se pudo detectar y controlar los protocolos en la política de seguridad, evitando así, amenazas y vulnerabilidades.

Por su parte, Moscote (2017) menciona que no hay un esquema de seguridad en las empresas, ademas encontró que en la empresa Minesa S.A.S en Bucaramanga utiliza reglas de Snort para la red local, sin embargo, necesita reforzar la seguridad en la VLan de servidor; es por esto, que se reitera la necesidad de una

crear infraestructuras que garanticen la seguridad de la información pero ademas, capacitar al personal para fortalecer los mecanismo de protección. Siguiendo esta línea, Rodriguez (2023) refiere que “a formación en seguridad informática radica en que la forma de aprenderla no es demasiado atractiva”, por lo que planteó un prototipo aplicado durante un evento en la Universidad Autónoma de Bucaramanga, donde mediante la metodología de la gamificación y la técnica Capture the Flag permitió el aprendizaje y aumentó el interés de los participantes sobre seguridad informática.

Sumado a lo anterior, las universidades han sido un tema de interés desde esta área, teniendo en cuenta, que diversos estudios han identificado carencias en la seguridad de la información, lo que los deja vulnerables a un ataque cibernético. Así, Gómez (2017) plantea que “la detección de los riesgos de seguridad mitiga la posibilidad que las organizaciones, sean víctimas de ataques informáticos”, de esta forma, detecto peligros en los procesos de seguridad de la Universidad Pontificia Bolivariana, con sede en Bucaramanga diseñando una metodología de auditoría de la seguridad para evaluar de forma descentralizada y, de esta forma, cumplir con las exigencias en la legislación colombiana.

De esta forma, se encuentran diferentes aspectos relevantes en las investigaciones realizadas, destacando que en su mayoría, coinciden manifestando que hace falta una cultura de la seguridad informática en todas las esferas, tanto a

nivel económico, estatal y educativo. Ademas, es posible notar la vulnerabilidad a la que se enfrenta la infraestructura a posibles ataques o delitos informáticos; de esta manera, es importante indagar más sobre la seguridad informática en todos los ámbitos, para construir planes de acciones en favor de garantizar la protección de la información.

5. MARCO REFERENCIAL

En este apartado, se llevará a cabo una conceptualización de los conceptos claves de la investigación, entre ellos, se encuentran seguridad informática, sistemas, instituciones de educación superior, dinámica de sistemas y, por otra parte, se aborda el marco legal desde la cual se fundamentan dichos conceptos según la legislación y el abordaje teórico que ha tenido.

5.1. MARCO CONCEPTUAL

5.1.1. Dinámica de sistemas:

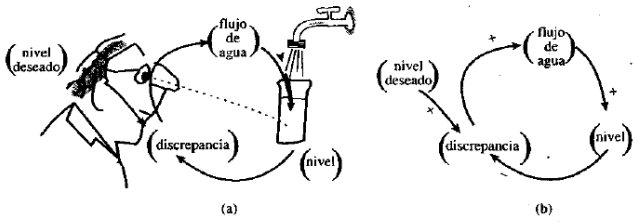
“Método concreto para el estudio de los sistemas que forman nuestro entorno”. (Aracil, 1997, p. 19).

La simulación en dinámica de sistemas permite ver en tiempo real el comportamiento de las variables añadiendo facilidades para su verificación y validación.

La dinámica de sistemas muestra de qué modo la estructura de realimentación de una organización domina la toma de decisiones por parte de los individuos.

En la siguiente Figura 1 se muestra mediante bucles de retroalimentación los distintos elementos que intervienen en la descripción del proceso. En el proceso (a), vemos que se traduce a un diagrama causal de influencias, en el que el nivel deseado aumenta la discrepancia y esta aumenta el flujo de agua que a su vez aumenta el nivel y a mayor nivel reduce la discrepancia. En el proceso (b) vemos su representación causal.

Figura 1. Proceso llenar un vaso de agua (a) con un grafo orientado (b) con un grafo signado.



Fuente: (Aracil, 1997, p. 19).

5.1.2. Pensamiento Sistémico:

El pensamiento sistémico es la visión completa de varios elementos y sus interacciones, que está orientado a examinar la interrelación de objetos que presentan un objetivo en común, proporciona una visión holística, abarcando una variedad de herramientas, métodos y principios.

> “El pensamiento sistémico es la quinta disciplina que integra las demás disciplinas, fusionándolas en un cuerpo coherente de teoría y práctica”. (Senge, 2010, p. 21)

Senge (2010) menciona que la esencia del pensamiento sistémico es ver las interrelaciones entre las variables en vez de las relaciones lineales de causa – efecto y ver los procesos de cambio. (p. 97).

> En el pensamiento sistémico, cada imagen cuenta una historia y se representan mediante diagramas causales. De cualquier elemento de una situación (“variable”), se pueden trazar flecha (“eslabones”) que representan la influencia sobre otro elemento. A la vez éstos revelan ciclos que se repiten una y otra vez, mejorando o empeorando las situaciones. (Senge, 2006)

La innovación tecnológica de las últimas décadas ha traído consigo, nuevos conceptos que con el pasar de los días va tomando relevancia, posicionándose hoy en día como destacados. Dentro de dichos conceptos encontramos, la seguridad informática, ciberseguridad, la dinámica de sistemas, entre otros conceptos.

En lo respecta a la seguridad informática, es importante mencionar que se debe hacer una distinción con la seguridad de la información, pues, estos dos conceptos tienen cosas en común pero no son lo mismo. Por su parte, “la seguridad

informática, con sus siglas en inglés IT security, es la disciplina que se encarga de llevar a cabo las soluciones técnicas de protección de la información.” (Figueroa, J. Rodríguez, R. Bone, C. Saltos, J. 2017)

En la misma línea, los autores Figueroa, J. Rodríguez, R. Bone, C. Saltos, J. (2017) citando a González (2011) quien considera que:

> la Seguridad Informática, es la “disciplina que se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que-articulados con prácticas de gobierno de tecnología de información-establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo”. (González, 2011) (Figueroa, J. et al. 2017)

Sumado a ello, para autores Gil, V. Gil, J. (2017) “la seguridad de la información se ha convertido en una tarea de vital importancia y preocupación para empresas, organizaciones e instituciones públicas y privadas.” (Gil, V. Gil, J., 2017) Sin embargo, son las mismas personas las que se han encargado de que exista una protección a la información, debido a que, con el desarrollo de la tecnología se le ha

incrementado el acceso a esta a más personas, las cuales se han convertido en una amenaza contra la protección de algunos datos. Es allí, donde surge el concepto de la seguridad de la información, el cual es definido como:

> una disciplina “que se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo (…) es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos, que nos exigen niveles de aseguramiento de procesos y de tecnología para elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información”. (ISOTools Excellence, 2017). (Figueroa, J. et al. 2017)

Adicional a ello, se debe tener en cuenta que esto tiene la finalidad de “proteger a los sistemas informáticos de las amenazas a los que están expuestos” Gil, V. Gil, J. (2017).

Es decir, la seguridad informática se enfoca en la protección del sistema como tal, mientras que, la seguridad de la información es la estrategia que se utiliza para la

protección de los datos. No obstante, estos dos conceptos deben trabajar de la mano, pues lo que buscan es la protección de los datos a través de diferentes estrategias que permiten no tener amenazas al sistema y a los datos.

Otros de los conceptos que ha adquirido mayor relevancia en los últimos años es la ciberseguridad, pues como se mencionó con anterioridad, con el avance tecnológico se ha permitido el acceso a muchas más personas que muchas veces buscan vulnerar el sistema, adquiriendo de forma información confidencial o privada, por lo tanto la ciberseguridad es definida como "la práctica de proteger los sistemas críticos y la información confidencial de los ataques digitales, es decir, busca garantizar la consistencia, integridad y confiabilidad de la información que se gestione a través de medios tecnológicos." (Solleiro, J. et al. 2022)

Adicional a ello, Solleiro, et al.,(2021) hacen mención a que:

> La ciberseguridad abarca todo lo relacionado con la protección de datos personales, información de identificación personal, información de salud, propiedad intelectual, datos y sistemas de información gubernamentales y de la industria contra el robo y el daño por parte de ciberdelincuentes y otras entidades que intenten ingresar en una red privada. La ciberseguridad aplica en diferentes contextos, desde

> los negocios hasta la informática móvil y puede dividirse en algunas categorías comunes. (Solleiro, J. et al. 2022)

Por su parte, la dinámica de sistemas “es una técnica de modelado de sistemas complejos cuya filosofía gira en torno al concepto de retroalimentación, o causalidad circular entre variables observables” (Gil, V. Gil, J., 2017)., de acuerdo, con lo anterior, para, Agudelo, D. y López, Y. (2018) la dinámica de sistema es entendida como:

> una herramienta para controlar y manejar de forma eficiente todos los sistemas y operaciones por medio de simulaciones que permitan ver el comportamiento y los cambios del proceso en el tiempo [13]. Esto lleva a que, por medio de la dinámica de sistemas, sea posible conocer el comportamiento de todo lo que influye en la administración del inventario para mejorar la productividad, disminuir costos, y aumentar la ventaja competitiva empresarial. (Agudelo, D. y López, Y., 2018)

Dentro de este mismo tema, encontramos la llamada hipótesis dinámicas, la cual se entiendo como:

> una explicación del comportamiento de una variable sustentada en un razonamiento basado en las estructuras de realimentación del modelo que la contiene y en experimentos de simulación. Además, esta hipótesis es la base para definir políticas y escenarios que buscan cumplir con un objetivo pre-establecido. (Aceros, V. Díaz, A. Escobar, J. García, A. Gómez, J. Olaya, C. Otero, V. 2011)

Estos conceptos que tal vez hace unos años no se tenían presente, hoy en día son más comunes y adquieren cada día más importancia en el mundo moderno.

5.2. MARCO LEGAL

La tecnología al estar presente en la mayoría de los ámbitos de la vida de la personas, ha tenido que ser regulado de cierta forma, sobre todo en lo que tiene que ver con la seguridad, pues como se ha mencionado, no todas las personas hacen uso adecuado de la tecnología, sino que por el contrario, buscan vulnerar los sistemas y la protección a los datos privados.

Por ello, en la mayoría de los países existe regulación sobre este tema y además existen sanciones para quienes infringen dichas normas o irrumpen en los sistemas sin tener autorización para ello.

Es por esto, que se hace necesario mencionar las normas más relevantes frente al tema aquí tratado y los posibles delitos que puede cometer una persona frente a la seguridad.

Específicamente en Colombia, desde la constitución política de 1991 se hace una protección a la intimidad, pues, en el artículo 15 se determina que: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar.

Sumado a ello, el estado ha creado una serie de leyes que buscan la protección de este derecho constitucional, dentro de los cuales se puede encontrar:

Decreto 2693 de 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones

Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.

Ley 23 de 1982 sobre Derechos de Autor.

Ley 1474 de 2011 Estatuto General Anticorrupción.

ISO 27001 (UTS. S.f.)

Adicional a ello, se encuentran estipulados delitos que, según Ojeda, J. Rincón, F. Arias, M. Daza, L. (2010)

> La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la *Ley de Delitos Informáticos*, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas. (Ojeda, J. et al. 2010)

También están las leyes informáticas según **actualización a 01 febrero 2018**

En el presente apartado se relacionan los elementos legales que están involucrados en el tema de seguridad informática, generando una construcción que delimite el campo de acción de esta y el impacto que tiene desde el ente jurídico.

LEY 527 DEL 18 AGOSTO DE 1999: Se define y se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y otras disposiciones.

LEY 1266 DEL 31 DE DICIEMBRE DE 2008: Establece las disposiciones generales del Hábeas Data y se controla el manejo de la información que contienen las bases de datos personales, en forma muy primordial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1273 DEL 5 DE ENERO DE 2009: Esta ley permite generar una protección completa para los cada uno de los datos que se brindan en las entidades, teniendo la posibilidad además de defenderlos en caso de ser mal utilizados.

LEY 603 DEL 27 JULIO DE 2000: Modifica el artículo 47 de la ley 222 de 1995.

LEY 1581 DEL 17 OCTUBRE DE 2012: Esta Ley, es acerca de la Protección De Datos Personales, siguiendo los lineamientos

establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

DECRETO 1377 DE JUNIO 27 DEL 2013: Este Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

5.3. MARCO TEORICO

5.3.1. Seguridad Informática

Para empezar, es menester definir qué es la seguridad informática, autores como Candelario y Rodríguez (2014) la definen como el conjunto de conocimientos de los sistemas que están encaminados a conseguir la seguridad de la información, de esta forma, el objetivo de estas son garantizar que los datos permanezcan integra y sin vulneraciones.

Por su parte, Peñafiel (2021) menciona que también “es conocida como ciberseguridad, es una rama de la Informática”, de esta forma, se establecen medidas y protocolos que protejan los dispositivos y la infraestructura de los sistemas. De esta manera, para hablar de seguridad informática es preciso saber

que, las amenazas son entendidas por López (2010) como la presencia de uno o diversos factores que tienen la posibilidad el atacar el sistema, teniendo en cuenta su vulnerabilidad. Además, estas últimas son consideradas como un efecto del sistema, que permite la oportunidad de ataques y podría causar daños (Avenía, 2017).

Con relación a lo anterior, Según Alegre y Garcia-Cervigon (2011) se puede dividir la seguridad informática en dos: la seguridad física, la cual se encarga de proteger el sistema informático, mediante mecanismos de control de amenazas accidentales como, por ejemplo, borrar información accidentalmente u el olvido de la contraseña; por otra parte, también se presentan las amenazas deliberadas que consisten en el robo de las contraseñas, extracción de información y robo de datos accidentales; por último, también se encuentran las amenazas naturales que como se puede inferir son por causa de incendios, terremotos y demás factores del medio ambiente.

Por otro lado, también se encuentra la seguridad lógica, donde se enfoca en el software del equipo, es decir, de los programas y los datos e información; en este caso, se encarga de prevenir robos , fraudes y sabotajes al ingresar datos confidenciales; también se encuentran la pérdida o destrucción de la información y, en el caso de las organizaciones, entre ellas, Instituciones de Educación Superior, perdida de dinero.

Pero, ademas, también se distinguen dos formas de seguridad según Cervantes y Ochoa (2012) los cuales son la activa y la pasiva; refieren que la primera evita daños en los sistemas informáticos encriptando los datos y mediante softwares de seguridad. Por otra parte, la seguridad pasiva, hace referencia a las copias de seguridad y el mantenimiento adecuado del hardware.

De esta manera, las herramientas de seguridad son técnicas que permiten diseñar, detectar y prevenir ataques de seguridad informática; a esto, según Alegre y Garcia-Cervigon (2011) menciona que el cifrado, el cual define como usar algoritmos matemáticos para transformar los datos, de esta forma, se encuentra protegida, puesto que para leer estos datos cifrados, se hace necesario descifrarlos. Para Kaspersky (2023) existen diferentes técnicas de cifrado entre ellas el simétrico y el asimétrico, diferenciándose en que la primera es una clave privada y la otra hace uso de claves privadas y públicas, vinculadas matemáticamente.

Otro mecanismo de seguridad es el control de acceso, mediante esto se refuerza el acceso a los recursos, permitiendo que solo pueda acceder a la información mediante autenticación y autorización, de esta forma, se mantiene protegida la información de usuarios no autorizados, según Microsoft (2023) hay tipos de control de acceso discrecional, obligatorio, basado en roles y, por último, basado en atributos.

En el discrecional el usuario es quien concede acceso; por otro lado, el obligatorio requiere de una autorización de una autoridad reguladora; en el modelo basado en roles, se concede de acuerdo con las funciones que ejerza el usuario dentro de la organización; y, por último, el basado en atributos se caracteriza porque se da acceso según la hora, la ubicación y la combinación de atributos del usuario.

Así, también se encuentra el relleno de tráfico, el cual según los autores Alegre y Garcia-Cervigon (2011) hacen referencia a la inserción de bits en un flujo de datos que dificulten el análisis de tráfico, de esta forma, el atacante no sabe que cantidad de datos son útiles. Consiguiente a esto, también plantean el control de enrutamiento, que es cuando se seleccionan rutas seguras para determinar datos y de igual forma, permite enrutar cuando haya una brecha de seguridad.

Así, también se hace menester reconocer los tipos de atacantes más comunes, para que de esta forma se prevenga de estas modalidades; sobre esto, Roque y Juárez (2018, citando a Magazine, 2009) hacen la distinción de que:

> “un hacker es una persona con alto nivel de conocimientos técnicos que utiliza una computadora para tener acceso a un equipo o red, con el objetivo de realizar actividades no autorizadas. Algunos expertos argumentan que los hackers poseen principios éticos y que sus acciones no llevan una intención

maliciosa. Por el contrario, un cracker aunque hace lo mismo que un hacker sí tiene unos objetivos maliciosos implícitos en su conducta."

Principalmente Alegre y Garcia-Cervigon (2011) refieren que los virus informáticos son un tipo de programa o código malicioso que se autorreplica o se adjunta a otros programas, dentro de los virus se pueden encontrar los gusanos, los cuales se reproducen de manera autónoma y pueden destruir datos y robar información; otro tipo de virus son los troyanos, el cual ingresa al ordenador de una forma en la que el usuario no sospeche que es un archivo nocivo, incluso según Jenab y Moslehpour (2016) pueden presentarse como una opción para eliminar virus y, al final, terminar infectando el sistema.

Otros medios que usan los delincuentes cibernéticos, es mediante el phishing el cual suplanta la identidad mediante correos electrónicos, llamadas telefónicas, entre otros, para obtener datos como contraseñas o información bancaria; otro tipo de ataque es mediante el ransomware, el cual encripta los datos y el atacante pide un rescate por ellos. Otra manera de recolectar información sin el consentimiento de la persona son los programas spyware, esto les permite a los delincuentes cibernéticos robar contraseñas, entre otras cosas.

Concretamente, los usuarios y las organizaciones deben protegerse de este tipo de acciones, por lo que entre los métodos de protección se encuentran los

antivirus, el mantenimiento de los equipos con una actualización constante para que se apliquen los parches de seguridad, el filtro de archivos dañinos usando técnicas de firewall, las copias de seguridad, la infraestructura de clave publica, pero sobre todo, la capacitación en este ámbito adaptándose a las necesidades, detectando y protegiendo de programas dañinos.

Las herramientas que actualmente se están usando para el análisis de las vulnerabilidades para Romero et al., (2018) son Nessus que permite evaluar categorizando las deficiencias según el riesgo, pero ademas, da datos estadísticos y genera alertas y notificaciones; ese programa tiene un monitoreo constante de la infraestructura; Otra herramienta que destacan estos autores es Acunetix, que escanea las vulnerabilidades, detectando fallas y falencias locales y en la red.

Otra propuesta para la seguridad de la información son las auditorias, las cuales son definidas por Ruiz (2011) como “el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, los servidores y las redes de comunicaciones”; en consecuencias, para garantizar la integridad de la información y su confidencialidad, es importante que las organizaciones, como las instituciones de educación superior, realicen auditorias periódicas a la infraestructura que tengan, de esta forma se realizaran diagnósticos y se plantearan políticas de seguridad.

Las fases de las auditorías a la seguridad de la información, se realiza en 3 fases según Solarte et al., (2015), donde la primera es la determinación de las vulnerabilidades, amenazas y riesgos; para esto se debe realizar un estudio en la organización que revele los aspectos sobre los cuales se debe tomar acción; la segunda fase, es sobre el análisis de riesgos y diagnóstico de la seguridad de la información, para esto, es posible usar un proceso de estudio según el estándar Magerit, esto influirá en la disminución del impacto en la organización de los hallazgos del estudio y se creara un plan de acción; la tercera fase, es la definición de controles para el diseño del Sistema de Gestión de Seguridad de la Información, con esto se determinan las causas de los hallazgos y se basa en los lineamientos de la norma ISO/IEC 27002.

A su vez, es importante comprender que con la digitalización en la vida cotidiana y el traslado del teletrabajo, las empresas no solo financieras, sino que también instituciones educativas, se han visto susceptibles a diversos ataques, provocando perdida de información y de dinero; en consecuencia de lo anterior, en los tiempos de la pandemia del COVID-19 los ciberataques aumentaron significativamente. Por lo que en este contexto educativo y social en general, la protección de los datos sensibles y personales debe garantizar el derecho a la intimidad; de igual manera, el gobierno debe garantizar que los datos de los usuarios

y las personas que transitan en internet no sean revelados a terceros con fines mercantiles, según Martinez y Martinez (2018).

Desde otra perspectiva, Cañón (2015) plantea la idea de que es importante la seguridad, especialmente en los niños que hacen uso de los dispositivos, puesto que esta población se encuentra expuesta a trampas contenidas en la red; para dar solución a esto, actualmente existen métodos de control parental y el establecimiento de límites a la hora de navegar por internet, sin embargo, se hace necesario el acompañamiento y la capacitación a los padres para evitar delitos como el acoso cibernético.

En el caso de Bogotá, según Castellanos (2019) pasaron de 33 a 44 modalidades de ataques informáticos, ademas, datos de la Interpol (2020) refieren que entre los meses de enero, hasta el 24 de abril de ese año “se detectaron 907.000 correos basura, 737 incidentes de tipo malware, y 48.000 URL maliciosas, todos ellos relacionados con la COVID-19”; esto, puede tener como consecuencia, la percepción de inseguridad de la ciudadanía en la red.

No obstante, también se han desarrollado estrategias de protección de la información, ya que en el estudio realizado por Deloitte (2020) se evidencia la labor de las entidades estatales y las organizaciones de todo tipo para que, en medio del crecimiento de los ataques, se pudiese estar a la par con medidas de protección

para las personas. Así, Kaspersky Security Network (2020) informó que neutralizaron más de 726 millones de ataques cibernéticos en durante el primer trimestre del 2020 durante la pandemia del COVID-19.

Teniendo en cuenta lo anterior, es importante considerar que con la rápida evolución de las nuevas tecnologías, se hace necesario que exista personal idóneo que detecte los puntos débiles y determinen medidas preventivas, una de las herramientas usadas es Honeynet, que detecta estas vulnerabilidades en el sistema. (Tirado et al., 2017).

Aunado a esto, es necesario tener en cuenta el desconocimiento sobre seguridad informática en la sociedad en general; en la investigación de Peñafiel (2021) encuestaron a 384 personas, de los cuales solo el 19,1% saben que es el phishing, de esta forma, se hace evidente la necesidad de educar a la sociedad en general sobre este aspecto.

Considerando lo anterior, la educación en la seguridad de la información debe tenerse en cuenta, para garantizar la integridad, la confidencialidad y la disponibilidad; aun así, Hernández (2019) manifiesta que:

“Algunos factores que ocasionan eventos o incidentes de seguridad relacionados a la fuga de información son: por descuido, falta de conciencia,

no tener el conocimiento apropiado, inconformidad de los funcionarios, no tener capacitaciones en los temas, por negligencia de las personas ya sea de forma accidental o premeditada ocasionando de esta manera numerosas amenazas”

5.3.2. Instituciones de educación superior

Desde otro contexto, según el Ministerio de Educación Nacional (2017) son definidas como “entidades que cuentan, […], con el reconocimiento oficial como prestadoras del servicio público de la educación superior en el territorio colombiano”, de esta forma, se catalogan en dos, las acreditadas por el Consejo Nacional de Acreditación o las que no, pero que cuentan con registro calificado vigente. Entre otras cosas, está comprometida por el Articulo 19, de la Ley 30 de 1992 a la investigación científica y tecnológica (Ministerio de Educación Nacional, 2017).

Por otra parte, para la UNESCO (2019) se considera educación superior, a programas educativos posteriores al bachillerato, por lo cual, son impartidos por universidades, entre otras instituciones de enseñanza autorizadas. Según el Ministerio de Educación (2023) en el año 2022 el 54,92% de los jóvenes se encuentran matriculados en alguna Institución de Educación Superior.

A lo anterior, se le suma que en un estudio entre los jóvenes de 16 a 25 años, solo el 41,8% opta por adquirir un software antivirus; ademas de esto, se señala en este estudio de Machuca y Cabrera (2020) que solo “el 26.8% utiliza control parental en los dispositivos tecnológicos de sus hijos”, de esta forma, los niños, niñas, adolescentes y jóvenes han tenido un contacto con la tecnología que ha aumentado desde la pandemia del COVID-19, aun así, “la percepción de conocimiento en seguridad informática de los padres tiende a estar entre un nivel medio y bajo” (Machuca y Cabrera, 2020).

En el caso de las redes sociales, es importante destacar el papel de estas en la juventud actual, sin embargo, “las redes son los medios más populares utilizados para el ciber-acoso, ya sea a través de chat, mediante la publicación de mensajes ofensivos o creando páginas de grupos de odio” (Arellano, 2017); por otra parte, también se menciona que existe riesgos comerciales, donde la información se comparte a empresas mediante aplicaciones, con el fin de hacerle seguimiento al comportamiento de su usuario. De esta forma, según Arellano (2017) esto constituye una amenaza como el acoso en internet.

Considerando esto, según Martinez y Martinez (2018) menciona que “se considera necesario que los niveles educativos sean el pilar para empezar a contrarrestar los ataques de los piratas informáticos sobre los datos personales e íntimos y formar una cultura de la seguridad de la información”, considerando esto,

se entiende que los delincuentes cibernéticos día a día encuentran nuevas víctimas y formas de acceder a la información de los usuarios.

Teniendo en cuenta esto, las universidades han tenido que adaptarse a los cambios tecnológicos de la actualidad y el uso del internet, lo que conlleva al uso de bases de datos y de infraestructura tecnológica que pueden presentar riesgos de ataques cibernéticos, considerando que Salazar et al., (2021) mencionan que “cuanto más grande es la organización, hay más probabilidades de sufrir un ataque”, aun así, es pertinente mencionar que también las organizaciones medianas y pequeñas, así como los individuos sin discriminar, puede ser víctima de estos ataques cibernéticos.

De esta forma, existe una relación entre las Instituciones de Educación Superior y la Seguridad Informática, puesto que no solo es la información de los estudiantes, docentes y administrativos la que manejan, sino que también, mediante ciberataques pueden llegar a robar, si no se toman medidas de protección, la información financiera que en estos sitios se suministra. Siendo entonces tan amplio este campo, se han caracterizado diferentes delitos cibernéticos, cada día las universidades deben actualizarse en los Sistemas de Gestión de la Seguridad Informática.

Con relación a esto, Zuñiga et al., (2021) en su investigación sobre el impacto en los procesos de seguridad informática en la Universidad Regional Autónoma de los Andes, entre sus hallazgos, se encuentra que el 67% de los participantes si tuvieron capacitación sobre seguridad informática, concluyendo que algunas universidades están a la vanguardia tecnológica en estos aspectos.

Por su parte, Chicaiza y Diaz (2014) refieren que las universidades públicas, tienen grados de desinterés en las temáticas como la seguridad de la información, esto conlleva a que se destine poco presupuesto a esta problemáticas; esto permite que no haya programas ni políticas establecidas que contribuyan a la seguridad de la información que manejan.

Lo anterior, representa un problema, si se parte de lo mencionado por autores como Solís et al., (2023) “la gestión de la seguridad informática minimiza las vulnerabilidades que un sistema pueda presentar, mejorando los mismos mecanismos de seguridad, bajando los costos y el tiempo requerido para solucionar un problema”, así, la información por su valor actual debería incentivar a estas instituciones a desarrollar estrategias de protección.

Es por esto, por lo que las Instituciones de Educación Superior deben actualizarse y brindando protección para las nuevas tecnologías, así como escanear manualmente o de manera automatizada las vulnerabilidades existentes para que

de esta forma, se tomen acciones para construir planes que fortalezcan la seguridad de la información (Igarza et al., 2018; Imbaquingo et al., 2019).

Otros autores como Wiseman (2017), así como Stanciu y Tinca (2016) destacan que es necesario considerar la concientización como un factor que dificulte estos ataques anteriormente mencionados, de esta forma, los usuarios, van a reconocer cuales son las vulnerabilidades potenciales y actuaran para mejorar la seguridad informático de sus dispositivos pero también de las organizaciones de la que hagan parte.

Sobre lo anterior, Roque y Juárez (2018) refieren que:

> “El objetivo principal de un programa de concientización es cambiar comportamientos, hábitos y actitudes; algunos recursos para lograrlo incluyen seminarios, entrenamientos en línea, vídeos, correos electrónicos, posters y juegos. Este objetivo se debe cumplir a través de un proceso continuo a largo plazo"

Otra propuesta es la implementación de Sistemas de Gestión de Seguridad de la Información en las Instituciones de Educación Superior, puesto que según Montilla (2020) el objetivo principal de las autoridades a cargo de la información académica, entendidas desde la perspectiva de ser uno de los activos más

importantes, es garantizar que la información que certifican es legítima, por lo tanto, deben elaborarse estrategias que eviten los delitos informáticos.

Por lo tanto, para la implementación de un Sistema de Gestión de Seguridad de la Información, para autores como Valencia-Duque y Orozco-Alzate (2017) se contemplan 5 fases, según la norma ISO/IEC 27001, la cual determina una primera fase para la aprobación de la dirección del proyecto, donde se establecen las prioridades, en este caso, de las instituciones de educación superior.

De esta forma, Hernández (2019) hace referencia a los Sistema de Gestión de Seguridad de la Información de la siguiente forma:

> “Dicho sistema contiene los lineamientos y las buenas prácticas para llevar a las organizaciones a un mejor nivel de seguridad y mejorar las respuestas de incidentes ante las amenazas que afectan estos activos, involucrando la estructura organizacional, las políticas, la planificación de actividades, los procesos, los procedimientos, los recursos tecnológicos y humanos con el fin de garantizar que el Sistema de Gestión de la Seguridad de la Información sea implementado de forma exitosa”

Seguido a esto, la siguiente fase es definir el alcance y los límites, para que así, se pueda avanzar a otra fase de análisis de los requisitos donde se establecen

los activos y se realiza la evaluación; la otra fase, es la valoración, evaluación y el tratamiento de los riesgos teniendo como eje la norma ISO/IEC 27005, y por último, se diseña el Sistema de Gestión de Seguridad de la Información mediante el monitoreo constante de la misma.

Por otra parte, Martinez y Martinez (2018) consideran que “la educación es el factor clave para iniciar con una cultura de la protección de la información, ya que la falta de seguridad digital implica que estemos expuestos a ataques de ciberdelincuentes y espionaje”; de esta forma, otros aspectos a considerar dentro de la seguridad informática es incorporar programas de estudio acerca de estrategias de protección de los datos y de esta forma, cuidar la información personal y de las organizaciones como las instituciones de educación superior.

Relacionado a esto, Hernández (2019) en la investigación realizada destaca que:

> “Por buenas prácticas el área de seguridad de la información recomienda que la información sea centralizada en un repositorio (Red compartida) para tener mejor control sobre esta, ya que por dispositivos removibles la información está expuesta a que personas no autorizadas accedan a ella provocando perdidas, robos o alteraciones de los datos.”

Así mismo, se propone que es necesario que los funcionarios, ya sean gubernamentales o de organizaciones privadas, sean capacitados constantemente dotándolos de formación acerca de la seguridad de la información y como sus acciones dentro de esta infraestructura pueden tener un impacto negativo, pero ademas, menciona Hernández (2019) que es importante “tener un control de las actividades para comprobar que se realizan correctamente”; de igual forma, hay que reconocer los riesgos a los que se exponen.

6. DISEÑO DE LA INVESTIGACIÓN

Para el presente trabajo se desarrollará una metodología descriptiva cualitativa debido a que, se pretende describir y analizar los componentes de la seguridad informática en las IES. Para el desarrollo descriptivo cualitativo esta investigación se apoyará en el estudio de documentos como los artículos científicos y repositorios universitarios, que desarrollan el tema, otorgando una la visión general del tema. Luego se realizará una hipótesis y la proposición de una política de mejoramiento.

El presente trabajo de investigación se llevará a cabo en tres fases con tres actividades cada una como se muestra en la siguiente tabla 1.

Tabla 1. Fases y actividades.

Metodología		Mes																			
		Mayo				Junio				Julio				Agosto				Septiembre			
Fase I																					
Actividad	Búsqueda de bibliografía																				
	Lectura de resumen de documentos																				
	Selección de documentos																				
Fase II																					
Actividad	Lectura completa de los documentos																				
	Exclusión de documentos																				

	Planteamiento de hipótesis	
Fase III		
Actividad	Escritura documento	
	Búsqueda de políticas	
	Conclusión	

Elaboración propia.

De esta manera, este trabajo de investigación en la fase I que está relacionado con el objetivo de determinar cuáles son los componentes de la seguridad informática mediante la revisión documental, se llevará a cabo en tres actividades, las cuales comprenden la búsqueda de los documentos; la lectura de los resúmenes, titulo y palabras clave; y por último, la selección inicial de los documentos.

Así, en la fase II responderá al objetivo de diseño de la hipótesis, por lo que se llevará a cabo una lectura completa de los documentos seleccionados inicialmente, luego, en la siguiente actividad se excluirán los artículos que no cumplan con los criterios y, la última actividad, tiene que ver con el planteamiento de la hipótesis con base a la documentación realizada en los artículos y repositorios.

En último lugar, la fase III, tendrá que ver con la proposición de la política que contribuya al mejoramiento de la seguridad informática en las IES, para esto,

después de las fases anteriores, se procede a escribir el documento, luego se realiza la búsqueda de las políticas y finalmente se realiza la conclusión.

A través del análisis final de la información encontrada en las bases de datos se pretende cumplir con el objetivo general planteado inicialmente para esta investigación, el cual es analizar la efectividad de los componentes de la seguridad informática en las IES desde una Perspectiva dinámica de sistemas.

7. DESARROLLO DEL TRABAJO DE GRADO

En este apartado, es necesario recordar que lo que se pretende con esta investigación es ampliar el conocimiento sobre el tema, al analizar la manera en la que la dinámica de sistemas es efectiva para la seguridad informática en las instituciones de educación superior.

En relación con lo anterior, se diseñaron diferentes fases por cada objetivo específico, de esta forma, se esperar lograr abarcarlos completamente, para esto, se plantearon actividades que permitan cumplirlos y, como fin último, cumplir con el objetivo general inicialmente planteado, ademas, esta búsqueda e hipótesis, permite dar una idea de la forma en la que se están abordando los investigadores a la seguridad informática desde las instituciones de educación superior.

Pero ademas, es un reto al comprender que la información en las bases de datos no es abundante como en otras áreas u otras organizaciones diferentes a las instituciones de educación superior; de esta manera, y siguiendo la línea de que las nuevas tecnologías son usadas en gran parte del mundo.

Pero que a la vez, hace falta implementar en la sociedad, una cultura basada en la seguridad de la información, teniendo en cuenta que como se menciona

anteriormente, es importante que los usuarios mantengan informados acerca de cómo cuidar su información .

Así que, se presentará el desarrollo del trabajo según las tres fases propuestas y como se llevarán a cabo para cumplir los objetivos, pero ademas, para que los resultados permitan el análisis planteado inicialmente, De esta forma, se describirá el desarrollo de cada una de las fases junto con las actividades, con la finalidad de evidenciar metodológicamente como se realizó la presente investigación.

Para empezar, en la fase I se ha denominado la fase de búsqueda e identificación de la información, esta, será realizada mediante tres actividades que van desde el mes de mayo al mes de junio. La intención de esta fase es obtener la literatura que sea útil para este trabajo de investigación.

Para lo anterior, se realizó la recopilación de documentos mediante el motor de búsqueda que almacena diferentes bases de datos, Google Académico; el cual incluye diferentes revistas incluidas Redalyc y repositorios de diferentes universidades, incluyendo nacionales; consiguiente a esto, se inició la indagación bajo unos criterios de búsqueda haciendo uso de operadores booleanos “seguridad informática” OR “seguridad informática en las IES” AND “Dinámica de sistemas”.

Todos los resultados fueron obtenidos en el idioma español, con resultados de países de América Latina. Ademas, los documentos tenidos en cuenta fueron publicados entre los años 2010 y el 25 de mayo del 2023 debido a que son pocas las referencias bibliográficas que tratan el tema aquí presentado.

Con relación a la búsqueda quedaron 199 documentos a revisar, de los cuales se excluyeron los que después de una lectura del resumen, el titulo y las palabras clave no estuvieran relacionados con el tema a tratar quedando un total de 52 después del proceso de selección.

De la anterior forma, se garantiza que los documentos encontrados para ser abordados en esta investigación son pertinentes de ser abordados y van a contribuir de manera significativa y evitar la lectura completa de textos que tienen otros enfoques teóricos y metodologías.

Luego de esto, se da inicio a la fase II, donde se realiza la lectura completa, incluyendo el título, resumen, palabras clave, introducción, metodología, resultados y discusiones o conclusiones, permitiendo a la vez, identificar los componentes de la seguridad informática cumpliendo así con el objetivo específico planteado, de esta manera, es importante destacar que esta fase tuvo una duración de dos meses, entre las últimas semanas de junio y las primeras semanas de agosto de 2023.

Por lo anterior, los artículos que se tuvieron en cuenta fueron los publicados hasta el 25 de mayo de este año en curso; así, en la búsqueda se encontraron diferentes artículos de diversos países aunque solo se incluyeron los publicados en Latinoamérica, sin embargo, es necesario resaltar que existen pocos estudios de este tipo, lo que permite inferir que existe poco interés desde esta y diversas áreas del conocimiento en esta temática.

Luego de la lectura completa, se excluyeron los documentos que fueran libros y conferencias, puesto que metodológicamente se hace esencial introducir en esta investigación artículos científicos y documentos de repositorios de universidades. Ademas, se incluyeron investigaciones cualitativas y cuantitativas, así como revisiones sistemáticas de la literatura.

Con relación a esto, se incluyen solamente 21 documentos para el análisis de los resultados; permitiendo después de la revisión completa plantearse las hipótesis establecidas en el segundo objetivo específico.

Posteriormente, en la fase III se procede a escribir los resultados de las anteriores fases y da paso a la búsqueda de políticas de mejoramiento para las Instituciones de Educación Superior en el ámbito de la seguridad informática como los modelos y las políticas de seguridad de la información (2022) o los Sistemas de

Gestión de Seguridad Informática; entre ellos, se destaca la realización periódica de auditorías.

Por lo anterior, representa un factor importante, ya que con base a esto, las instituciones de educación superior, como las universidades podrán fortalecerse en ese aspecto no solo a nivel de infraestructura, sino que también en la implementación de políticas de cultura de la seguridad informática desde la dinámica de sistemas.

Esta dinámica de sistemas, según lo encontrado permitirá ver el sistema de una manera íntegra, teniendo en cuenta la perspectiva holística que aporta este sistema, por lo que es posible hacer un análisis, de todos los aspectos que componen la seguridad informática, pero a la vez las instituciones de educación superior.

De esta forma, se da paso al análisis de los componentes que contribuyen a que en las universidades o instituciones de educación superior existan, desde una perspectiva de la dinámica de sistemas, mecanismos de respuesta ante los ataques cibernéticos.

El análisis se realiza desde la literatura encontrada, por lo que es importante hacer una lectura detallada para de esta forma describir los componentes, pero

ademas, el formular nuevas hipótesis alrededor de la pegunta de investigación es pertinente para ampliar el panorama e incentivar a que se desarrollen nuevos estudios, pero ademas para la creación de nuevas políticas de seguridad.

8. RESULTADOS

En la actualidad el mundo vive en una era tecnológica, donde cada día se ve más inversa en el diario vivir de las personas, es por ello, que la seguridad informática toma relevancia. En lo que tiene que ver con la protección de los datos, las empresas, corporaciones e instituciones deben contar con un plan de protección para la información, pues se debe garantizar la protección a los datos privados, es por ello, que empresas e IES cuentan con planes de seguridad informática, que tiene una constante evaluación de eficacia.

Es muy escaso el nivel investigativo a este nivel lo cual sustenta la importancia de realizar investigaciones de este corte en el orden nacional.

Se describe estudio al respecto de universidades nacionales e internacionales que permitirán abordar en primera instancia una caracterización de la temática en el estudio realizado y cuál ha sido el enfoque, lo mismo la relevancia para la universidad y su impacto a nivel de la seguridad informática en el sistema de datos de esta. (Montilla, 2020)

Muchas IES nacionales han implementado en su normativa de seguridad cibernética una serie de protocolos que han diseñado cuidadosamente en base a

los múltiples ataques que han sufrido en los últimos años por causas externas o bien sea internas, y que con disciplina han logrado mejorar ese número de incidentes y/o ataques en los que se han visto envueltos.

En la siguiente Tabla 1. Se muestran algunos componentes clave de la seguridad informática en las IES en Colombia, al igual que en cualquier otra organización, implica una serie de componentes esenciales para proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas. A continuación, se presentan los componentes clave de la seguridad informática en este contexto:

Tabla 2. Serie de componentes esenciales para proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas.

COMPONENTES	DESCRIPCION DE LA VARIABLE
Entorno cambiante (Externo e interno)	En el centro de este modelo se encuentra un entorno dinámico que incluye factores tanto externos como internos que afectan la seguridad informática. Estos factores pueden incluir cambios en las regulaciones gubernamentales, avances tecnológicos,

	amenazas cibernéticas emergentes y la evolución de la infraestructura de TI interna.
Evaluación y riesgos de amenazas	La institución realiza evaluaciones de riesgos y amenazas de manera periódica o en respuesta a cambios significativos en el entorno. Esto puede incluir la identificación de vulnerabilidades en sistemas, evaluación de la probabilidad de ataques cibernéticos y el impacto potencial de incidentes de seguridad.
Políticas y normativas de seguridad	Se establecen políticas y normativas de seguridad sólidas en función de las evaluaciones de riesgos. Estas políticas definen las pautas y procedimientos para proteger la información y los sistemas. Además, se actualizan en respuesta a cambios en el entorno o nuevas amenazas.
Implementación de medidas de seguridad	Se implementan medidas de seguridad tecnológicas y operativas basadas en las políticas y normativas establecidas. Estas medidas pueden incluir firewalls, sistemas de detección de intrusiones, sistemas de respaldo

	de datos y procedimientos de autenticación sólida.
Educación y concientización	Las instituciones invierten en la capacitación continua de su personal y usuarios en prácticas seguras de seguridad informática. Esto ayuda a crear una cultura de seguridad y reduce los riesgos relacionados con la ingeniería social, como el phishing.
Monitoreo y detención	Se implementan sistemas de monitoreo constante para detectar actividades inusuales o sospechosas en la red y los sistemas. Estos sistemas alertan al personal de seguridad sobre posibles amenazas.
Respuestas a incidentes	Si se detecta un incidente de seguridad, la institución tiene planes de respuesta bien definidos que se activan de inmediato. Esto incluye la mitigación de daños, la recuperación de datos y la notificación de las partes interesadas, según sea necesario.
Actualizaciones continuas	La institución mantiene sus sistemas y software actualizados con los últimos parches

	de seguridad para mitigar las vulnerabilidades conocidas.
Auditorias y cumplimientos	Se realizan auditorías periódicas para evaluar la eficacia de las medidas de seguridad y garantizar el cumplimiento de las regulaciones y normativas locales e internacionales.
Recursos y presupuesto	La institución asigna recursos financieros y humanos adecuados para respaldar todas estas actividades de seguridad informática.
Comunicación externa	La institución se comunica de manera proactiva con otras organizaciones y entidades gubernamentales para mantenerse al tanto de las últimas amenazas y mejores prácticas de seguridad.
Mejora continua	Después de cada incidente o auditoría, se realizan evaluaciones para identificar áreas de mejora. Las políticas y procedimientos se ajustan en consecuencia, y se inicia un ciclo de mejora continua.

Fuentes del autor.

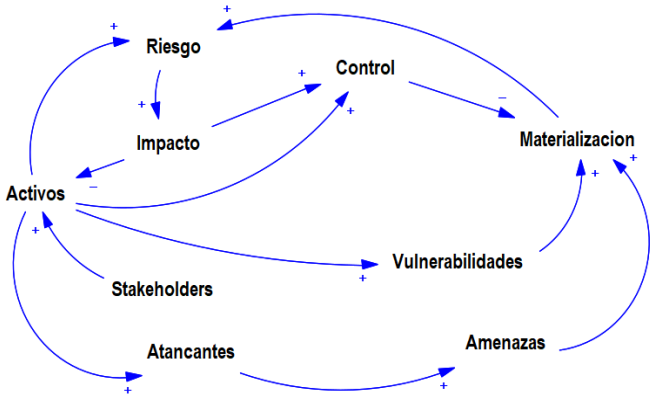
Parada et al., (2018). Los autores presentan la propuesta de un modelo que permite medir la seguridad de la información relacionando la complejidad de los diferentes elementos involucrados, presentando como resultado que los controles juegan un papel fundamental en la valoración de los activos, en un escenario sin controles se puede apreciar la materialización del riesgo de los activos.

Consideran que la seguridad está compuesta de siete elementos fundamentales: los interesados, los activos, las vulnerabilidades, el riesgo, los controles, las amenazas y los agentes de amenaza (atacantes o intrusos).

El presente artículo contribuye a la tesis puesto muestra la interacción entre los diferentes elementos que involucran a la seguridad (Figura 2). Mencionan cinco bucles:

1. Activos – Atacantes – Amenazas – Materialización – Riesgo – Impacto – Activos;
2. Activos – Vulnerabilidades – Materialización – Riesgo – Impacto – Activos;
3. Activos – Riesgo – Impacto – Activo;
4. Activos – Controles – Materialización – Riesgo – Impacto – Activos;
5. Riesgo – Impacto – Controles – Materialización – Riesgo.

Figura 2: Diagrama de influencias de los componentes de seguridad.



Fuente: Adaptado de Parada et al., (2018).

Para Palacaio, A. (2017). Las cifras de ataque obligan a tomar medidas para la protección de las diferentes empresas, dentro de las más básicas de pueden encontrar:

1. **Sensibilización y capacitación de empleados.** Uno de los principales riesgos para la información de las empresas son las prácticas descuidadas de sus trabajadores al usar Internet. Estas prácticas incluyen abrir correos electrónicos con programas malintencionados, uso de Wifi libre que puede comprometer la transferencia de información e incluso la pérdida de dispositivos de almacenamiento, teléfonos inteligentes o tabletas que contienen información relevante o claves de acceso de la empresa. Por esto es importante sensibilizarlos y capacitarlos

sobre buenas prácticas en el uso de Internet y dispositivos. (Palacaio, A., 2017)

2. **Contar con un servidor propio.** Es recomendable si en la empresa se usan más de cinco computadoras, ya que disminuye el riesgo de pérdida de archivos. (Palacaio, A., 2017)

Teniendo en cuenta lo descrito por Guevara R., Gómez S., y Sepúlveda, J. (2017) en el texto Formación profesional en el campo de la seguridad informática, a los componentes que se deben destacar son:

1. **Componente gestión de información**, según la cual se debe:

   Suministrar todos los conocimientos necesarios para conducir al especialista en seguridad de la información, a comprender de una forma estructurada como se hace la gestión de la seguridad de la información, aplicando estándares internacionales de Sistemas de Gestión de la Seguridad de la Información (SGSI), tales como los pertenecientes a la familia ISO 27001 (ICONTEC, 2006). (Guevara R., Gómez S., y Sepúlveda, J., 2017).

2. **Componente seguridad a nivel ofensivo**, este componente determina que:

> Todos los conceptos relacionados con las técnicas y herramientas usadas por los atacantes informáticos se verán de forma secuencial y ordenada, aplicando metodologías y estándares de auditorías de seguridad del tipo Hacking Ético y/o PenetrationTesting en sistemas, redes informáticas y dispositivos móviles, donde de forma secuencial se aplican todas las fases de una auditoria de seguridad ética y ejecutada por profesionales de la seguridad de la información. (Guevara R., Gómez S., y Sepúlveda, J., 2017).

Cabe resaltar que los profesionales deben estar en constantes capacitaciones, dado que, cada día surgen formas nuevas de realizar ataques a los sistemas.

Teniendo en cuenta los objetivos del trabajo a realizar, es diseñar una hipótesis dinámica con la que explique el comportamiento de los componentes de seguridad informática en las IES en Colombia.

8.1. Identificación de las variables en base a los componentes de la seguridad informática que pueden interactuar en un modelo dinámico

En la siguiente Tabla 2, se puede distinguir las variables identificadas para diseñar el modelo acorde a los controles de Seguridad de la Información que maneja con

Seguridad Informática, esto servirá de base para la elaboración del modelo cualitativo.

Tabla 3. Tabla de variables identificadas para el modelo.

VARIABLES	DESCRIPCION DE LA VARIABLE
Vulnerabilidades	Debilidades o errores en el software, hardware o en la configuración de un sistema que pueden ser explotados por atacantes para comprometer la integridad, disponibilidad o confidencialidad de la información que procesa un sistema.
Ataques	Intento deliberado de dañar o interrumpir un sistema informático o una red.
Alertas de Seguridad	Aviso emitido por un proveedor de seguridad informática, como una empresa de ciberseguridad o un organismo gubernamental, para informar sobre situaciones concretas en las que existen amenazas al acceder a una red o dispositivo.
Control	Salvaguardia o contramedida, medio de gestión de riesgos.

Vulnerabilidades mitigadas	Vulnerabilidades a las cuales se han aplicado controles.
Total de ataques	Resultado de varias acciones reactivas de un equipo de seguridad, acumulativo.
Ataques mitigados	Resultado de controles de equipos de seguridad y buenas prácticas.
Flujo de alertas de seguridad	Alertas de los equipos de seguridad y cómputo.
Alertas remediadas	Alertas que han sido controladas.
Nivel de capacidad	Valor obtenido por el Cobit 5.
Probabilidad de ataque	Grado de ocurrencia de un ataque.
Tasa de ataques mitigados	Porcentaje de ataques que mitigan los equipos de seguridad.
Planificación del cumplimiento de políticas	Número de políticas que se pretende cumplir.
Tasa de incumplimiento del control	Numero de incumplimiento del control.
Tasa de alertas de seguridad confirmadas	Numero de alertas que son por falsos dispositivos.
Tasa de remediación de alertas de seguridad confirmadas	Porcentaje de remediación de alertas que no son por falsos dispositivos.

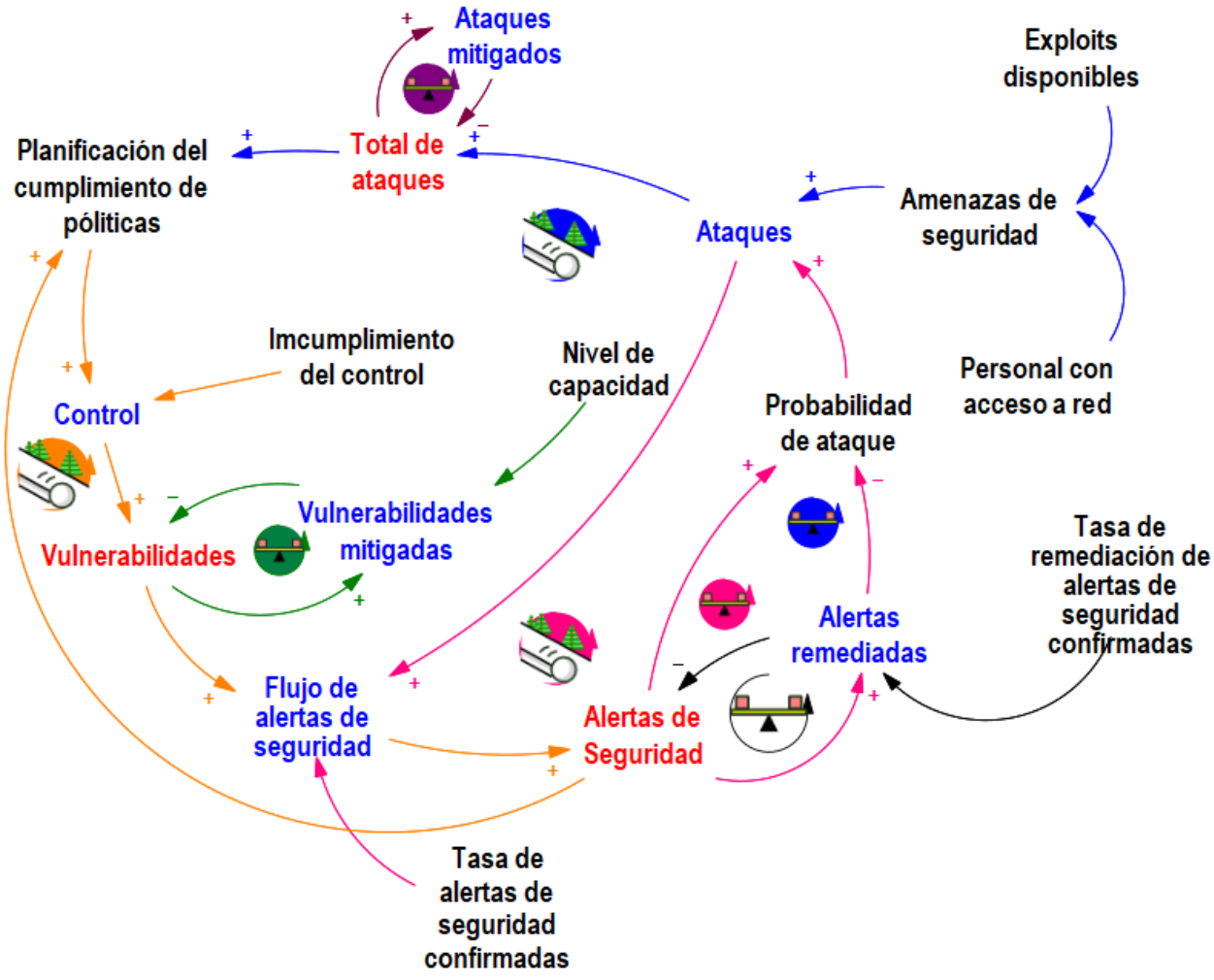
Personal con acceso a red	Número del personal con autorización a red.
Exploits disponibles	Uso de vulnerabilidades aprovechadas por atacantes.
Amenazas de seguridad	Elemento que es capaz de producir daño a un activo.

Fuente: adaptado de Cáceda, C. Rodríguez, R (2021).

Las variables de color rojo son variables de nivel, las de color azul son variables de flujo y las de color negro son variables auxiliares. (Figura 3). Además, se asume que las IES cuentan con equipos de seguridad para protegerse de los diferentes ataques. En base a los indicadores definidos anteriormente, se plantea el siguiente diagrama causal (se muestra en la Figura 3).

8.2. Modelo dinamico causal del comportamiento de los componentes de la seguridad informatica en las IES.

Figura 3. Modelo causal de variables



Fuente de: Cáceda, C. Rodríguez, R (2021)

Bucle 1: Reforzador

Ataques - Flujo de alertas de seguridad - Alertas de seguridad - Probabilidad de ataques – Ataques.

En el modelo causal Figura 3, podemos apreciar el bucle causando un efecto de un ataque se genera una alerta de seguridad, entonces a mayor cantidad de ataques tenemos más alertas de seguridad; pero estas alertas no son solo reactivas, también pueden ser preventivas, como una actualización de versión, entonces el flujo de alertas de seguridad viene influenciado por dos variables, los ataques (reactivo) y las vulnerabilidades existentes (preventivo), sabemos que en las áreas de seguridad informática se tienen también alertas por falsos dispositivos, que son falsas alertas que brindan los equipos de seguridad y generan inversión de tiempo por parte de los encargados.

Bucle 2: Balanceador 

Ataques - Flujo de alertas de seguridad - Alertas de seguridad - Alertas remediadas - Probabilidad de ataques – Ataques.

En la Figura 3, así como en el bucle anterior se explicó que a mayor cantidad de ataques generan mayor flujo de alertas de seguridad y esta mayor cantidad de alertas de seguridad, que pueden ser remediadas, si son remediadas reducen la probabilidad de que se dé un ataque, por lo tanto, hay menor cantidad de ataques.

Bucle 3: Balanceador 

Alertas de seguridad - Alertas remediadas - Alertas de seguridad

En la Figura 3, podemos observar que a mayor cantidad de alertas de seguridad aumentan la cantidad de alertas remediadas (se asume que se tiene mecanismos para remediar una alerta) y a mayor cantidad de alertas remediadas reducen las alertas de seguridad.

Bucle 4: Balanceador 

Total de ataques - Ataques mitigados - Total de ataques

Como se muestra en la Figura 3, podemos observar que a mayor cantidad de ataques se incrementan los ataques mitigados por los controles de los dispositivos, estos ataques mitigados reducen el total de ataques que tienen las instituciones, mas no el flujo de ataques, ya que los ataques se mitigan con controles, entonces para la cantidad de ataques que no han sido mitigados, se va a planificar controles (planificación del cumplimiento de políticas).

Bucle 5: Reforzador 

Ataques - Total de ataques - Planificación del cumplimiento de políticas - Control - Vulnerabilidades - Flujo de alertas de seguridad - Alertas de seguridad - Probabilidad de ataque – Ataques

En la Figura 3, vemos que los ataques incrementan el total de ataques y para los que no han sido mitigados se realiza la planificación del cumplimiento de políticas, esta planificación incrementa el control; pero que pasa si hay incumplimiento de los controles, entonces se incrementan las vulnerabilidades y a mayor cantidad de vulnerabilidades se tiene mayor flujo de alertas de seguridad, que incrementa la cantidad de alertas de seguridad y si no han sido remediadas hay mayor probabilidad de que ocurra un ataque y esto incrementa los ataques.

Bucle 6: Balanceador 

Ataques - Total de ataques - Planificación del cumplimiento de políticas - Control - Vulnerabilidades - Flujo de alertas de seguridad - Alertas de seguridad - Alertas remedidas - Probabilidad de ataque – Ataques.

En la Figura 3 se puede observar que como se mencionó anteriormente del flujo de ataques que incrementa el total de ataques, estos incrementan la planificación de cumplimiento de políticas que a su vez aumentan el control; pero si hay incumplimiento de los controles entonces hay más vulnerabilidades y a mayor

cantidad de vulnerabilidades se tiene mayor cantidad de alertas de seguridad, estas a su vez aumentan la cantidad de alertas remediadas y a mayor cantidad de alertas remedidas reducen la probabilidad de que ocurra un ataque y esto disminuye la cantidad de ataques.

Bucle 7: Reforzador 

Planificación del cumplimiento de políticas - Control-Vulnerabilidades - Flujo de alertas de seguridad - Alertas de seguridad - Planificación del cumplimiento de políticas.

En el bucle anterior se vio que a mayor planificación de cumplimento de políticas se incrementa el control; pero si hay incumplimiento de los controles entonces incrementan las vulnerabilidades y a mayor cantidad de vulnerabilidades se tiene mayor cantidad de alertas de seguridad que si no son remediadas es porque los controles tienen vulnerabilidades que conducen a la planificación del cumplimiento de políticas.

Bucle 8: Balanceador 

Vulnerabilidades - Vulnerabilidades mitigadas – Vulnerabilidades.

Las vulnerabilidades incrementan y su ves las vulnerabilidades mitigadas se ven en aumento, estas vulnerabilidades mitigadas se ven influenciadas por el nivel de capacidad que nos ayuda a mitigar las vulnerabilidades (a mayor nivel de capacidad tengo menos vulnerabilidades).

En la Figura 4 se puede apreciar que las vulnerabilidades propician más alertas de seguridad y si actuamos de una manera preventiva con controles entonces tenemos más vulnerabilidades mitigadas.

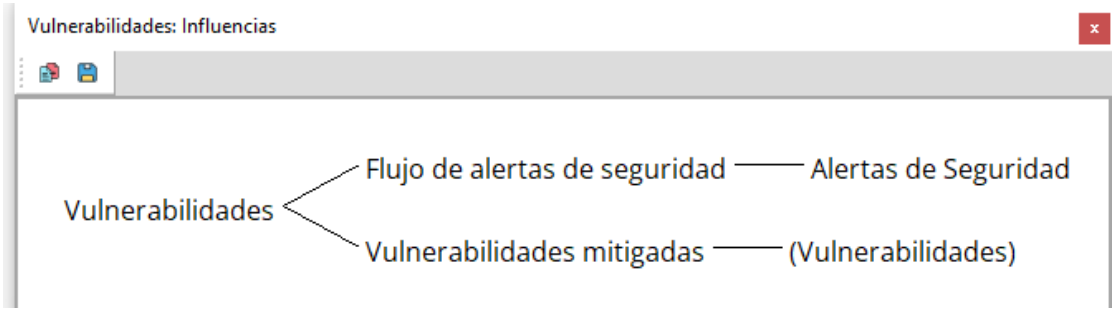


Figura 4. Influencia de las vulnerabilidades.

En la Figura 4 se puede apreciar que aquellos ataques que llegan afectar las IES, es decir si los equipos no estuvieron configurados correctamente o no los detectaron, conducen a la planificación de nuevas políticas en la organización, de manera que el sistema de seguridad actúe de una forma eficiente para la siguiente vez, en cambio si los equipos actúan correctamente protegiendo la infraestructura,

por ciertos patrones, los ataques van a ser mitigados inmediatamente san detectados.

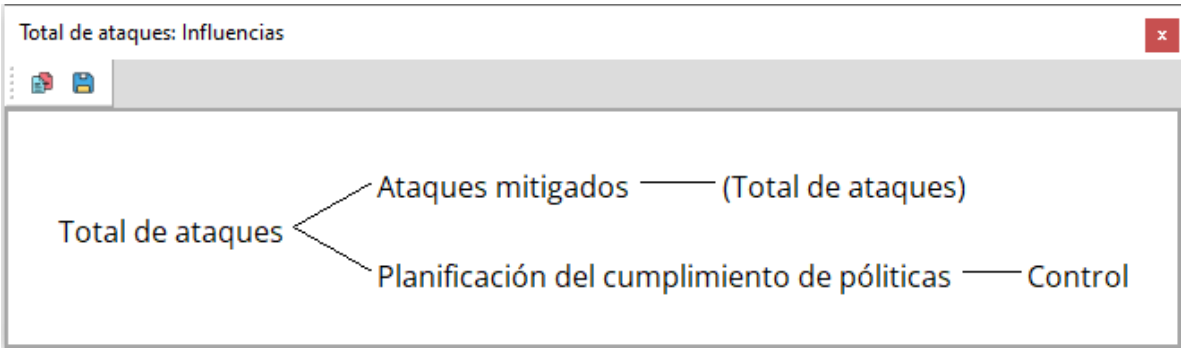


Figura 5. Influencia de ataques.

En la Figura 6 se toma en cuenta un aspecto muy importante, sabemos los ataques conducen a las alertas de seguridad en los equipos y esto hace más vulnerable las IES, entonces [Un mayor número de vulnerabilidades obviamente conduce a un inminente ataque, al igual que la falta de monitoreo o contramedidas.

Si la organización tiene alertas de seguridad que no han sido remediadas, estas conducen a la planificación del cumplimiento de políticas, a su vez si tienen más alertas y actúan preventivamente estas serán remediadas. Las alertas remediadas reducen las alertas de seguridad e influyen en la probabilidad inminente de ataque.

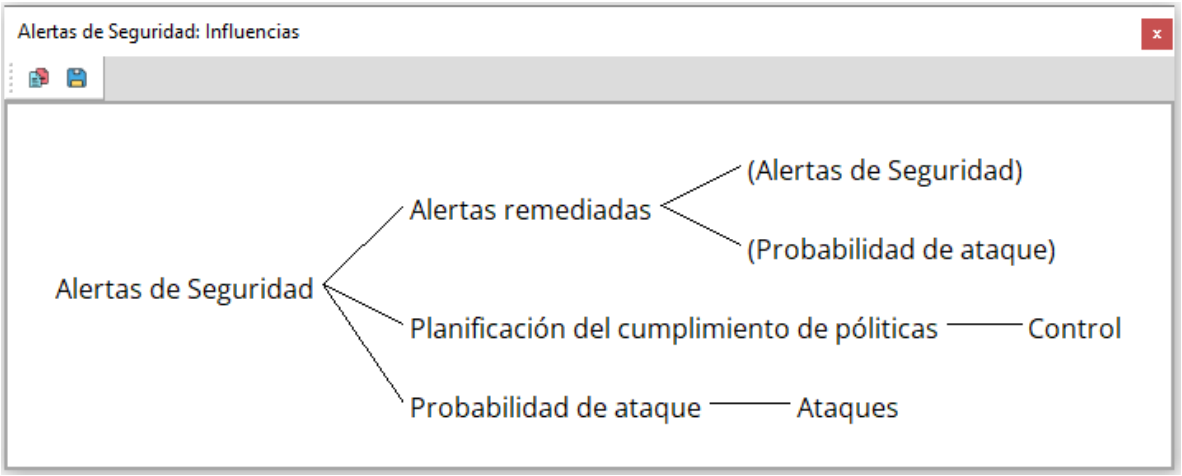


Figura 6. Influencia de las alertas de seguridad.

8.3. Estrategias que se deben implementar dentro de las IES para una mayor seguridad del sistema son las siguientes:

- No abrir los correos electrónicos de dudosa procedencia
- El Reducir el número de cuentas con privilegios de administrador y de ejecución de macros
- Actualizar el software automáticamente
- Filtrar los archivos adjuntos ejecutables en los mensajes de correos electrónicos
- Implementar líneas de defensa con AntiPhishing, Awarenes, Firewalls, Antivirus, Soluciones Antiransomware y capacitación al personal
- Reducir al máximo de compartir carpetas

- Capacitar a los empleados en temas de seguridad (prevención contra el Phishing, los Awarenes, el ransomware, la ingeniería social)
- Backups de los datos de manera periódica
- Configurar las extensiones ocultas en los archivos
- Restaurar el sistema para volver a un estado previo conocido sin infecciones
- Deshabilitar los archivos que se ejecuten desde las carpetas APPData y LocalAppData

Por otra parte, dentro de los objetivos se proponer una política que ayude al mejoramiento de la eficacia de los componentes de la seguridad informática en las IES a nivel nacional como una medida preventiva. En lo que respecta a las IES, cuentan con una política general de seguridad de la información, la cual establece que:

Esta política de alto nivel aborda la necesidad de proteger la información de la organización contra posibles amenazas y riesgos de seguridad. La política general de seguridad de la información se basa en el análisis de riesgos y establece medidas de seguridad necesarias para proteger la información de las instituciones. A continuación, se presentan algunos aspectos que se deben tener en cuenta al elaborar una política general de seguridad de la información. Política de Seguridad de la Información (2022):

- ✓ Definir el alcance de la política, es decir, a qué activos de información, procesos y personas se aplica.
- ✓ Establecer los objetivos y principios de la política, así como los roles y responsabilidades de los diferentes actores involucrados.
- ✓ Identificar los riesgos y amenazas a los que está expuesta la información de las instituciones y definir las medidas de seguridad necesarias para mitigarlos.
- ✓ Definir los procedimientos y controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información.
- ✓ Establecer los mecanismos de supervisión y seguimiento para garantizar el cumplimiento de la política y su efectividad en la protección de la información.

8.4. Política de Seguridad Informática en Instituciones de Educación Superior

Objetivo: Mejorar la eficacia de la seguridad informática en las IES a nivel nacional, protegiendo la integridad, confidencialidad y disponibilidad de la información y sistemas críticos.

Marco Normativo y Regulatorio:

Establecer un marco normativo y regulatorio claro y actualizado para la seguridad informática en las IES, en línea con las regulaciones nacionales e internacionales.

Gestión de Riesgos:

- Exigir que todas las IES realicen evaluaciones periódicas de riesgos y amenazas a la seguridad informática.
- Promover la implementación de planes de mitigación de riesgos y la asignación de recursos adecuados para abordar los riesgos identificados.

Cooperación y Colaboración:

- Facilitar la colaboración entre las IES, el gobierno y el sector privado para compartir información sobre amenazas y mejores prácticas en seguridad informática.

Educación y Concienciación:

- Establecer programas de capacitación en seguridad informática para el personal de las IES y los estudiantes.
- Promover la concienciación sobre seguridad informática en toda la comunidad educativa.

Recursos y Presupuesto:

- Asegurar la asignación de recursos financieros y humanos adecuados para implementar medidas de seguridad informática efectivas en cada IES.

Auditorías y Cumplimiento:

- Exigir auditorías regulares de seguridad informática para evaluar el cumplimiento de las políticas y regulaciones.
- Establecer sanciones para las IES que no cumplan con los estándares de seguridad.

Respuesta a Incidentes:

- Definir protocolos de respuesta a incidentes de seguridad y requerir que todas las IES los implementen.
- Establecer un mecanismo de notificación de incidentes de seguridad a las autoridades pertinentes.

Investigación y Desarrollo:

- Fomentar la investigación y el desarrollo en el campo de la seguridad informática en las IES para estar a la vanguardia en la prevención de amenazas.

Evaluación y Mejora Continua:

- Establecer un ciclo de mejora continua que involucre la revisión periódica de políticas y procedimientos de seguridad informática.

Divulgación Pública:

- Fomentar la divulgación pública de buenas prácticas en seguridad informática para que las IES puedan aprender unas de otras.

Conformidad Internacional:

- Alinear la política nacional de seguridad informática en IES con estándares internacionales reconocidos para garantizar la competitividad y la colaboración global.

Responsabilidad y Transparencia:

- Establecer un punto de contacto o entidad responsable de supervisar la implementación de la política y garantizar la transparencia en la gestión de la seguridad informática.

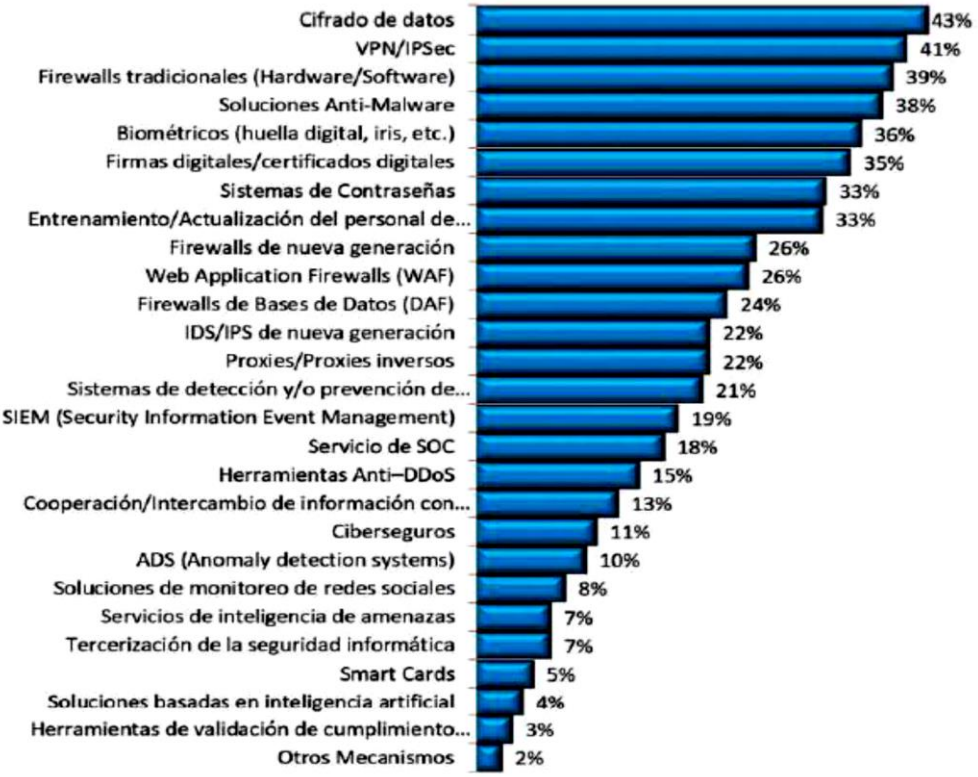
Estas políticas a nivel nacional proporcionarían un marco sólido para el mejoramiento de la seguridad informática en las IES en Colombia y promovería la cooperación entre las instituciones, el sector público y privado, y la comunidad educativa en su conjunto. La colaboración y el cumplimiento con esta política ayudarían a proteger los activos de información crítica y a mantener la integridad y calidad de la educación superior en el país.

Según un estudio, el 76% de las IES cuenta con una política de seguridad definida, pero solo el 30% cuenta con una política que incluye objetivos alineados a los objetivos de la institución. Por lo tanto, es importante que las políticas de seguridad informática se alineen con los objetivos de la institución

para garantizar su eficacia. Además, es importante que se realicen auditorías de seguridad periódicas para evaluar la eficacia de las políticas implementadas y realizar mejoras si es necesario.

Salazar et al.,(2021).

Figura 7. Mecanismos de seguridad más comunes



Fuente: Los Sistemas Ciber riesgo: el riesgo sistemático

Una vez analizada la gráfica, los 3 mecanismos más usados en la seguridad de la información son:

- Cifrados de datos con el 43%
- VPN/IPSec con el 41%

- Firewall o cortafuegos con el 39%.

9. CONCLUSIONES

Las IES en Colombia tienen cada vez mucho más interés en tener una seguridad informática eficiente, que les brinde la posibilidad de salvaguardar su información y sus datos de manera permanente. Porque de esta manera no solo estarán dando cumplimiento a la normatividad legal vigente en el país, sino que además están brindando la seguridad que requieren el personal, ya sean administrativos, docentes, estudiantes o todos aquellos que se encuentran vinculados a ellas, para de esta manera lograr mantener su información a salvo direccionando, manejando con eficiencia la información que allí se maneje.

Dentro de las investigaciones existen grupos y personas encargadas directa y exclusivamente del manejo de la seguridad informática, hecho que genera el reconocimiento de la importancia de esta y de las múltiples posibilidades de mejora que la investigación proporciona.

Las estrategias de las universidades por tener seguridad informática son similares, dado que cuentan con unas características comunes donde todas se alimentan y amparan en los elementos legales vigentes en el país.

En resumen, la seguridad informática en las IES en Colombia debe ser una prioridad para proteger los datos de los estudiantes, profesores y personal, y garantizar un entorno de aprendizaje y trabajo seguro en un mundo cada vez más digital.

Teniendo en cuenta a los autores (Parada, Flórez, & Gómez, 2018) sobre su modelo dinámico de los componentes de seguridad informática, el desarrollo, diseño y resultados obtenidos del anterior trabajo, están enfocados en los análisis desarrollados por dichos autores.

En cuanto a los análisis que se realizaron para identificar los componentes de la seguridad en las IES a nivel nacional, se basó en el modelo de Cáceda, C. Rodríguez, R (2021). En el cual se pueden distinguir las variables se identifican para diseñar dicho modelo, esto acorde a los controles de Seguridad de la Información que maneja con Seguridad Informática.

10. RECOMENDACIONES

Desde una perspectiva dinámica de sistemas se puede fomentar desde las mismas IES el estudio, análisis e investigación de la seguridad informática, para desarrollas nuevos elementos que permitan que la información y los datos se encuentren mucho más seguros. Ya que este apoyo genera que sea un trabajo cada vez más eficiente, poniendo los conocimientos de los docentes y estudiantes en favor del mejoramiento de la seguridad informática de la IES, además porque estos procesos investigativos permiten la visibilizar una labor dentro de los estudiantes, docentes y administrativos, enalteciendo la labor de los procesos realizados en este sentido.

Así mismo se pueden y se logran generar redes entre las IES que compartan experiencias respecto al tipo de vulneraciones que ha acontecido dentro de sus instituciones para generar una barrera desde las experiencias de los demás, de esta manera podría fundamentarse de una manera más contundentes con el apoyo entre todas.

La creación de una red permitirá una mayor organización en el ámbito de la seguridad informática en las instituciones de educación superior (IES). Esto se logrará al considerar los procesos y modelos de seguridad de cada institución, lo que fomentará la importancia de la seguridad informática en todas las IES. Además,

al compartir y reproducir prácticas exitosas entre las IES, se espera mejorar continuamente los procedimientos de seguridad en todas ellas.

11. REFERENCIAS BIBLIOGRÁFICAS

Aceros, V. Díaz, A. Escobar, J. García, A. Gómez, J. Olaya, C. Otero, V. (2011). ¿Cualitativo o cuantitativo? Esa no es la cuestión: un método para el desarrollo de hipótesis dinámicas. Departamento de Ingeniería Industrial, Grupo TESO, CeiBA-Complejidad, Universidad de los Andes, Bogotá. Obtenido de: http://wwwprof.uniandes.edu.co/~colaya/Metodo_ESE_dsllo_HD_Aceros_et al_DEFINITIVO.pdf

Agudelo, D. y López, Y. (2018). Dinámica de sistemas en la gestión de inventarios. Ingenierías USBMed. 9 (1). p. 75-85. obtenido de: http://www.revistas.usb.edu.co/index.php/IngUSBmed/article/view/3305/2782

Alegre, M, y Garcia-Cervigon, A. (2011). Seguridad Informática. Editorial Paraninfo, S.A. Madrid.

Aracil, J. (1997). *Dinámica de sistemas.* Alianza Universidad textos.

Arias, N. Celis, J. (2015). Modelo Experimental De Ciberseguridad Y Ciberdefensa Para Colombia. Universidad Libre Facultad De Ingeniería Programa De Ingeniería De Sistemas. Obtenido de: https://repository.unilibre.edu.co/bitstream/handle/10901/10904/TRABAJO%20DE%20GRADO%28Nicolas%20Arias%20y%20Jorge%20%20%20Celis%29.pdf?sequence=1isAllowed=y

Arellano, I. (2017). La cultura sobre seguridad informática en las redes sociales: el caso de los estudiantes de la Preparatoria de San Diego Cuentla, México. Revista Iberoamericana de las Ciencias Sociales y Humanísticas, Vol.6(11). Disponible en: https://www.redalyc.org/pdf/5039/503954319002.pdf

Arroyo, C. (2018). Implantación de un Esquema de Seguridad Informática. [Tesis]. Universidad Autónoma de Madrid, España. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/688003/Arroyo_Criado_Cilene_tfg.pdf?sequence=1&isAllowed=y

Avenía, C. (2017). Fundamentos de la seguridad Informática. Bogotá D.C., Fundación Universitaria del Área Andina. Disponible en: https://core.ac.uk/download/pdf/326424171.pdf

Bermejo, I. (2007). Seguridad informática dentro de la red de la Universidad de Sotavento. [Tesis]. Universidad Nacional Autónoma de México, México. Disponible en: http://132.248.9.195/ptd2009/agosto/0646966/0646966_A1.pdf

Bolaño, J. (2015). Implementación de políticas tipo BYOD bajo enfoque NAC basadas en software libre para la gestión de seguridad en redes de datos. [Tesis]. Universidad Autónoma de Bucaramanga, Colombia. Disponible en: https://repository.unab.edu.co/bitstream/handle/20.500.12749/3555/2015_Tesis_Bola%c3%b1o_Carracedo_Johana_Yulieth.pdf?sequence=1&isAllowed=y

Cáceda, C. (2021). *Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación.* [Tesis]. Universidad Mayor de San Marcos, Perú. Disponible en: https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/16013/Caceda_rc.pdf?sequence=3&isAllowed=y

Cairo, M., Valdés, O., Pérez, I., Portelles, R., y Sánchez, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. Revista Cubana de Ciencias Informáticas. Vol. 10(2). Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992016000200002

Candelario, J., y Rodríguez, M. (2014). Seguridad Informática en el Siglo XXI: Una perspectiva Jurídica tecnológica Enfocada hacia las organizaciones nacionales y mundiales. Universidad Nacional Abierta y a Distancia. https://doi.org/10.22490/25394088.1441

Cañon, L. (2015). Ataques informáticos, Ethical Hacking y conciencia de seguridad informática en niños. [Tesis]. Universidad Piloto de Colombia, Colombia. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2870/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Castellanos, C. (2020). Modalidades de cibercrimen en tiempos de pandemia COVID-19 en Bogotá (Colombia). [Tesis] Universidad Militar Nueva Granada. Disponible en:

https://repository.unimilitar.edu.co/bitstream/handle/10654/37304/CastellanosVegaCarlosJacinto2020_Formato.pdf?sequence=1&isAllowed=y

Castillo, S. (2013). El comercio electrónico en Mexico: Un análisis de la seguridad informática y su aspecto jurídico en las transacciones electrónicas realizadas por los consumidores. [Tesis]. Universidad Nacional Autónoma de México, México. Disponible en: http://132.248.9.195/ptd2013/Presenciales/0704798/0704798.pdf

Ochoa, S., y Cervantes, O. (2012). Contribuciones a las Ciencias Sociales. Revista Contribuciones a las Ciencias Sociales. Disponible en: https://www.eumed.net/rev/cccss/21/oocs.html

Chicaiza, P., y Díaz, A. (2014). Diseño de un plan de gestión de seguridades de la información para instituciones públicas ecuatorianas. [Tesis]. Escuela Politécnica Nacional. Quito, Ecuador.

Corredor, F. (2012). Sistema distribuido basado en inferencia para la detección de intrusiones en una red de área local. [Tesis]. Universidad Autónoma de Bucaramanga, Colombia. Disponible en: https://repository.unab.edu.co/bitstream/handle/20.500.12749/3472/2012_Tesis_Corredor_Felipe_Andres.pdf?sequence=1&isAllowed=y

Deloitte. (2020). Consideraciones de ciberseguridad en medio de una pandemia global. Deloitte. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/ar/Documents/risk/arg-2020-consideraciones-ciberseguridad-ante-pandemia-global.pdf

Duran, J. (2017). Estudio de seguridad informática de los metadatos contenidos en archivos publicados en las web de las organizaciones: Alcaldía de Pamplona, Cámara de Comercio de Pamplona, Gobernación de Norte de Santander, Diario La Opinión y la DIAN. [Tesis]. Universidad Nacional Abierta y a Distancia, Colombia. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/14449/1/91274294.pdf

Figueroa, J. Rodríguez, R. Bone, C. Saltos, J. (15 de diciembre de 2017). La seguridad informática y la seguridad de la información. Revista polo del conocimiento 2 (12). p. 145-155. Obtenido de: https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

Gamboa. J. (2022). Importancia De La Seguridad Informática Y Ciberseguridad En El Mundo Actual. Universidad Piloto de Colombia. Obtenido de: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

Gil, V., y Gil, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Revista Scientia Et Technica, 22(2). P. 193-197. Obtenido de: https://www.redalyc.org/pdf/849/84953103011.pdf

Gómez, A. (2017). Diseño de una metodología para auditar la seguridad de la información en productos de software orientados a servicios de gestión e

información en instituciones de educación superior. [Tesis]. Universidad Autónoma de Bucaramanga, Colombia . Disponible en: https://repository.unab.edu.co/bitstream/handle/20.500.12749/3441/2017_Tesis_Arelis_Gomez.pdf?sequence=8&isAllowed=y

Guevara R., Gómez S., y Sepúlveda, J. (2017). Formación profesional en el campo de la seguridad informática. Revista de reflexión y saberes 6. 34-37. Obtenido de: http://34.231.144.216/index.php/RevistaRyS/article/view/1183/1561

Gutiérrez, N. (17 de febrero de 2022). 30 estadísticas Importantes de Seguridad Informática (2022). Fundamentos de Ciberseguridad. Obtenido de: https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica#:~:text=Los%20datos%20reflejaban%20que%20m%C3%A1s,pirater%C3%ADa%20y%20corrupci%C3%B3n%20de%20datos.

Guzmán, C. Angarita, P. (2017). Protocolos Para La Mitigación De Ciberataques En El Hogar. Caso De Estudio: Estratos 3 Y 4 De La Ciudad De Bogotá. Universidad Católica De Colombia Facultad De Ingeniería Programa De Especialización En Seguridad De La Información. Obtenido de: https://repository.ucatolica.edu.co/server/api/core/bitstreams/69cddf96-2ee2-4eae-aa5a-d37357413aca/content

Hernández, S. (2019). Cultura en seguridad de la información. [Tesis]. Universidad Piloto de Colombia, Colombia. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6436/Art%

C3%ADculo_Cultura_Seguridad_de_la_Informaci%C3%B3n.pdf?sequence=1&isAllowed=y

Hilarión, F. (2017). Auditoria a la seguridad informática de los servicios de tecnologías de la información en la E.S.E Hospital San Francisco de Guachetá. [Tesis]. Universidad Nacional Abierta y a Distancia, Colombia. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/12796/1074416618.pdf?sequence=1&isAllowed=y

Hillstone, M. (04 de noviembre de 2022). ¿Por qué es importante capacitar al personal de tu empresa en seguridad informática? Hillstone networks. Obtenido de: https://www.hillstonenet.lat/blog/seguridad-de-la-red/importante-capacitar-al-personal-de-tu-empresa-en-seguridad-informatica/#:~:text=En%20ese%20sentido%2C%20la%20capacitaci%C3%B3n,los%20sistemas%20de%20la%20empresa.

Igarza, A. S., Gioia, C. V., & Eterovic, J. (2018). Análisis del Marco Normativo Legal para el ciclo de vida de la evidencia digital. RedUNCI-UNNE, 1043-1046. http://sedici.unlp.edu.ar/bitstream/handle/10915/68349/Documento_completo.pdfPDFA.pdf?sequence=1&isAllowed=y

Imbaquingo, D., Herrera-Granda, E., Herrera-Granda, I., Arciniega, S., Guamán, V., y Ortega-Bustamante, M. (2019). Evaluación de los sistemas de seguridad informáticos universitarios. Caso de estudios: sistema de evaluación docente. Revista RISTI, (E22), 349-362.

Interpol. (2020). Ciberdelincuencia: Efectos de la COVID-19. Secretaría General de la Interpol. https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

Jenab, K. and Moslehpour, S. (2016). Cyber Security Management: A Review. Business Management Dynamics, 5 (11), 16-39. Disponible en: https://www.proquest.com/openview/802a433a6f31918da532a017d563c2d4/1?pq-origsite=gscholar&cbl=2050645

Jiménez, A. (2011). myEchelon: Un sistema de Auditoría de Seguridad Informática Avanzado bajo GNU/Linux. [Tesis]. Universidad de Almeria, España. Disponible en: http://www.adminso.es/recursos/Proyectos/PFC/PFC_Alberto.pdf

Kaspersky Security Network. (2020). Desarrollo de las amenazas informáticas en el primer trimestre de 2020 Estadísticas. Disponible en: https://securelist.lat/it-threat-evolutionq1-2020-statistics/90344/

Kaspersky Security Network. (2023). ¿Qué es el cifrado de datos? Definición y explicación. Disponible en: https://latam.kaspersky.com/resource-center/definitions/encryption

Lesmes, L. (10 de abril de 2023). Colombia recibió 20.000 millones de ciberataques en 2022. El tiempo. Obtenido de: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-colombia-datos-sobre-ciberataques-en-el-pais-

757651#:~:text=De%20estos%2C%20en%20el%20caso,por%20ciento%20frente%20a%202021.

López, F. (2018). Mejoramiento de las políticas de seguridad informática en la Estación de Guardacostas Urabá. [Tesis]. Universidad Nacional Abierta y a Distancia, Colombia. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/20419/13748364.pdf?sequence=4&isAllowed=y

López, P (2010). Seguridad Informática, Madrid, España: Editorial Edix SA

Machuca, J., y Cabrera, A. (2020). Percepción de la exposición en seguridad informática de los niños y adolescentes durante la pandemia de COVID-19. Revista Polo del Conocimiento, Vol. 5(1). 37-51. Disponible: https://dialnet.unirioja.es/descarga/articulo/7659376.pdf

Mayordomo, D. (2016). Sistema adaptativo de prevención de intrusos mediante Honeypots. [Tesis]. Universidad Autónoma de Madrid, España. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/676764/Mayordomo_Trujillano_Daniel_tfg.pdf?sequence=1&isAllowed=y

Martínez, N., y Martínez, R. (2018). Los jóvenes y la ciberseguridad en zonas rurales del estado de Oaxaca. Caso: Instituto de Estudio de Bachillerato del Estado de Oaxaca (IEBO), plantel 165. Revista de Estudios de Contaduría, Administración e Informatica, Vol. 7(20). Disponible en: https://www.redalyc.org/journal/6379/637968308002/html/

Mejía, A. (2020). Caso de estudio para el análisis de vulnerabilidad y propuesta de aseguramiento de la seguridad de la información en la infraestructura tecnológica de la empresa Nostradamus S.A.S. [Tesis]. Universidad Nacional Abierta y a Distancia, Colombia. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/34626/amejiaes.pdf?sequence=1&isAllowed=y

Microsoft. (2023). Definición del control de acceso. Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-access-control

Ministerio de Educación Nacional. (2017). Convocatoria ideas para el cambio ciencia y TIC para la Paz. Disponible en: https://minciencias.gov.co/sites/default/files/upload/convocatoria/anexo_13_terminos_y_definiciones_1.pdf

Ministerio de Educación Nacional. (2023). Información Nacional 2012-2022. Disponible en: https://snies.mineducacion.gov.co/1778/articles-391286_recurso_10.xlsx

Montilla, (2020) Estado actual de la seguridad informática en las IES en Colombia IES. Universidad Nacional Abierta y a Distancia-UNAD. Obtenido de: https://repository.unad.edu.co/bitstream/handle/10596/34638/leonardo.montilla.pdf.

Moscote, R. (2017). Sistema de detección y prevención de intrusos IPS para la VLan de Servidores de la Sociedad Minera de Santander S.A.S en Bucaramanga

(Santander). [Tesis]. Universidad Nacional Abierta y a Distancia, Colombia. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/14341/1/84087203.pdf

Ojeda, J. Rincón, F. Arias, M. Daza, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia*. Cuadernos de contabilidad. 11(28). Obtenido de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Palacaio, A. (20 de abril de 2017). Las mejores medidas de Seguridad Informática. Obtenido de: https://www.teamnet.com.mx/blog/las-mejores-medidas-de-seguridad-informatica

Pantoja, J. (2017). Protocolo para la implementación de buenas prácticas de Seguridad Informática y de la Información para los usuarios en la Universidad del Valle. [Tesis]. Universidad del Valle, Colombia. Disponible en: https://bibliotecadigital.univalle.edu.co/server/api/core/bitstreams/ec163656-395d-44ae-a253-f2f7ed0ff180/content

Parada, D., Flórez, A., & Gómez, U. (2018). *Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. Obtenido de:* doi:10.4067/S0718-07642018000100027.

Peñafiel, K. (2021). Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación móvil para concientizar sobre los Impactos de los Activos. Revista Fides et Ratio. Vol. 21(21). Disponible en:

http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2021000100009

Política General De Seguridad De La Información En Las Unidades Tecnológicas De Santander. Obtenido de: https://www.uts.edu.co/sitio/wp-content/uploads/2019/11/politica_seguridad_informacion_uts.pdf

Política de Seguridad de la Información (2022). Obtenido de: https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/31_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf.

Portafolio. (31 de agosto de 2022). El 73% de las empresas en el mundo ha sufrido ciberataques. Obtenido de: https://www.portafolio.co/economia/finanzas/ciberseguridad-el-73-de-las-empresas-en-el-mundo-ha-sufrido-ciberataques-570387.

Portafolio. (12 de julio de 2022). Más de 29.000 ciberdelitos se han denunciado en 2022. Obtenido de: https://www.portafolio.co/economia/finanzas/mas-de-29-000-ciberdelitos-se-han-denunciado-en-2022-568103.

Ramirez, J. (2015). Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la Alcaldía de Pamplona -Norte de Santander. [Tesis]. Universidad Nacional Abierta y a Distancia, Colombia. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/3415/1/88030934.pdf

Rodriguez, A. (2023). Aplicativo Web para el aprendizaje de la fundamentación conceptual de seguridad informática soportada en técnica de gamificación y capture the flag. [Tesis]. Universidad Autónoma de Bucaramanga, Colombia. Disponible en: https://repository.unab.edu.co/bitstream/handle/20.500.12749/20325/Trabajo%20de%20grado.pdf?sequence=2&isAllowed=y

Romero, K. (2018). Propuesta de seguridad informática para mejorar el proceso de acceso remoto en una entidad financiera. [Tesis]. Universidad San Ignacio de Loyola, Perú. Disponible en: https://repositorio.usil.edu.pe/server/api/core/bitstreams/c10453a7-ef96-490a-b0f4-a6f27efac39e/content

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., Murillo, Á., y Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Editoria Área de Innovacion y Desarrollo, S. L., España 3ciencias. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Salazar, J., Cruz, C., Balderas, A., y Diaz, H. (2021). La Seguridad Informática en las instituciones de educación superior. Revista TECTZAPIC. Disponible en: https://www.eumed.net/es/revistas/tectzapic/vol-7-no-2-diciembre-2021/seguridad-informatica

Senge, P. M. (2006). *La Quinta Disciplina en la Práctica. Estrategias y herramientas*

Para construir la organización abierta al aprendizaje (Primera ed.). GRANICA.

Senge, P. M. (2010). *La Quinta Disciplina. El arte y la práctica de la organización abierta al aprendizaje* (Segunda ed.). GRANICA.

Solís, B., Valderrama, H., Tejedor, E., y Vásquez, D. (2023) Seguridad de los Sistemas informáticos Universitarios: Retos Pendientes. Revista Especializada de Ingeniería y Ciencias de la Tierra. Vol, 2(2). Disponible en: https://revistas.up.ac.pa/index.php/REICIT/article/view/3585

Solleiro, J. Castañón, R, Guillén, A. Hernández, T. y Solis, N. (2022). Vigilncia tecnológica en ciberseguridad. Boletín No. Universidad Nacional Autónoma de México. Obtenido de: https://www.icat.unam.mx/wp-content/uploads/2022/09/Vigilancia_Tecnologica_en_Ciberseguridad_Boletin.pdf

Tirado, N., Ramos, D., Leuvany, E., Morales, Á., y Carreño, S. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. Revista Publicando, Vol. 4(10), 462-473. Disponible en: https://revistapublicando.org/revista/index.php/crv/article/view/367/pdf_332

UNESCO. (2019). Educación Superior. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Disponible en: https://siteal.iiep.unesco.org/sites/default/files/sit_informe_pdfs/siteal_educacion_superior_20190525.pdf

Vaca, P. (2019). Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles en los distritos de educación del Ecuador. [Tesis]. Universidad Tecnica de Ambato, Ecuador. Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/30565/1/Tesis_t1650msi.pdf

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

Villamil, J., y Sarmiento, M. (2021). Diseño de un sistema de gestión de seguridad de la información en los procesos de laboratorio investigación e ingeniería en la empresa Bio D.S.A. bajo lineamiento de la norma ISO/IEC 27001: 2013. [Tesis]. Universidad Piloto de Colombia, Colombia. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/10036/TRABAJO%20FINAL%20SGSI%20BIO%20S.A.%202021.pdf?sequence=1&isAllowed=y

Zuñiga, A., Jalón, E., Andrade, M., Giler, J. (2021). Análisis de seguridad informática en entornos virtuales de la universidad Regional Autónoma de Los Andes extensión Quevedo en tiempos de Covid-19. Revista Universidad y Sociedad, Vol. 13(3), 454-459. Disponible en: http://scielo.sld.cu/pdf/rus/v13n3/2218-3620-rus-13-03-454.pdf

Leyes Informáticas Colombianas (2018).

Colombia, C. d. (18 de agosto de 1999). Ley 527 de 1999.

Colombia, C. d. (19 de junio de 2019). Ley 1266 de 2008.

Senado, S. d. (13 de mayo de 2019). Ley 1273 de 2009.

Mintic, (29 de junio de 2019) Ley 1341 de 2009.

Colombia, C. d. (27 de julio de 2000). Ley 603 de 2000.

Colombia, C. d. (15 de junio de 2019). Ley 1581 de 2012.

Colombia, C. d. (26 7 de junio de 2013) Ley 1377 de 2013.

J.M. Salazar Mata C. Cruz Navarro A. V. Balderas Sánchez H. F. Díaz Uribe (2021). COMPUTER SECURITY IN HIGHER EDUCATION INSTITUTIONS. Obtenido de: https://dialnet.unirioja.es/descarga/articulo/8524233.pdf.

CANO M., J. J. (junio de 2019). *Ciberseguridad y ciberdefensa: Retos y perspectivas en un mundo digital.*