Estado actual de la seguridad informática en las instituciones de educación superior en Colombia IES.

Leonardo Montilla Malaver

Universidad Nacional Abierta y a Distancia-UNAD
Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI
Programa Especialización en Seguridad Informática
CCAV Dosquebradas
2020

Estado actual de la seguridad informática en las instituciones de educación superior en Colombia IES.

Trabajo de grado como requisito para optar al título de especialista en seguridad informática

Leonardo Montilla Malaver

Director de trabajo de grado
Ing Edgar López MSc

Universidad Nacional Abierta y a Distancia-UNAD
Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI
Programa Especialización en Seguridad Informática
CCAV Dosquebradas
2020

NOTAS DE ACEPTACIÓN

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Dosquebradas, mayo de 2020

Agradecimientos

Gracias a Dios quien me ha ayudado a lo largo de mi vida, A mis Padres Leonel y Gladys por su apoyo y afecto, A mi incondicional Directora Dra. Edith María González y su familia, A Lina María García, mis tutores, Compañeros y docentes de la UNAD y a todos los amigos y demás personas que después de tanto esfuerzo hicieron posible la obtención de tan anhelado triunfo

CONTENIDO

LISTA DE TABLAS

Listado de Figuras

Listado de Gráficos

LISTA DE ANEXOS

GLOSARIO

ATAQUE ACTIVO: Son ataques a través de acciones directas que pretenden penetrar la infraestructura y también establecerse dentro de ella de forma permanente con el objetivo de sabotear o desplegar malware a fin de ejercer algún tipo de espionaje o secuestrar equipos con objetivos contra terceros.

ATAQUE PASIVO: Se refiere al proceso de monitorización del sujeto atacado es una forma no invasiva que puede no afectar a los equipos sin embargo puede afectar a la información por cuanto la puede monitorear y que en algunos casos es información pública. Como contraataque para este tipo de ataque se utilizan técnicas de monitoreo de tráfico buscando documentos, contraseñas denominados OSINT. Este tipo de ataques tienen el objetivo de conseguir información que más adelante puede ser utilizada en un ataque activo, es por esto que la importancia de detectar un ataque pasivo puede alertar al usuario para prevenir otros ataques más profundos o activos.

CANALES CUBIERTOS: pertenecen a canales de comunicación que permiten a un proceso transferir información de firma que vulnera la seguridad del sistema.

CRACKERS: Es la persona que pretende tener acceso a los recursos de red y su intención es delictiva.

CURIOSOS: Son los atacantes juntos con los Crackers los que más se dan en un sistema.

EMPLEADOS ACTIVOS: En ocasiones no se tiene en cuenta que las personas de la organización o personas ajenas a ella pueden estar involucradas en la estructura informática y comprometer la seguridad del sistema.

ERM: Enterprise Risk Management (Gestión de riesgos empresariales) el es proceso de planificación, organización, liderazgo y control de las actividades, con el fin de minimizar los efectos del riesgo en el capital de las ganancias de una organización

EXEMPLEADOS: Como ya se dijo pueden ser exempleados descontento**s** con la empresa y que además conocen el sistema y sus debilidades, y así pueden insertar troyanos, y demás virus o se conectan como si aun trabajaran en el sistema.

GRC: Governance Risk Compliance (Riesgo de gobernanza y el cumplimiento) es la gestión ética de una organización, en donde se enfoca al **riesgo** de mitigar los obstáculos de las operaciones y **cumplimento** es al desarrollo de conformidad con las operaciones o prácticas comerciales

GUSANOS: Son programas capaces de ejecutarse y propagarse por sí mismos a través de redes, aprovechando los BUGS de los sistemas a los que se conectan para afectarlos no son fáciles de programar y su número no es muy elevado pero los daños causantes son muy graves.[1]

HACKERS: Personal no autorizado a ingresar a los sistemas o redes su intención es maliciosa, aunque no siempre ese es su objetivo

HERRAMIENTA DE SEGURIDAD: Las herramientas de seguridad que tienen un claro objetivo para mejorar la seguridad del sistema también puede ser utilizada por intrusos para obtener información de las fallas y a su vez aprovecharlas para atacar los equipos. los equipos, herramientas como NESUS, SAINT o STAN pasan de ser útiles a peligrosas cuando las utilizan crackers.

[1] Catarina, s.f.

INTRUSOS REMUNERADOS: Son personas con gran experiencia en seguridad y son remunerados para obtener secretos o información de forma ilícita o también para afectar la imagen de la organización.[2]

ISO 27005: permite recomendaciones y directrices generales para gestionar el riesgo en los SGSI

ISO 31000: es una norma internacional que ofrece las directrices y principios para gestionar el riesgo.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los sistemas de Información. Eta relacionada con el uso de los medios electrónicos, informáticos y telemáticos, que también permite minimizar los riesgos garantizando la autenticación, confidencialidad, la integridad y la disponibilidad de os sistemas de información

PUERTAS TRASERAS: Es común que los programadores inserten atajos en los sistemas de autenticación del programa, hacen parte del código de ciertos programas que no hacen ninguna función hasta que son activados y cuando son activados pueden causar perjuicios y afectación al sistema.

SARO: más conocido como Sistema de Administración de Riesgo Operativo (SARO) y es identificar, medir, controlar y monitorear el riesgo operativo asociado a los diferentes procesos al interior de Fogafin

SEGURIDAD FÍSICA: Su función primordial es lograr la protección del sistema de información mediante la utilización de limitaciones y formas de controlar físicamente el sistema evitando ataques físicos que puede provocar el hombre de forma voluntaria o accidental.

[2] Catarina, s.f.

SEGURIDAD INFORMÁTICA: Es el área del conocimiento que se dedica al diseño de normas, métodos y procedimientos que buscan conseguir un mejor. Más seguro y confiable el sistema de información. [3]

.

SEGURIDAD LÓGICA: La seguridad lógica impide la vulneración del software sus programas y datos.

SOFTWARE INCORRECTO: Pertenecen a esta clase los errores de programación denominados BUGS y los EXPLOITS que son los programas que aprovechan esos errores.

VIRUS: consiste en secuencias de código que se insertan en ficheros ejecutables denominados huésped y de esta manera cuando el archivo se ejecuta el virus también lo hace insertándose en los programas.

[3] Aguilera, López, 2010

RESUMEN

Las entidades del sector educativo en el orden profesional son las salvaguardas de la información educativa de sus estudiantes activos y egresados y propenden por optar estrategias para evitar los delitos informáticos[4] y de esta forma garantizar que la información que certifican es legítima y veraz, siendo este el objetivo primordial de las autoridades y funcionarios a cargo de la información académica de las universidades colombianas.

La información que estas entidades salvaguardan, tienen que ver con registros académicos, calificaciones, hojas de vida de docentes, programas, archivos confidenciales y por tal razón su custodia es imprescindible para el buen funcionamiento de las IES su credibilidad y prestigio está en juego, con el fin de revisar los factores que se relacionan con la seguridad de la información a este nivel, se propone una investigación documental sobre la situación actual de la seguridad informática, en el sector educativo universitario en los siguientes temas: 1) Seguridad de la información e informática, 2) seguridad física y lógica, 3) servicios de seguridad, 4) Marco legal que normaliza la seguridad informática en las entidades Colombianas y Normas ISO relacionadas, 5) evaluación del análisis de riesgos, mediante el análisis de esta temática se establecerá la situación sobre la seguridad informática en las IES y se propondrán como conclusiones y recomendaciones los ajustes a seguir en cada uno de los factores revisados.

Palabras Clave: Ciberseguridad, IES, modelos de gestión, riesgo, seguridad informática, vulnerabilidad

[4] Huarahuara, 2009

ABSTRACT

The entities of the educational sector at a professional level are the safeguards of the educational information of their active and graduated students and must opt to assume strategies to prevent and avoid computer crimes and in this way guarantee that the information they certify is legitimate and truthful. the primary objective of the authorities and officials in charge of the academic information of the Colombian public universities the information that these entities safeguard have to do with academic records, qualifications, curriculum, teachers, programs, confidential files and for this reason their custody is essential for the good functioning of the IES its credibility and prestige is at stake, in order to review the factors that relate to information security at this level, is to propose a documentary research on the current situation of computer security in the university education sector in the following topics: 1) Information and computer security, 2) physical and logical security, 3) security services, 4) Legal framework that normalizes computer security in Colombian public entities and related ISO standards, 5) evaluation of risk analysis, through the analysis of this subject will be established the situation regarding computer security in HEIs and the adjustments to be followed in each of the factors reviewed will be proposed as conclusions and recommendations.

.

Keywords: Cybersecurity, IES, management models, risk, computer security, risk

INTRODUCCIÓN

Las entidades estatales en Colombia consideran la implementación de estrategias de seguridad informática o el mejoramiento y ajuste de las ya existentes, es por esto que especialmente las entidades del sector educativo por ser las salvaguardas de la información educativa de sus estudiantes activos y egresados como archivo histórico que garantiza que la información sea legítima y corresponda a los estudiantes activos y titulados de cada universidad.

"La seguridad informática hoy día es un tema central para todos los usuarios de equipos de cómputo, ya sean de escritorio o móviles, en el hogar, en la escuela o dentro de una organización. Esto se debe a que el uso del Internet con su popularización ha traído consigo importantes riesgos de seguridad"[5].

En este sentido, la principal responsabilidad de los administradores, encargados del manejo de la seguridad de la información académica de las Universidades Colombianas, es desempeñar un rol que garantiza y acredita que dicha información sea auténtica y verdadera, fundamental en este tipo de información, debido a las necesidades observadas y evidenciadas por parte de los administradores, rectores y personal de informática de las Universidades; en consecuencia surge la necesidad de determinar modelos de gestión, que preserven y prevengan posibles vulneraciones de la información de las Instituciones de Educación Superior (IES).

Con estos antecedentes, se plantea el problema de indagación en esta monografía y se propone una reflexionar sobre la respuesta a la pregunta:

[5] Roque Hernández, Ramón Ventura y Juárez Ibarra, Carlos Manuel. Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios

¿Cuál es el estado actual de los modelos de gestión de la seguridad informática en los sistemas informáticos y procesos de información, a nivel de las instituciones de educación superior en Colombia y cómo el estudio del estado actual de la Seguridad Informática contribuye a mejorar la SI en las IES del país?

Se propone un estudio de tipo análisis documental monográfico, que permite construir una reflexión sobre la revisión de fuentes científicas y documentos existentes en torno a la temática de la seguridad informática, tipos de seguridad, análisis de riesgo y vulnerabilidad, " seguridad de acceso, seguridad de dispositivos, manejo de contraseñas y control de vulnerabilidades, entro otros, y cada uno de estos requiere un estudio, un presupuesto y una aplicación, ya sea preventiva o correctiva, sobre los temas de seguridad que se puedan encontrar"[6] y los modelos de gestión del riesgo para prevenir y fortalecer la seguridad en las IES. En este sentido, es necesario abordar conceptos relacionados con la información, tipos de información y la seguridad en términos generales desglosando aspectos como la prevención del riesgo, transferencia del riesgo, mitigación del riesgo y su aceptación, definición de seguridad de la información y seguridad informática, al igual que las implicaciones en los usuarios, la información y la infraestructura.

El marco teórico comprende temáticas relacionadas con los fundamentos de ciberseguridad, "La acelerada evolución de la convergencia tecnológica, el aumento de la densidad digital y la asimetría de la información en una sociedad cada vez más digital y tecnológicamente modificada"[7] los pilares de la seguridad que son la confidencialidad, la integridad y la disponibilidad de la información, los diversos tipos de seguridad informática; física y lógica e igualmente las amenazas y vulnerabilidad, como también, la evaluación de riesgos, de amenazas y

[6] MONSALVE-PULIDO, APONTE-NOVOA, CHAVES-TAMAYO, David Fernando. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia)2014, vol.23, n.37

[7] CANO M., ROCHA, Ciberseguridad y ciberdefensa: Retos y perspectivas en un mundo digital. *RISTI* [online]. 2019, n.32

vulnerabilidad, y en esta última la metodología para el análisis de vulnerabilidades y las herramientas usadas para este análisis. Se revisan las estrategias de seguridad y las medidas básicas para la seguridad informática y finalmente, se abordan las normatividades vigentes y aspectos legales en torno al delito informático.

1. PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Con el avance de las tecnologías y su influencia en la vida social, también han surgido los delitos informáticos, los cuales ponen en peligro al usuario que tiene acceso a una red, sea este un sujeto autónomo o una organización de educación superior. En Colombia existe una legislación acerca de los delitos informáticos: la Ley 1273 de 2009, que brinda a los usuarios un control legal sobre los incidentes que se pueden presentar y que en la actualidad son frecuentes. Esta legislación permite identificar y sancionar los delitos informáticos.

Figura No.1 Fallas de seguridad

Fuente: Sistemas CiberRiesgo: un riesgo sistematico [8]

De acuerdo con la información planteada en la figura 1, son diversos los tipos de incidentes que se suscitan en la actualidad a nivel informativo, siendo el incidente

[8] Martínez, J. J. (29 - 30 de agosto de 2019). Ciberriesgo: Un riesgo sistemático. (J. J. Martínez, Ed.) doi:10.29236/sistemas p.24

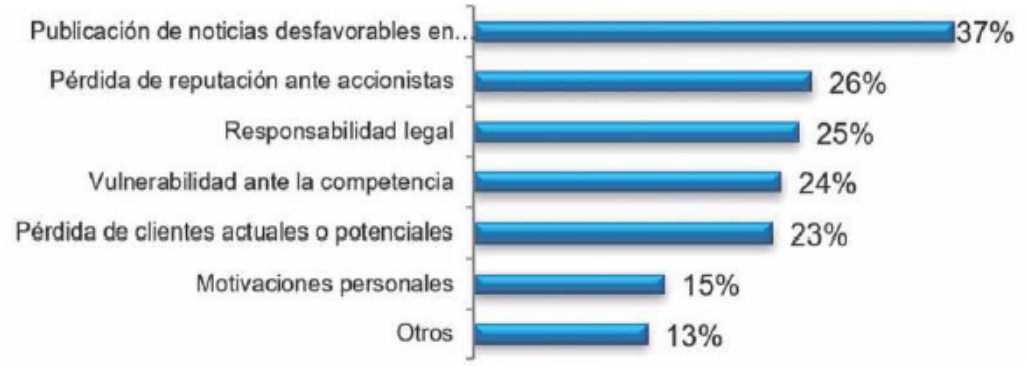
que prevale con 41% se relaciona con los errores humanos y siendo el menor con 1% Pharming; desde esta perspectiva se plantea una pregunta de investigación.

Así entonces es pertinente comprender que “La evaluación de riesgo es el proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de importancia del riesgo.

El objetivo de esta evaluación es identificar y evaluar los riesgos. Los riesgos son calculados por una combinación de valores de activos y niveles de requerimientos de seguridad”[9].

Una encuesta realizada por Ciberriesgo, en el año 2019 en Colombia se determino el motivo por el cual las entidades no denuncian los incidentes contra ataques ciberneticos, ya que esto generalia perdidas economicas debido a la perdida de la imagen, reputacion y responsabilidad

Figura No.2 Motivos para no denunciar



Fuente: Sistemas Ciberriesgo: un riesgo sistematico [10]

[9] Freitas, 2009 Vidalina. Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Enlace* [online]. 2009, vol.6, n.1

[10] Martínez, J. J. (29 - 30 de agosto de 2019). Ciberriesgo: Un riesgo sistematico. (J. J. Martínez, Ed.) doi:10.29236/sistemas p.26

1.2. PREGUNTA DE INVESTIGACIÓN

¿Cuál es el estado actual de los modelos de gestión de la seguridad informática en los sistemas informáticos y procesos de información, a nivel de las instituciones de educación superior en Colombia?

1.3. FORMULACIÓN DEL PROBLEMA

Al establecer el estado actual de la seguridad informática, en cuanto a las medidas de control implementadas, tipos de vulnerabilidad existente, y actualizaciones, además de cómo se interviene los delitos informáticos, por parte de las instituciones, en la actualidad y las estrategias de prevención que se han establecido de acuerdo con los respectivos análisis de riesgo. Así mismo y en coherencia se define como objetivo general de la investigación: Realizar una reflexión sobre la seguridad informática en las Instituciones de Educación Superior en Colombia según las políticas y estrategias de control de seguridad.

El FBI reporto en el 2018, un total de 320 universidades fueron víctimas de un ataque cibernético a nivel mundial,el cual fue atribuido a 9 iraníes que trabajan en el Cuerpo de la Guardia Revolucionaria Islámica, este ataque cibernético genero el robo 31.5 terabytes en los cuales incluye documentos y datos, investigaciones científicas, publicaciones de revistas.

Figura No.3 Irani más buscados por el FBI

Fuente FBI [11]

[11] FBI, 2018

2. JUSTIFICACIÓN

Con la inclusión de las Tecnologías de la Información y la Comunicación (TIC) a los procesos de gestión administrativa de las organizaciones, se genera la necesidad de crear, comprar y administrar sistemas de gestión para mantener la seguridad en los sistemas de información de las empresas y aun con mayor razón en las instituciones de educación superior por ser entidades que guardan la información veraz y fidedigna de los procesos académicos.

La veracidad de esta información descansa en los archivos de las diversas Instituciones de Educación Superior y es tal su importancia que estas instituciones son las únicas salvaguardas de esta información relacionada con los procesos de académicos, entre los que están, los registros de matrícula y desempeño del estudiante, los títulos profesionales, entre otros y es el acervo probatorio de que si cursaron y aprobaron los diferentes programas cada uno de los graduandos existentes, a través de la historia de cada universidad. Por tal razón se hace necesaria la aplicación de herramientas tecnológicas que permitan asegurar sistemas de gestión de seguridad informática empresarial, “La seguridad informática, de igual manera a como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada”[12] para evitar posible pérdida de información o incursiones de ciber-delincuentes o la ejecución de delitos como la violación de la información, cambios no autorizados, hackeo o robo de información con fines de estafa o suplantación y demás delitos informáticos.

[12] Gil Vera, Víctor Daniel, Gil Vera, Juan Carlos Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia Et Technica [en linea]. 2017, 22(2), 193-197[fecha de Consulta 15 de Abril de 2020]. ISSN: 0122-1701. Disponible en: https://www.redalyc.org/articulo.oa?id=84953103011

Como aporte desde la Especialización en Seguridad Informática de la Escuela de Ciencias Básicas, Tecnología e Ingeniería de la UNAD, se realiza esta reflexión, a fin de entender los modelos de gestión de la seguridad informática que aplican a la prevención y evitan el delito informático en las IES.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Establecer el estado actual de las políticas y estrategias de control de seguridad informática como la legislación y normatividad vigente dirigidas hacia las instituciones públicas de educación superior (IES).

3.2. OBJETIVOS ESPECÍFICOS

- Reconocer los Modelos de gestión de la seguridad informática en las algunas Instituciones de educación superior IES.

- Determinar las posibles causas de vulnerabilidad y el riesgo existente en los sistemas informáticos y bases de datos de las IES de las cuales se analizan los modelos de gestión de la seguridad informática.

- Proponer estrategias de mejoramiento a implementar en las IES, como medidas preventivas en primera instancia a fin de salvaguardar de forma segura las bases de datos: registros académicos, calificaciones e historia académica, procesos académicos, programas e información docente, archivos administrativos información del sistema de investigación y demás información existente

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

Con claridad es necesario comprender desde la perspectiva de los autores, elementos determinantes que permitan ejemplificar y profundizar algunos elementos que se plantean en la presente monografía, de esta manera en este apartado se plantearan elementos teóricos pertinentes que den una mayor veracidad al proceso realizado.

4.1.1. Análisis y la gestión del riesgo informático

Uno de los elementos primordiales que deben ser tenidos en cuenta son los avances de las TICS en la actualidad han obligado a los diferentes gobiernos y organizaciones públicas y privadas a buscar estrategias y mecanismos tecnológicos y humanos a fin de preservar y cuidar uno de sus más grandes e importantes activos como es la información, “La información es uno de los activos más importantes para las empresas y por lo tanto es fundamental una adecuada gestión del riesgo”.

4.1.2. Los sistemas informáticos

Otro elemento que representa el fundamento de la seguridad informática en las universidades es la gestión de riesgos se define Padilla plantea como una disciplina que existe para hacer frente a los riesgos no especulativos, que son los riesgos de los cuales solo puede ocurrir una pérdida para la organización. La gestión de riegos considera los siguientes objetivos: eliminar los riesgos, reducir a niveles “aceptables” aquellos riesgos que no se pueden eliminar entonces la opción es aceptarlos y ejercer el control respectivo o transferirlos por medio de aseguradoras a alguna otra organización[13]. (Gestión riesgo – INCIBE –MINTIC - NIST)

[13] Arévalo Moscoso, F. M., Cedillo Orellana, I. P., & Moscoso Bernal, S. A. (mayo - agosto de 2017). Metodologia agil para la Gestion de Riesgos informaticos. *Revista Killkana, 1*(2), 39-42.

Con respecto a la importancia que tiene la gestión del riesgo de los sistemas informáticos se puede decir que esta importancia radica en la protección de un activo primordial como es la información y los aspectos relacionados con esta que comprenden factores físicos o de infraestructura lo mismo que factores intangibles que están involucrados en la transmisión y recepción de datos, para Tarazona también la seguridad debe hacer referencia a proteger la seguridad de los derechos de autoría en este sentido a proteger la propiedad intelectual e información importante de organizaciones y personas.

Las amenazas y las vulnerabilidades los cuales son factores relacionados y que cuando no hacen presencia conjunta no se puede hablar de una posible consecuencia de riesgo en la información, las amenazas pueden se originan a nivel interno o externo y las vulnerabilidades hacen referencia a una debilidad tecnológica que puede estar tanto en la transmisión, procesamiento o recepción de la información[14.]

Pero para comprender la utilidad de los elementos mencionados en los párrafos anteriores, se hace completamente necesario analizar cuál es la metodología de la gestión del riesgo

El método que está destinado a determinar, analizar, valorar y clasificar el riesgo para buscar mecanismos de control del mismo riesgo a este aspecto se le denomina gestión del riesgo. Un elemento ampliamente relacionado con este tema es el concepto de activo que es un concepto abordado en los sistemas contables y en este caso se refiere a la información como un activo por su gran valor en sí mismo. Otro elemento es la amenaza que es considerada como todo aquello que puede provocar daño al activo. y la vulnerabilidad que se refiere a las inseguridades que posee el activo o información debido a problemas técnicos o a

[14] Tarazona (2007)

aspectos de procedimiento y el riesgo que es la consecuencia de que una amenaza se produzca debido a la presencia de una vulnerabilidad.

Una gestión eficiente del riesgo está relacionada con la mejora continua por cuanto es consistente con la dinámica del riesgo y que se sustenta en la necesidad de hacer presencia durante todo el proceso, y se debe evaluar la gestión del riesgo a partir de métodos, funciones y responsabilidades, las herramientas y tecnologías en la organización. Una ejecución de buenas prácticas para la gestión del riesgo tendrá como consecuencias beneficios tangibles de negocios y la presencia de un número mínimo de eventos inesperados y fracasos, así mismo se obtendrá una mejor calidad de la información, se generará mayor confianza entre las partes interesadas, se lograrán nuevas incursiones en innovación traducidas en nuevas aplicaciones.

Como estrategias más utilizadas para reducir o mitigar los riesgos se pueden contar con las siguientes:

Evitación del riesgo: Consiste en salvaguardar la información retirándose de las situaciones que causan los riesgos y atender de manera inmediata las causas o raíz que los originan.

Reducir los riesgos/ mitigación: Se refiere a medidas que se deben tomar en primera instancia identificar los riesgos y ejecutar las acciones respectivas que van dirigidas a reducir la frecuencia y el impacto del riego, mediante la aplicación de los controles respectivos. La eficiencia de la estrategia se evalúa a través de los indicadores de gestión y planes de control.

Riesgo compartido / Transferencia: Se refiere a disponer en otros una parte del riesgo de manera que se minimicen sus costos mediante el aseguramiento o la subcontratación, esto no exime a la empresa de su responsabilidad total sino que

comparte un 50% del riego pero también queda expuesta a los riesgos propios de la asegurabilidad y la subcontratación.

Aceptar el Riesgo: Consiste en consentir el hecho de que existen riesgos y se acepta la pérdida cuando esta se produzca, No se ignora el riesgo se acepta como una medida que implica que al reducirlo resulta más costoso.[15]

4.1.3. Gestión de riesgo su impacto

Es además fundamental en el camino de la presente monografía comprender que en la gestión del riesgo, su impacto se puede evidenciar en la minimización de los riesgos detectados a partir de una evaluación realizada de forma sistemática y mediante una metodología que intente, primero identificar los riesgos en la organización a través de los indicadores más objetivos posibles, en un proceso de evaluación diagnóstica y a partir de lo encontrado y evaluado tomar las decisiones más adecuadas contando con las herramientas tecnológicas e infraestructura que se posee para este fin, igualmente se cuenta con el recurso humano y su capacitación para el control y prevención de las posibles vulnerabilidades y amenazas, o en su defecto si se evidencia la presencia del riesgo real ejecutar las acciones ya referenciadas como son mitigación, compartir el riesgo o convivir con él pero enmarcándolo en unos límites aceptables que permitan un flujo adecuado de la dimensión acerca de sistemas informáticos en la empresa sin afectar de forma pronunciada su activo.

4.1.4. Evaluación del nivel de riesgos

Finalmente, después de comprender las dimensiones e importancia de los riesgos informativos, es fundamental comprender como pueden ser evaluados, ya que esto permite que se evidencie el resultado que se está obteniendo en el caso de implementarse alguna de las metodologías expuestas. Con el fin de evaluar el

[15] Fernández, L.A (2010). La gestión del Riesgo Operacional de la teoría a su aplicación. México: Limusa – Noriega Editores

riesgo se deben realizar metodologías como la de vulnerabilidad denominado igualmente test de penetración que son herramientas para evaluar y analizar el estado de seguridad a nivel de la infraestructura de la empresa.

El proceso que pretende gestionar el riesgo en una organización permite reconocer la situación actual de la seguridad y a partir de este diagnóstico se tomaran decisiones acerca de que estrategias se deben utilizar para reducir los riesgos, lo mismo que diagnosticar que estrategias debe tomar a largo y corto plazo y como resultado final establecer si las decisiones tomadas fueron las correctas o no.

En la gestión del riesgo se deben tener en cuenta cuatro factores que son:

a) La realidad actual: Se debe realizar un diagnóstico de los aspectos relacionados con la seguridad de la empresa, con el fin de entender cómo se están gestionando los activos y sus niveles de seguridad lo mismo que referir las normas utilizadas y definir cuales no se están usando así se evalúa en esta fase lo referente a la vulnerabilidad o penetración.
b) Establecer los pasos a seguir: Con base en la información detallada de la realidad de la empresa se establece un comité conformado por técnicos y funcionarios responsables de los sistemas, el área de recursos humanos y la dirección o gerencia a fin de que decidan que se debe hacer y las medidas a tomar para enfrentar los riesgos.
c) Ejecución: A partir de los estudios realizados y decisiones sigue la fase de implementación y ejecución de las estrategias que comprenden normas, procedimientos rediseños de actualización y ajustes requeridos y aprobados previamente por el comité designado.
d) Monitoreo o seguimiento: Consiste en analizar el éxito de las implementaciones realizadas, evaluar los puntos favorables y los errores

> cometidos y a partir de lo anterior se formularán nuevos diagnósticos y evaluaciones a futuro de acuerdo con las necesidades de la organización. [16]

Así con los anteriores elementos a tener en cuenta en los pasos en donde se identifican los riesgos la empresa determina los niveles de riesgo de acuerdo a los límites de riesgo normatizados por la empresa, según Mintic las fases a tener en cuenta en la guía de evaluación del riesgo se determinan como la probabilidad y su impacto, definiéndolos así: La probabilidad se refiere a la contingencia de que el riesgo ocurra, la cual se evalúa mediante indicadores de frecuencia o de factibilidad considerando aspectos internos o externos y el impacto se define como los efectos que se ocasionan a la empresa cuando el suceso o riesgo se produce realmente, con estos pasos a seguir se produce la calificación del riesgo que comprende entonces la probabilidad de que el riesgo se presente y el impacto producido por su ocurrencia.

La evaluación del riesgo según Mintic en su guía 21 de evaluación de riesgos (2018) sugiere que la evaluación se realiza de forma cualitativa y se genera mediante la comparación del análisis de la probabilidad de que ocurra el evento y su impacto y el resultado supone la demostración a través de una matriz que se denomina matriz de calificación que contiene una estimación de los riesgos y así se califican los riesgos describiendo además de la probabilidad y el impacto las zonas de riesgo y determinando las estrategias más viables para su control y tratamiento. Uno de los elementos primordiales en este aspecto es el apetito al riesgo es la cantidad de riesgo que una organización está dispuesta a asumir para alcanzar sus objetivos estratégicos.

[16] Parra Moreno, (2012)

4.1.5. Fundamentos de la Ciberseguridad

Sin duda alguna comprender cuales son los elementos que se proponen a nivel de ciberseguridad, implican observar

4.1.5.1. Los tres pilares de la Seguridad

Figura No.4 Pilares de la seguridad

Fuente: Introducción a la seguridad informática y el análisis de vulnerabilidades[17]

Los tres pilares de la seguridad se originan y sustentan en aspectos tales como el requerimiento de obtener información, la integridad de esta y la disponibilidad que se tenga de obtenerla, con el objetivo de sacar el máximo provecho con un mínimo riesgo.[18]

La seguridad está fundamentada en tres pilares como se observa en la figura 1 sin embargo puede haber otros aspectos que la fundamentan, si alguna de las dimensiones falla se perderá seguridad o usabilidad, si faltan alguna de estas la empresa o institución se verá expuesta a posibles intentos de vulneración.

[17] Romero et al (2018) p. 25
[18] Romero et al (2018) p. 25-26

4.1.5.2. Confidencialidad

Para seguridad informática “la confidencialidad se define como la guarda o protección de la información evitando su propagación sin autorización, la ausencia de confidencialidad tiene implicaciones de tipo legal y la reducción de la credibilidad”. Toda información debe estar a salvo de su divulgación no autorizada tanto a nivel personal como empresarial o información con derechos reservados de uso. [19]

Los principios relacionados con confidencialidad se destinan además de proteger la información también a la protección de datos que estén a su cargo o tengan responsabilidad sobre ellos por su carácter de confidencialidad o el alto valor que tengan para la empresa, la perdida de la confidencialidad surge cuando se producen filtraciones en las entidades bancarias o grandes empresas o Gobiernos donde quedan expuestas públicamente, algunas de sus actividades.

La confidencialidad igualmente se refiere a la acción que se describe como acceden a esta información solo el personal autorizado, usando los recursos que requiere para ejercer su tarea y así recurre a tres recursos que son:

- **Usuarios acreditados:** consiste en verificar la identificación de quien o quienes acceden a la información y si realmente son quienes dicen ser.
- **Uso de privilegios:** Se refiere a los usuarios que están autorizados para acceder a la información y solo la información o datos autorizados.
- **Cifrado de información:** “se denomina también al cifrado con el término encriptación, así mediante esta estrategia se impide que los datos sean accesibles a personal no autorizado, de esta manera la información se hace ilegible aspecto que juega tanto para quienes están autorizados como para

[19] Romero et al (2018) p. 26

quienes no lo están, solo a graves de las verdaderas y reales claves se hace posible extraer los datos que están allí guardados para su trasmisión"[20]

4.1.5.3. Integridad

Como un segundo pilar de la seguridad se menciona a la estrategia que evita que la información se pierda o se vulnere de forma voluntaria o accidental. La integridad según seguridad informática hace referencia a la forma como debe asegurarse la información para que esta no se pierda o se vea comprometida así se de forma voluntaria o involuntaria en acciones no autorizadas. [21]

También y relacionado con la seguridad es considerar la información errónea como verdadera por su impacto que es tan grave como perder la información, lo que hace que se tomen decisiones equivocadas, para contrarrestar esas fallas y lograr la integridad de la información corresponde realizar:

- Realizar seguimientos del tráfico de red a fin de determinar y detectar posibles intrusos.
- Realizar auditajes de los sistemas para implementar procesos a fin de registrar quien hace, que hace, cuando lo hace y con qué información.
- Ejecutar métodos de control a nivel de cambios de forma sencilla a fin de validar los resúmenes de los archivos guardados con el objetivo de determinar si sus cambios son correctos o existen falsificaciones etc.
- Un recurso para ejecutar y que es muy importante es realizar y mantener copias de seguridad que facilitan en caso de pérdida de la información o vulneración de la original es susceptible volver al estado inicial y recuperar la información.

[20] Romero et al (2018) p. 26
[21] Romero et al (2018) p. 26

4.1.5.4. Disponibilidad

Este factor se define como la organización está dispuesta a proporcionar los servicios y requerimientos en torno a la información y así se evitan pérdidas importantes, como la credibilidad o productividad de esta. [22]

La consideración de poseer una seguridad mínima de la información, no solo implica que quien necesite la información acceda a ella y que la use eficientemente y si el acceso se convierte en algo tedioso o casi imposible también es función a evitar, la información debe estar al alcance de quien la necesite lo que la hace útil y valiosa, de acuerdo a esto se deben tener en cuenta aspectos recomendables para facilitar su disponibilidad, con este fin se deben implementar factores de control como los que sugiere. entre otros son los siguientes:

- El acuerdo o nivel de servicio o (SLA)
- Balanceadores de carga de tráfico para minimizar el impacto del DDoS
- Copias de seguridad para restauración de información perdida.
- Disponer de recursos alternativos a los primarios[23].

A la luz de estos pilares de la Ciberseguridad, se ejemplifica con esmero la utilidad que tiene dentro de una universidad la posibilidad de aplicarlos de manera eficiente, permitiendo permear todas las áreas y de esta manera ejercer un proceso mucho más eficiente.

4.2. MARCO CONCEPTUAL

Información: "Acción que se relaciona con informar, la etimología de la palabra información deriva del sustantivo latino (informatio (-nis) y del verbo informare,

[22] Romero et al (2018) p. 27
[23] Romero et al (2018) p. 27

significa “dar forma a la mente”, “disciplinar”,”istruir”,”enseñar”, como proviene del latín la palabra informationis era se usaba para indicar un concepto o una idea” [24]

Las diferentes dimensiones de la información se dividen en los siguientes tipos de información:

Información privilegiada: Información que se caracteriza porque tienen acceso pocas personas o pueden poseer esta información antes que las demás personas a las cuales la información debe llegar.

Información Reservada: Este tipo de información se caracteriza por ser secreta.

Características de la información

Dentro de las características más notables de la información son las siguientes:

Significado: Este aspecto se relaciona con el sentido que posee una información en el cual se evalúan sus consecuencias y la comunidad a la cual llega la información adecuan sus acciones y actitudes de acuerdo con esas consecuencias que se caracterizan por ser predictores del significado de la información.

Importancia: En cuanto a la importancia de la información se enfoca a la importancia relativa al receptor: quiere decir lo anterior que la importancia e interés de la información para un receptor se refiere al grado en que este puede modificar su actitud a partir de la información recibida. Se puede evaluar la importancia de la información por el efecto que esta puede tener en cuanto a modificar las actitudes de los receptores la información que no modifica o no tiene un impacto significativo es poco importante.

[24] Diccionario de la real academia de español, 22th ed., *s.v. información.*

Vigencia: Se define esta característica por el hecho de tener la cualidad de ser reciente o relacionarse con hechos acontecidos recientemente o si es una información ya muy desactualizada por el tiempo o por su poca importancia ya no tendría vigencia.

Validez: Es un factor relacionado con una cualidad que debe tener la información cuando sale del emisor: y se refiere a la confiabilidad del emisor y si este puede suministrar información falsa o errónea. Un ejemplo actual es la gran cantidad de FAKE NEWS (noticias falsas que circulan en las redes sociales ya sea acerca de gobiernos, personas, deportistas etc.)

Valor: Se refiere a que tan útil es la información para el destinatario o receptor.

La Seguridad en términos generales

Se definen “la seguridad como la búsqueda de gestionar el riesgo en cuanto a que en este sentido la seguridad busca la gestión de riesgos en cuanto a evitarlo o prevenirlo mediante la planeación y ejecución de acciones en uno u otro caso”.

Se puede entender a la seguridad como la ausencia de riesgo, para determinar la seguridad como cualidad se enmarcan cuatro acciones que son:

- La prevención del riesgo
- La transferencia del riesgo
- La mitigación del riesgo
- La aceptación del riesgo.

Son acciones que se deben tener en cuenta en las áreas que intenten tener más y mejor autoridad.[25]

[25] Romero et al (2018) p. 13.

Seguridad de la Información: Se refiere a la seguridad de las redes y la comunicación y la búsqueda de la seguridad en los datos.

Seguridad informática: Def. Se refiere a las precauciones y protecciones que buscan evitar que algún factor o acción pueda afectar a la información [26]

Se plantea otra definición consistente en “asegurar la información en cuanto a los recursos o activos de una empresa en cuanto a que el conocimiento o la modificación de la información o el acceso a la misma sea solo posible a las personas suficientemente acreditadas y dentro de los términos de su acreditación”[27].

Seguridad informática y Seguridad de la información

Para aclarar los terminos del concepto de seguridad informática y seguridad de la información, el primer término tiene que ver con la seguridad referida al medio informático, y la seguridad de la información no solo se encarga del medio informático sino de cómo salvaguardar la información. Es tarea primordial de la seguridad informática minimizar los riesgos, que puede clasificarse desde la entrada de datos de igual manera se debe referir al medio que transporta la información y en este caso se puede referir al hardware que transmite o recibe que también es susceptible de riesgos, otros riesgos pueden provenir de los mismos usuarios y protocolos, la función principal de la seguridad informática es minimizar los riesgos y lograr eficiencia y mayor seguridad, los factores que enmarca la seguridad son los siguientes:

- ✓ **Los Clientes o usuarios**: Se puede decir que es la dimensión más débil por cuanto las personas son difíciles de controlar.

[26] Macías Valencia, 2017 Seguridad en informática: consideraciones. Revista Cientifica: Dominnio de las Ciencias

[27] Catarina, s.f Seguridad informatica - conceptos básicos

- ✓ **La información:** Esta dimensión es el factor más importante y por el cual se diseña la seguridad informática por ser el activo primordial y ser el factor de protección.

- ✓ **La infraestructura:** Dimensión que se puede controlar eficientemente, pero dependiendo de los procesos que se manejen, los riesgos más propensos a suceder en esta dimensión son accesos no facultados, falsedad en la autenticación de la identidad y otros daños como robo del equipo o los daños debidos a desastres naturales[28]

4.3. MARCO HISTÓRICO

4.3.1. Contexto de los delitos informáticos

Para comprender el referente legal de los procesos relacionados en la presente monografía es precio mencionar que algunos autores plantean que con los sistemas informáticos pasan cosas y situaciones muy parecidas a las que pasan con la historia ya que los sujetos se interesan cada vez más por la informática, debido a su grandioso desarrollo y a la importante fuerza que tiene en el desarrollo de las actividades cotidianas.

No hay actualmente muchas personas que no utilicen elementos informáticos o de cómputo en el desarrollo de su vida cotidiana, lo que demuestra con claridad el alcance y el impacto que tiene en el planeta entero, convirtiéndose en una herramienta fundamental para el ser humano. Igualmente ese desarrollo venía acompañado de ciertos riesgos, ya en 1980 la Arpanet (AdvancedResearch Project Agency Network) creadora de la internet documentó que en su red se emitieron extraños mensajes que aparecían y desaparecían de forma aleatoria y que algunos códigos ejecutables de los programas usados sufrían una extraña mutación, en ese momento los hechos no pudieron comprenderse pero los

[28] Romero et al (2018) p. 14

técnicos altamente calificados del pentágono usaron un antivirus para solucionar esos problemas. Trend Micro. Desde este momento se inicia el desarrollo de programas y estrategias a fin de contrarrestar la vulnerabilidad de los sistemas de información y asegurar la legitimidad y salvaguardar la información en Colombia este proceso fue más lento y hasta la expedición de las Leyes 599 del 24 de julio de 2000 y 1273 del 5 de enero de 2009 se dieron herramientas jurídicas y legales para intervenir el delito informático en Colombia [29]

En el desarrollo del contexto es importante mencionar que por ejemplo La Universidad Nacional Australiana (ANU, siglas en inglés) informó el 04 de junio de 2019 que fue víctima de un ataque masivo de sus sistemas, en el que los piratas informáticos accedieron a información personal de las últimas dos décadas. Los ciberpiratas accedieron a los nombres, direcciones, fechas de nacimiento, contactos personales, información salarial, cuentas de bancos y pasaportes, así como los registros académicos de estudiantes, según la ANU.

España, Taiwan, Rusia, Portugal, Ucrania, Turquía y Reino Unido, fueron víctimas de uno de los ataques cibernéticos más agresivos de toda la historia. Un virus tipo 'ransomware' llamado 'WannaCry', en diciembre de 2017, viéndose afectadas diferentes organizaciones, donde no solo perdieron información valiosa sino que además fue expuesta información privada que los usuarios tenían en las plataformas.

4.4. MARCO TECNOLÓGICO

Son diversos los espacios en los que la seguridad informática son aplicados, en tanto como se evidencia con el auge de la sociedad del conocimiento, cada vez más son los espacios en donde debe ser aplicada, encaminar el desarrollo

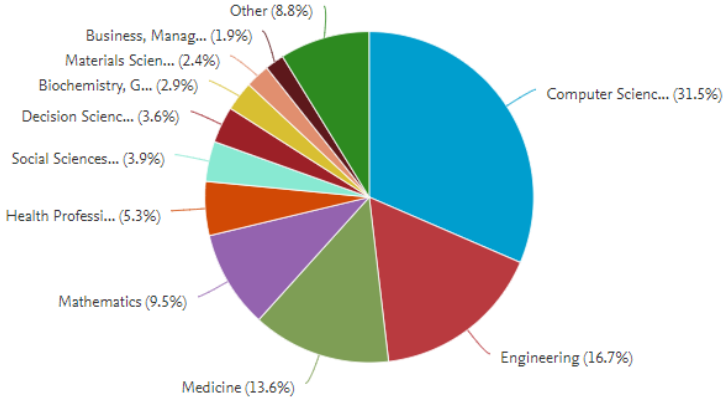
[29] Ojeda Pérez, Rincón Rodríguez, Arias Flórez, & Daza Martínez, 2010

tecnológico en esta dirección es uno de los elementos más relevantes de la vanguardia.

4.4.1. La seguridad informática por áreas de aplicación

Grafica No. 1 Se observan las diferentes áreas donde la seguridad informatica esta siendo aplicada para la seguridad de la informacion y prevención en la vulneracion de los datos, observando en ella que no solo es en los procesos de ingenieria en donde se esta desarrollando la seguridad informatica, ahora en los negocios, la medicina, las ciencias sociales y en general en todos los proceso academicos dandole la pertinencia a la presente monografia, el analisis de consulta es del año 1976 al primer trimestre 2020

Grafica No. 1 Áreas profesionales con estudios en seguridad Informática

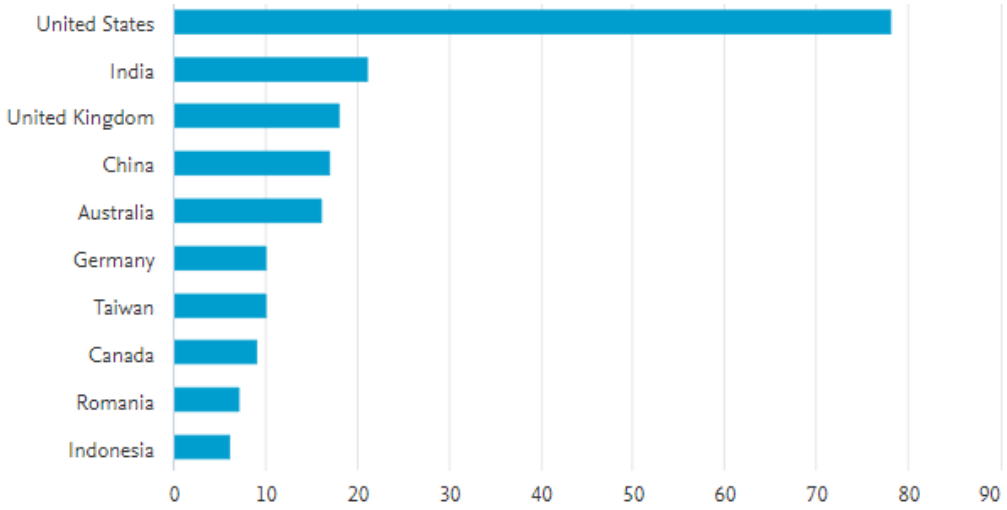


Fuente: Herramientas para extraer y analizar índices de impacto (Scopus) [30]

Los documentos publicados en idioma inglés, el país que lleva la delantera es Estados Unidos, seguido de la India, según estos datos es claro que la investigación

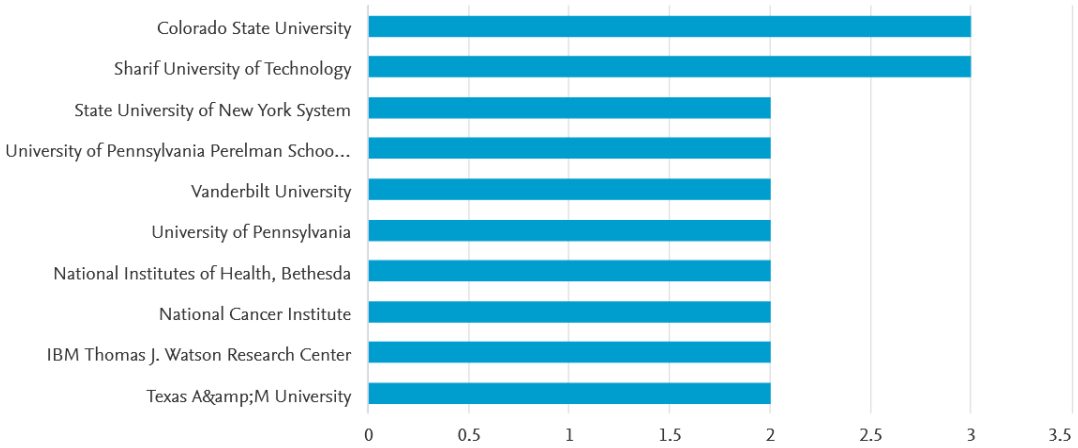
[30] Scopus, Area por Profesion, 2020

Grafica No. 2 Publicaciones en seguridad informática de acuerdo con los 10 países con mayor número de investigaciones



Fuente: Herramientas para extraer y analizar índices de impacto [31]

Grafica No. 3 Publicaciones en Universidades de los Estados Unidos corresposndiente al periodo 2015 al 2020 primer periodo



Fuente Herramientas para extraer y analizar índices de impacto [32]

[31] Scopus, Publicaciones en Seguridad Informatica, 2020
[32] Scopus, Publicaciones de Universidades de Estados Unidos, 2020

4.5. MARCO LEGAL Y NORMATIVIDAD

Leyes Informáticas Colombianas 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. [33].

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[34].

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[35].

LEY 1341 DEL 30 DE JULIO DE 2009: Donde se encuentran principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.[36].

[33] Colombia, C. d. (18 de agosto de 199). Ley 527 de 1999.
[34] Colombia, C. d. (19 de junio de 2019). Ley 1266 de 2008.
[35] Senado, S. d. (13 de mayo de 2019). Ley 1273 de 2009
[36] Mintic, (29 de junio de 2019) Ley 1341 de 2009

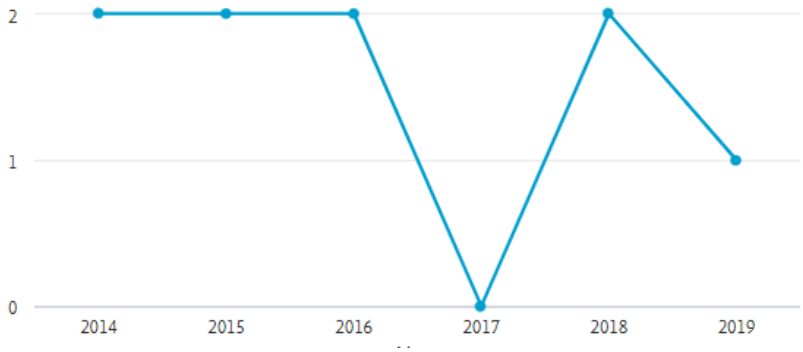
LEY 603 DEL 27 JULIO DE 2000: Modifica el artículo 47 de la ley 222 de 1995[37].
LEY 1581 DEL 17 OCTUBRE DE 2012: Esta Ley, es acerca de la Protección De Datos Personales, siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.[38].

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[39].

4.5.1. Publicaciones sobre seguridad informática

Los estudios y la publicación científica sobre la seguridad informática son reducidos y es solo a partir de la primera década de este siglo que empiezan a realizarse publicaciones (Grafica No. 4). En cuanto a las publicaciones en idioma ingles también presentan un ascenso a partir del año 2000.

Grafica No. 4 años de publicaciones en español identificadas por SCOPUS.



Fuente Herramientas para extraer y analizar índices de impacto[40].

De acuerdo con lo consultado en Scopus el país que muestra la mayor cantidad

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

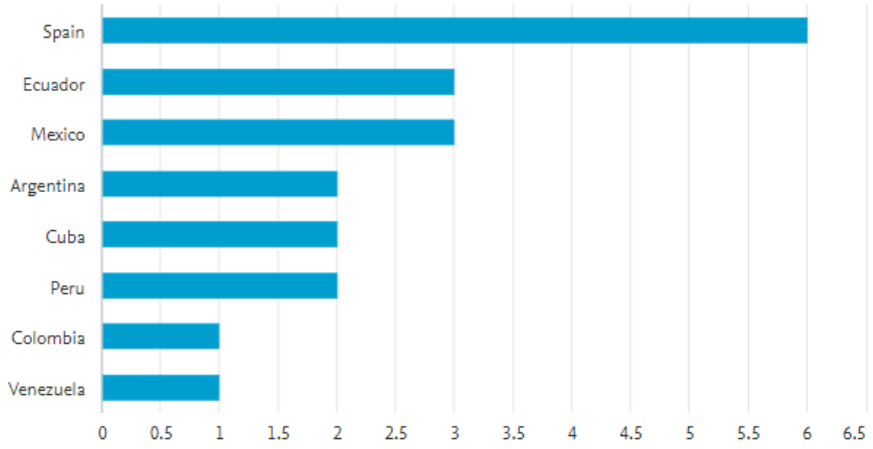
[38] Colombia, C. d. (15 de junio de 2019). Ley 1581 de 2012

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

[40] Scopus, Publicaciones en Español del 2014 al 2019, 2020

de estudios sobre esta temática es España, Ecuador y México de habla hispana, Colombia está en el puesto 7 con una sola publicación

Grafica No. 5 Publicaciones en seguridad informática en Hispanoamericana con investigaciones



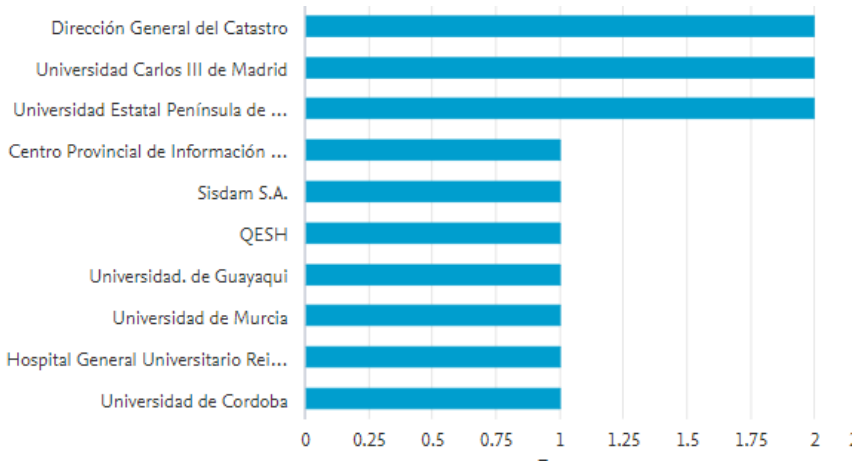
Fuente: Herramientas para extraer y analizar índices de impacto [41]

4.5.2. El tema de la seguridad

El tema de la seguridad informática muestra que son las universidades las que tienen mayores publicaciones, esto es de esperarse en el sentido de que una de las funciones de las universidades es la investigación, sin embargo, son muchas las empresas que están interesadas en este tema. Para el caso de las publicaciones en castellano y lo reportado por las bases de datos es la Universidad Carlos III de Madrid, junto con la universidad Estatal Península de Santa Elena, las que reportan más estudios hasta la fecha (ver gráfico No. 3). En ingles la universidad que más ha presentado estudios es la Shanghai Jiao Tong University en la gráfica se puede observar que son las universidades las que presentan mayor interés por el tema.

[41] Scopus, Publicaciones en Seguridad Informatica, 2020

Grafica No. 6 Universidades que han presentado más estudios sobre seguridad en España



Fuente: Herramientas para extraer y analizar índices de impacto [42]

[42] Scopus, Universidades de España con estudios de seguridad, 2020

5. DESARROLLO DE LOS OBJETIVOS

5.1. MODELOS DE GESTIÓN DESARROLLO DEL OBJETIVO 1

Con respecto a las investigaciones sobre seguridad informática en las IES colombianas 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 la misma.

Universidad Externado de Colombia

Tuvo la iniciativa de crear un semillero en torno al tema de la seguridad informática cuyos objetivos fueron los siguientes:

El objetivo general, fue motivar y desarrollar la actitud investigativa de los alumnos vinculados al Departamento de Derecho Informático, así como crear espacios de discusión, crítica y analítica, enfocados en las áreas de interés planteadas por el Departamento, que a la postre, puedan llegar a ser considerados como desarrollo de los diferentes proyectos estructurados dentro del CIDI [43]

Los logros del proyecto son los siguientes:

1. Entendimiento del contexto de negocio del Laboratorio de Informática con el fin de identificar problemáticas a resolver con Data Science.
2. Obtención y análisis de eventos de seguridad obtenidos de una solución SIEM (Security Information and Event Management) para el sistema de información los Laboratorios de Informática.

[43] Externado de Colombia, 2015.

3. Desarrollo de un modelo predictivo y descriptivo para el sistema de información del Laboratorio de Informática con el fin de resolver las problemáticas identificadas previamente
4. Aplicación del ciclo de vida de Data Science para la identificación de incidentes en sistemas de información críticos protegidos por el CCOC (Conjunto Comando Cibernético) de las Fuerzas Armadas de Colombia.

Universidad Nacional de Colombia

La universidad tiene unas políticas definidas de seguridad informática y de la información desarrolladas desde el año 2015 por la Dirección Nacional de tecnologías de la información y comunicaciones dependiente de la Vicerrectoría General que presenta su política de seguridad informática y de la información versión 02 del 11 de octubre de 2015. [44]

El acuerdo 228 de 2016 según acta No. 07 del 26 de julio de 2016, Por el cual se expide la política de seguridad informática y de la información de la Universidad Nacional de Colombia" [45]

El Acuerdo 046 del 2009 del Consejo Superior Universitario "Por el cual se definen y aprueban las políticas de informática y comunicaciones que se aplicaran en la Universidad Nacional de Colombia" [46].

Universidad Nacional Abierta y a Distancia UNAD

La información institucional que se maneja en la Universidad a través de las redes, equipos y aplicaciones informáticas en general representan un activo muy valioso para la Universidad, el cual puede encontrarse expuesto a diversos riesgos que de ser explotados causarían un impacto significativo en la continuidad de las

[44] Nacional de Colombia, Seguridad de la informacion, 2015.
[45] Nacional de Colombia, 2016.
[46] Nacional de Colombia, Acuerdo 046 de 2012 or el cual se aprueba el Plan Estratégico de Tecnologías de Información y Comunicaciones PETI, 2012.

funciones normales de la institución. [47]

Estrategias de control y prevención en seguridad informática dirigida a los estudiantes, los docentes y administrativos en la UNAD.

- Acuerdo 006 del 26 de agosto del 2008 Por el cual se aprueba el Estatuto de la Propiedad Intelectual de la UNAD
- Resolución 2945 del 2009: deroga la resolución 8547 del 8 de septiembre del 2019
- Resolución 5452 de 2012 que deroga la Resolución 1708 de 2011, Resolución 4256 del 3 de marzo del 2015
- Resolución 6079 del 7 de diciembre del 2012: Alistamiento del Campus Virtual 2013
- Resolución 5071 de 2013 por la cual se define políticas de la renovación tecnológica para UNAD y deroga la resolución 8547 del 8 septiembre del 2016
- Resolución 4256 del 3 de marzo de 2015 el cual define la política del marco de referencia del SGSI
- Resolución 8547 del 8 de septiembre 2016 el cual se reglamenta el uso de los servicios de Tecnología de la UNAD
- Resolución 9803 del 13 de septiembre del 2017 por el cual se modifica la política y los objetivos del sistema integrado de gestión – SIG de la UNAD y se deroga la Resolución 6858 del 2014,la Resolución 7966 de 2014 y la Resolución 5317 de 2015
- Noticias de seguridad: Boletines de seguridad para el personal administrativo
- Boletín de seguridad
- Noticias de seguridad: https://gidt.unad.edu.co/seguridad-de-la-informacion/noticias-de-seguridad

[47] Universidad Nacional Abierta y a Distancia, 2014.

Escuela Tecnológica Instituto Técnico Central

Realizó un macroproyecto sobre seguridad informática que abarque toda la institución, las líneas de investigación a tratar fueron:

1. Ciberseguridad y Ciberdefensa
2. El Delito y laTecnología
3. Vulnerabilidades en la Nube

Dentro del desarrollo del proyecto se crearon dos semilleros de investigación, ellos estuvieron enfocados a determinar el estado de la seguridad informática a nivel de la institución y así detectar las falencias y las vulnerabilidades informáticas, una vez realizados se establecen las políticas se seguridad de la ETITC y se imparte capacitación a los funcionarios administrativos y los docentes de todas las áreas sobre el manejo adecuado de la información.

El resultado que presenta es el informe del resultado denominado: Análisis de las vulnerabilidades informáticas, Proyecto de la investigación: Análisis de rendimiento, las vulnerabilidades y laprevención de fallas de seguridad en la información de la ETITC, se crea un curso corto sobre Pivoting en los servidores remotos, y se elaboran tres trabajos de grado sobre el Big Data, la elaboración del aplicativo para gestionar la carga académica y el Diseño de las políticas de seguridad informática para la ETITC. [48]

Universidad de Cundinamarca

La institución cuenta con las Políticas de Seguridad de la información con la Resolución 088 del 17 de mayo de 2017, Políticas de los tratamientos de Datos [49] Resolución 050 del 8 de mayo de 2018 y con los documentos SGSI. [50]

[48] Trejos Motato, 2015.
[49] Cundinamarca, Política Global del Sistema de Gestión de Seguridad de la Información – SGSI, 2017
[50] Cundinamarca, 2018.

Tabla 1 Documentos del SGSI

ENTRADAS	PROCEDIMIENTOS	SALIDAS
Política de Levantamiento de los activos de la Información Inventario de los activos de la Información Clasificación de los activos de la Información Etiquetado de los activos de la Información	ASIP15 – Gestión de Activos de la Información	Inventario de los activos de la información de la Universidad de Cundinamarca clasificado, etiquetado y publicado
Política de la Protección de Datos de los Titulares de la Universidad de Cundinamarca Solicitud de consulta, reclamo o supresión de datos	ASIP17 – Consulta, Reclamos y Supresión de Datos	Respuesta a la solicitud
Ley 1581 de 2012 Decreto 1377 de 2013 Decreto reglamentario 104 de 2015 Política de Protección de Datos de los Titulares de la Universidad de Cundinamarca Solicitud de la recolección del tratamiento de datos de los titulares de la universidad de Cundinamarca ASIM004 – Manual para el tratamiento de los Datos personales	ASIP22 – Recolección de Datos Personales	Datos recolectados de los titulares de la Universidad de Cundinamarca
Ley 1581 de 2012	ASIP23	Los Datos almacenados

Decreto 1377 de 2013 Decreto reglamentario 104 de 2015 Política de la Protección de Datos de los Titulares de la Universidad de Cundinamarca Datos recolectados de los titulares de la Universidad de Cundinamarca	Almacenamiento de Datos Personales	de los titulares de la Universidad de Cundinamarca
Ley 1581 de 2012 Decreto 1377 de 2013 Decreto reglamentario 104 de 2015 Política de Protección de Datos de los Titulares de la Universidad de Cundinamarca Datos almacenados de los titulares de la Universidad de Cundinamarca	ASIP24 – Uso y Circulación de Datos Personales	Control de los datos personales que se usan y circulan por las diferentes áreas de la institución

Fuente: Responsable del sistema de gestion de seguridad de la informacion[51]

Universidad del Valle

Define la estructura normativa, la cual da a conocer a la comunidad universitaria el uso de los recursos tecnológicos, permitiendo promover los objetivos de la Universidad en un ambiente seguro y claro

La política de seguridad que implementa la Universidad del Valle se basa bajo los principios preservar, asegurar y proteger los activos de la institución.

a. Normatividad
    1. Principio de propiedad de la información.
    2. Principio de protección de la información.

[51] Martínez Clavijo, s.f.

3. Principio de protección de los recursos tecnológicos.
4. Principio de orientación al cumplimiento de la misión de la universidad.
5. Principio de autorización de usuarios.-
6. Principio de la responsabilidad
7. Principio de la disponibilidad
8. Principio de la integridad
9. Principio de la confianza.
10. Principio del esfuerzo de equipo
11. Principio del soporte primario para la seguridad de la información

b. Recomendaciones de la seguridad

Uso del Correo electrónico [52]

Universidad Distrital Francisco de José de Caldas

La Universidad Distrital cuenta con su sistema de seguridad de la información versión 0.0.1.0 desarrollado por el comité de informática y las telecomunicaciones (CIT), y cuenta con las siguientes normatividades

- Resolución 711 del 26 de diciembre 2008: el uso del servicio de internet y los correos electrónicos
- Resolución 461 del 29 julio de 2011: Desarrollo OPENUP/AOS: implementación de software al interior de la institución
- Resolución 678 del 28 de septiembre 2011adopta la política de seguridad de la información y otorga funciones al comité de informática y telecomunicaciones
- Resolución 690 del 1 de noviembre de 2011 adopción y uso de software en la institución [53](Distrital Francisco Jose de Caldas, Secretaria General, s.f.)

Dentro de las políticas aplicadas cuentan con la confidencialidad, la integridad y la disponibilidad, aplicando los aspectos de Autenticidad, posibilidad de auditoria,

[52] Valle, s.f.
[53] Distrital Francisco Jose de Caldas, Secretaria General, s.f.

protección a la duplicación, no repudio, legalidad y confidencialidad de la información [54]

Tabla 2 Seguridad implementadas en la algunas Universidades de Colombia

Universidad	Tipode control		Factor diferenciador
	SGSI	Politicas	
Externado de Colombia	No	Si	Crearon el departamento de derecho informático con la vinculación de los estudiantes, dentro de la estructura Centro de Investigación en Derecho Informático - CIDI
Nacional de Colombia	Si	Si	Como resultado del análisis de brecha en el 2015 se diseñó el Plan Director de Seguridad, que incluye SGSI y Políticas
Universidad Nacional Abierta y a Distancia - UNAD	Si	Si	Con la resolución 4256 del 3 marzo del 2015 se definen las políticas del SGSI y con la resolución 4793 del 22 de agosto de 2013, se crea la política de seguridad de la información
Escuela Tecnológica Instituto Técnico Central La Salle	Si	Si	Como parte del Sistema de Gestión de Calidad, tiene el proceso Gestión de Informática y Comunicaciones, el cual contiene documentos relacionado con la seguridad de la información.

[54] Distrital Francisco Jose de Caldas, 2011.

de Cundinamarca	Si	No	Tiene implementado el SGSI según la norma ISO 27001, pero no Políticas de seguridad Informática.
del Valle	Si	Si	Cuenta con la normatividad de las políticas del uso de los recursos informáticos para la seguridad de la información
Distrital Francisco de José de Caldas	Si	Si	En el 2015 el subsistema de Gestión de seguridad de la información SGSI

Fuentes del autor

5.2. CAUSAS DE VULNERABILIDAD Y RIESGO DESARROLLO DEL OBJETIVO 2

Existen amenazas que por su naturaleza son difíciles de controlar es el caso de los desastres naturales o los errores humanos, sin embargo, se deben tener en cuenta en el cálculo de los riesgos. Por otra parte, existen amenazas voluntarias que provienen de los ataques deliberados su origen puede ser externo o interno, dentro de los internos contamos con los empleados insatisfechos o los exempleados con credenciales aun no revocadas o cambiadas. Dentro de las externas puede ser competencia desleal de otras empresas, activistas o terroristas y cibercriminales. (* Ver Glosario)

- *Empleados activos
- *Exempleados
- *Curiosos
- * Los Hackers
- *Los Crackers
- *Los Intrusos remunerados

Amenazas lógicas:

- *El Software incorrecto
- *La Herramienta de seguridad
- *Las Puertas traseras
- *Los Canales Cubiertos
- * El Virus o códigos maliciosos
- *Los Gusanos
- El Robo de información
- La Suplantación de identidad

Amenazas Físicas:

Las que corresponden a esta clase de eventos los robos, sabotajes, destrucción de los sistemas, el suministro eléctrico, las condiciones atmosféricas, las catástrofes naturales**.**

Bases de Datos

Las bases de datos es la infraestructura más importante de una organización, para este caso en la IES. En ellas se encontraron las vulnerabilidades, las amenazas o los riesgos que podamos incurrir frecuentes en las Base de Datos y se pueden categorizar de los siguientes factores: [55]

- La Contraseña débil
- El Dar privilegios excesivos e inutilizados
- El Abuso de privilegios
- Los Privilegios de usuarios por privilegios de grupo
- Las Características de BD innecesariamente habilitadas
- La Base de datos desactualizadas y sin cifrar
- Las Inyecciones SQL
- El Malware y spear phishing

[55] TICbeat, 2013

- La Falta de Auditoria o deficientes
- El Backup no se encuentran bien asegurados
- La Explotación de vulnerabilidades y bases de datos mal configuradas
- Los Datos sensibles mal gestionados
- La Denegación de servicios (DoS)
- La Limitación de conocimientos y experiencias en seguridad y educación
- El Desbordamiento de bufer

Algunas Universidades que fueron víctimas contra los ataques cibernéticos, durante los últimos 10 años

Tabla 3 Universidades víctimas de ataques cibernéticos

Universidad	País	Año	Tipo de ataque
Yale	EEUU	Ago. 2011	El Robo de la información de estudiantes y exalumnos
Stanford	EEUU	Jul. 2013	El Acceso a los usuarios y contraseñas
Berkeley	EEUU	Dic. 2014	El Robo de la información de los empleados y los exempleados
Pensivania	EEUU	2014	El Robo de la información
Harvard	EEUU	Mayo 2015	El Ataque a la página web
Rutgers	EEUU	Dic. 2015	La Obstaculización ilegítima de sistema informático o red
Nueva Jersey	EEUU	Dic. 2015	La Obstaculización ilegítima de sistema informático o red
Tolima	Colombia	Enero 2018	El Acceso abusivo al sistema informático
Maastricht	Países Bajos	Dic. 2018	El Ransomware
Oriente	Salvador	Oct. 2019	Ataque DDos

Fuente del Autor

A medida que va aumentando la vanguardia de la tecnología, también va creciendo los ataques cibernéticos, el cual debemos identificar los principales riesgos que puede acarrear un ataque cibernético a la organización entre ellas podemos definir.

La Vulnerabilidad de software: los fallos de seguridad, el cual son corregidos rápidamente por el proveedor

Los Malos hábitos de seguridad:la descarga de información de sitios dudosos o email, permitido de esta manera el robo de la información o el chantaje como es el caso del Ransomware.

La Mala configuración de los sistemas: No realizar un estudio previo acerca de las políticas de la seguridad en los servidores, firewall y otros sistemas

El Software no autorizado: la Instalación de programas sin autorización y aplicando la herramienta para activar el programa desarrollada por los ciberdelincuentes

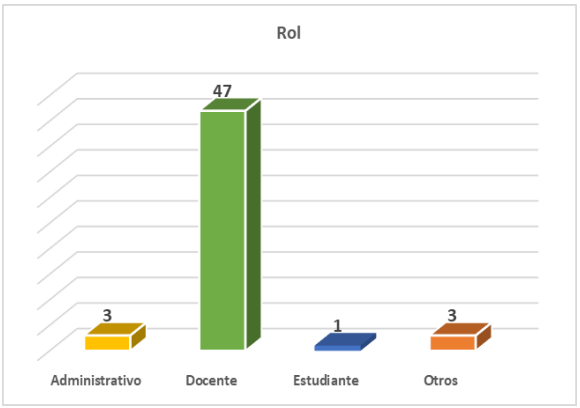
5.2.1. Análisis de la encuesta realizada para analizar el estado actual de la seguridad informática en las IES

La encuesta fue aplicada a un total de 54 personas vinculadas a una IES a partir de diferentes roles

Como se evidencia en a gráfica 1, 47 de las personas que realizaron a la encuesta, tienen el rol de docente dentro de una IES, en tanto las respuestas que aquí se muestran están directamente relacionadas con la percepción de estos respecto a la seguridad informática. Así también se encuentra 3 personas en el rol

administrativo, 3 en otras funciones dentro de la IES y finalmente una 1 sola persona en el rol de estudiantes de una IES

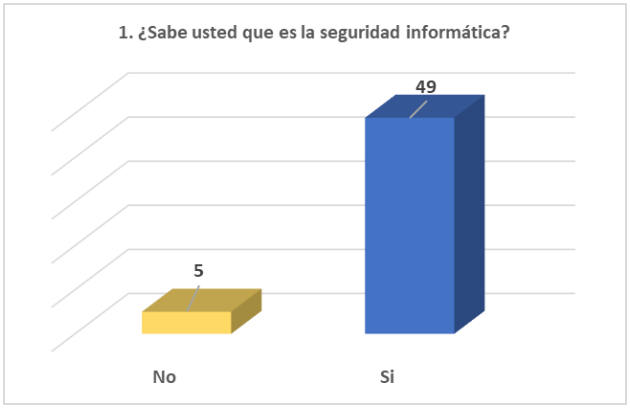
Grafica No. 7 Rol del encuestado



Fuente del Autor

La gráfica 7 determina que un total de 49 personas de los encuestados reconocen la seguridad informática, de esta manera ellos comprenden a que se refiere y probablemente en algún momento han tenido algún contacto con ella. Contrastando de esta manera con 5 personas que no saben que es y por lo tanto pueden significar un riesgo de vulneración importante.

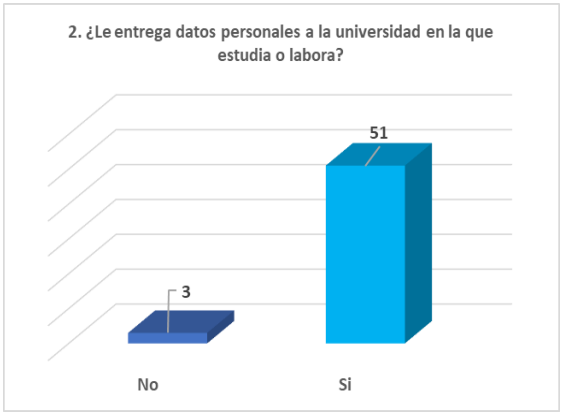
Grafica No. 8 El conocimiento seguridad informática



Fuente del Autor

Esta es una de las preguntas centrales de la encuesta realizada, dado que les permite observar que 51 de ellos, (casi la totalidad de los encuestados), manifiestan que entregan información personal a la universidad, de esta manera se demuestra que la información que se guarda y cuida en la universidad es de mucho valor. Solo 3 personas manifestaron no dar este tipo de información a la universidad.

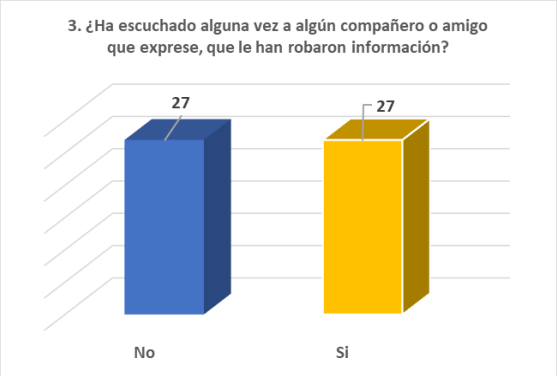
Grafica No. 9 El conocimiento seguridad informática



Fuente del Autor

La pregunta demuestra que a pesar de que no todas las personas encuestadas han sido víctimas o conocen a alguien que ha pasado por un robo de información informático, si hay una cifra preocupante de 27 personas que manifiestan que si, por lo tanto, la mitad de las personas encuestadas conocen a alguien que ha tenido esta situación.

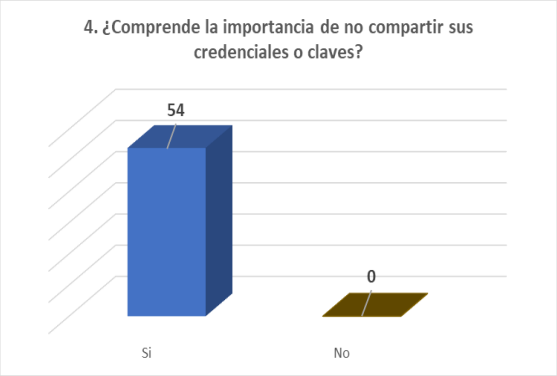
Grafica No. 10El Robo de información



Fuente del Autor

Esta es una pregunta que brinda un panorama positivo, para la seguridad informática de las IES, ya que demuestra como las personas son cada vez más conscientes de la importancia de no compartir sus datos, las credenciales o las claves con otras personas, ya que esto significaría un riesgo para la información.

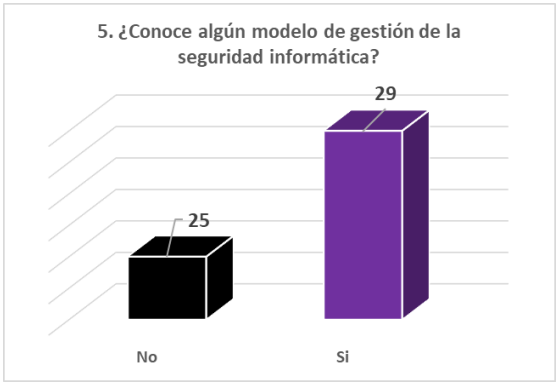
Grafica No. 11 La Importancia no compartir su información



La Fuente del Autor

La respuesta determina, que a pesar de que 29 de las personas encuestadas si conocen algún modelo de gestión informática, todavía son muchos los que lo desconocen con una cifra de 25 personas en total que demuestran que el proceso debe continuarse con mayor ímpetu para que todas las personas que tienen contacto con las IES lo reconozcan.

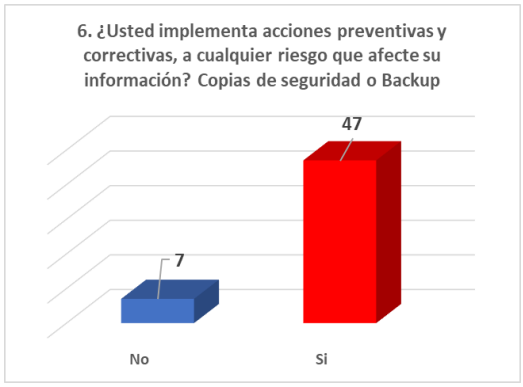
Grafica No. 12 Los Modelos de gestión de seguridad informática



La Fuente del Autor

Su resultado es positivo para la encuesta, dado que demuestra que cada vez son más las personas que tienen conciencia acerca de la importancia de tener copias de seguridad o backup. Teniendo como resultado un total de 47 personas que lo hacen y solo 7 personas que aún deben mejorar en este proceso para fomentar la seguridad informática.

Grafica No. 13 Las Acciones preventivas y correctivas

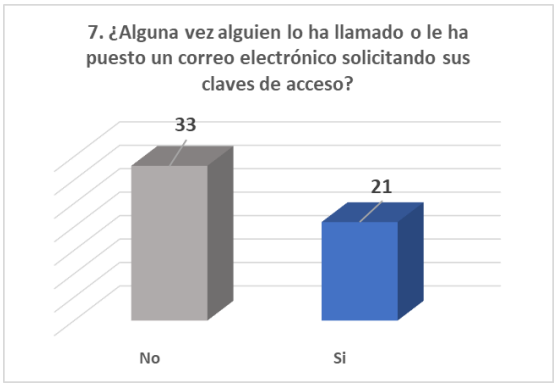


La Fuente del Autor

Es esta una pregunta determinante, que genera no solo la posibilidad de comprender la cantidad de personas que han podido ser víctimas del robo de su información sino además la cantidad de ocasiones en las que la información de la IES pudo estar en riesgo, de esta manera 33 de ellas manifiestan que no han recibido nunca un correo electrónico o una llamada solicitando claves de acceso,

pero 21 de ellas manifiestan que sí. Por lo tanto, la labor de los modelos de seguridad informática tiene toda la pertinencia dentro de las IES dado que se presentan riesgos de manera constante

Grafica No. 14 El Riesgo de la seguridad



Fuente del Autor

5.3. PROPUESTAS DE MEJORAMIENTO DESARROLLO DEL OBJETIVO 3

Para evitar un ataque la mejor estrategia a implementar dentro de las instituciones de la educación Superior IES son las siguientes:

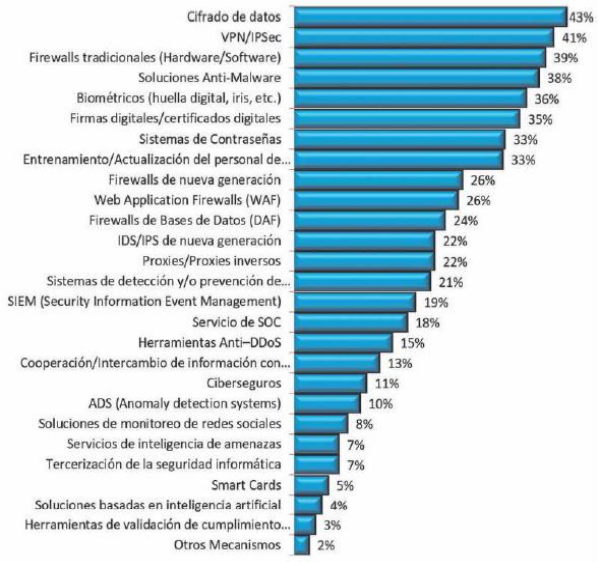
1. No abrir los correos electrónicos de dudosa procedencia
2. El Reducir el número de cuentas con privilegios de administrador y de ejecución de macros
3. Actualizar el software automáticamente
4. Filtrar los archivos adjuntos ejecutables en los mensajes de correos electrónicos
5. Implementar líneas de defensa con AntiPhishing, Awarenes, Firewalls, Antivirus, Soluciones Antiransomware y capacitación al personal
6. Reducir al máximo de compartir carpetas
7. Capacitar a los empleados en temas de seguridad (prevención contra el Phishing, los Awarenes, el ransomware, la ingeniería social)

8. Backups de los datos de manera periódica
9. Configurar las extensiones ocultas en los archivos
10. Restaurar el sistema para volver a un estado previo conocido sin infecciones
11. Deshabilitar el protocolo RDPU
12. Deshabilitar los archivos que se ejecuten desde las carpetas APPData y LocalAppData

Otro elemento importante son los recursos, que resultan ser activos tangibles o intangibles con que se cuentan para la realización y el desarrollo de las actividades en el caso de la información que es uno de los activos más importantes y valiosos de la organización, se refiere a un intangible que son las mismas bases de datos relacionadas con los clientes o los usuarios, también pueden ser archivos de datos como los manuales, las investigaciones de los informes de mercado, las patentes etc. En cuanto a los tangibles corresponden a los elementos físicos como la maquinaria, los servidores, los PC, las redes, los teléfonos y las otras infraestructuras físicas con que se cuenta.

Ellos deben tener en cuenta, cuáles serían los mecanismos más usados, hasta el 2019

Grafica No. 15 Mecanismos de seguridad más comunes



Fuente:Los Sistemas Ciberriesgo: el riesgo sistematico [56]

Una vez analizado 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% y el Firewall oel cortafuegos con el 39%

En la institución podemos implementar los siguientes mecanismos que nos ofrecen la seguridad ya sean el Hardware, el software o la capacitación a los empleados

Otra de las implementaciones que debemos tener dentro de la organización son las evaluaciones de los riesgos al menos una vez al año, de esta manera estaríamos minimizando el ataque.

Los tipos de metodología que podemos usar y mitigar los riesgos de la seguridad

[56] CANO M., J. J. (junio de 2019). *Ciberseguridad y ciberdefensa: Retos y perspectivas en un mundo digital.* Obtenido de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952019000200001&lng=pt&nrm=iso

informática son: (* Ver Glosario)

- ***ISO 31000**
- ***ISO 27005**
- ***Saro**
- ***GRC**
- ***ERM**
- ***Magerit**

Base de Datos:

Para temer una base de datos segura los expertos nos sugieren tener en cuenta las siguientes recomendaciones. [57]

- ✓ **Identificar todas las vulnerabilidades que podamos encontrar en nuestras bases de datos**

Se deben analizarla información importante que van a proteger, para así determinar dónde y cómo se almacenan los datos sensibles

Los datos de la compañía deben tener un inventario, de las áreas de esta, para si tener claro el registro de las instancias y las bases de datos de la compañía.

El inventario es de útil ayuda al momento de hacer un respaldo de la información, así se evita que los datos críticos queden fuera del esquema

- ✓ **Contraseñas:**

Evitar contraseñas simples

Utilizar contraseñas más complejas y que incluya símbolos, mayúsculas y minúsculas

[57] Acens, 2015

Realizar cambios de contraseñas periódicamente

- ✓ **Después de realizar una configuración, nos recomienda hacer una auditoria**

Se debe auditar y registrar los movimientos y las acciones de los datos, que les permita saber cuándo, que, quien, ha manipulado la información, asi pueden evitar fuga de la información, ya que se tendría un historial completo de los movimientos que se realizan en la base, y controlar los cambios fraudulentos, detectar las acciones sospechosas en tiempo real.

- ✓ **Mantener el software actualizado**

Recuerden que deben actualizar regularmente el sistema operativo y el software que tienen instalado en el equipo, poner especial atención a las actualizaciones del navegador web. En algunas ocasiones, los sistemas operativos presentan fallos, los que son aprovechados por los delincuentes informáticos. Muchas veces aparecen actualizaciones que solucionan esos fallos. Deben estar al día con las actualizaciones, y aplicar los parches de seguridad que les recomienden los fabricantes, esto les ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

- ✓ **Vigilar todas las acciones sobre las bases de datos**

Recuerden seguir los consejos mencionados, ser precavidos cuando vayan a administrar y proteger las bases de datos, la información que estas tienen es muy importante para la empresa y un botín muy codiciado para los atacantes.

- ✓ **Revisar los accesos**

Entre más símbolos y signos tengan los privilegios y permisos mejor, el control para el acceso es el primer paso que las personas deben tener en cuenta para tener los atacantes lejos de la información.

Las personas deben tener en cuenta: Solo los usuarios autorizados, y algunas personas deben tener acceso para realizar consulta sobre la información sensible (personal del usuario).

Que las personas no ingresen a la información fuera del horario laboral o habitual.

Lo ideal es que se deshabiliten los servicios y los procedimientos que no se estén utilizando, y que la base de datos este en el servidor que no tenga acceso a internet, para q no se presenten los atacantes remotos.

- ✓ **Realizar copias de seguridad o Backup**

Deben hacer copias de seguridad, cada 15 u 8 días, en las bases de datos y a la vez encriptarlas, guárdalas en un sitio seguro.

Para evitar que caigan manos de otros funcionarios o personas ajenas dentro de las áreas de trabajo, o que por equivocación confundan el medio magnético para guardar otra información que no corresponda a lo que se asignó, a este medio para respaldar su copia de la información

- ✓ **Bases de Datos, no son productivas**

El enmascaramiento se usa para crear una versión similar,a la información original, pero alterando los datos sensibles para así protegerlos, con esta técnica se cambian los valores respetando el formato.

Estos datos se pueden cambiar de diferentes maneras, cifrándolos, cambiando las palabras, mezclándolos entre sí, pero se deben mantener las reglas y los formatos, se debe garantizar que el proceso sea irreversible, lo cual significa que no se puedan obtener los datos originales.

La técnica se utiliza y se recomienda para las bases de datos que forman parte de entornos de pruebas y desarrollo, garantiza que la información sensible del cliente no esté disponible fuera del entorno de producción.

- ✓ **Cifrar las Bases de Datos**

Cuando ya se tiene conocimiento de los datos sensibles y de la información confidencial, se recomienda la utilización de algoritmos robustos para cifrar los datos.

Los atacantes buscan la vulnerabilidad para tener el acceso a el servidor o el sistema, lo que primero hará es robar las bases de datos, pues es el tesoro más codiciado por ellos, para preservar la información debe ser ilegible para las personas que deseen llegar a ella sin autorización

6. CONCLUSIONES

Las universidades 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 los docentes y estudiantes 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.

Ninguna de las universidades analizadas en la presente monografía considera que la seguridad informática no es importante para el desarrollo de sus actividades y para enfrentar los retos de la sociedad de la información y el conocimiento.

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 la misma y de las múltiples posibilidades de mejora que la investigación proporcionan.

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.

7. RECOMENDACIONES

Fomentar desde las mismas universidades 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 se aun 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 visibilizarían de la labor dentro de los estudiantes, docentes y administrativos, enalteciendo la labor de los procesos realizados en este sentido.

Se pueden generar redes entre las universidades 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 de todos.

Esta red permitirá que exista una fuerza mucho más estructurada, en la que los procesos y modelos de cada universidad sean tenidos en cuenta, fomentando la seguridad informática como un elemento primordial en todas las IES, de esta manera cada elemento que se aplique en una puede ser reproducido en las otras y de esta manera mejorar cada vez más los procesos de seguridad.

BIBLIOGRAFIA

ACENS, Technologies. “Bases de datos y sus vulnerabilidades más comunes” Internet: (https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf)

ALMANZA, Andres, “Revista Sistemas: Encuesta. Seguridad Informática en Colombia Tendencias 2012 - 2013”. Internet: (http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013)

ANONIMO, “Capitulo 1: Seguridad Informatica: Conceptos Basicos”, Internet: (http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf)

ANONIMO, “Capitulo 2: Seguridad Informatica”, Internet: (https://www.coursehero.com/file/45648812/A5pdf)

ARÉVALO, Moscoso y Franklin Mauricio y Cedillo Orellana y Irene Priscila y Moscoso Bernal y Santiago Arturo, “Metodologia agil para la Gestion de Riesgos informaticos”, Internet (https://docplayer.es/127165258-Revista-killkana-tecnica-volumen-1-numero-2-mayo-agosto-2017-issn-impreso-issn-electronico.html)

BARZANALLANA, Rafael, “Introducción a la Seguridad Informática: Gestión de la Seguridad en Sistemas de Información), Internet (https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf)

BASALDUA ALVAREZ, Luis Daniel, Seguridad Informatica: Auditoria de Sistemas. Tesis Maestro en Ingeniería de Sistemas Empresariales. Mexico, D.F. Universidad Iberoamericana. 2005

CANO, Jeimy y Rocha, Alvaro, “Ciberseguridad y ciberdefensa: Retos y perspectivas en un mundo digital”, Internet: (http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952019000200001&lng=pt&nrm=iso)

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 83.(29, noviembre de 1993). Por la cual se establecen normas para el ejercicio de control interno en las entidades y organismos del estado y se dictan otras disposiciones. Bogota D.C., 1993

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 594. (14, julio de 2000). Por medio de la cual se dicta la ley General de Archivos y se dictan otras dispociones, Bogota D.C., 2000

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599. (24, julio de 2000). Por la cual se expide el Codigo Penal, Bogota D.C., 2000

COLOMBIA, CONGRESO DE LA REPUBLICA.Ley 603. (27, julio de 2000). Por la cual se modifica el articulo 47 de la ley 22 de 1995. Bogota D.C., 2000

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 734. (5, febrero de 2002). Por el cual se xpide el Codigo Disciplinario Unico, Bogota D.C., 2002

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. (5, enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, Bogota D.C., 2009

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341. (30, julio de 2009). Por el cual se definen principios y conceptos sobre la sociedad de la informacion y la organización de las Tecnologias de la Informacion y las Comunicaciones – TIC, se crea la agencia Nacional del Espectro y se dictabn otras disposicioooenes. Bogota D.C., 2009

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527. (15, junio de 2019). Por medio de la cual se define y 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 se dictan otras disposiciones. Bogota D.C., 2019

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581. (15, junio de 2019). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogota D.C., 2019

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. (19, junio de 2019). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Bogota D.C., 2019

CSIRT-cv, 12 medidas básicas para la seguridad Informática. Valencia: (Union Europea, Madrid, España) Documento Publico, España

DACCACH, José Camilo, “Ley de Delitos Informáticos en Colombia” Internet: (https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia)

DE FREITAS, Vidalina, “Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolíva”, Internet: (http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1690-75152009000100004&lng=es&nrm=iso)
DUQUE, Cesar y Asociados Consultores de Riesgos, “Metodologia para la Gestion de Riesgos: Como integrar la seguridad a los objetivos estrategicos de los negocios de una manera costo-beneficiosa”. Internet:(http://www.ridsso.com/documentos/muro/207_1469148692_57916e1488c74.pdf)

FEDERAL BUREAU OF INVESTIGATION, FBI “Irani una Mabna Hackers” Internet: (https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers)

FERNANDEZ LAVIADA, Ana, “La Gestión del Riesgo Operacional: De la teoría a su aplicación.”, Internet: (https://books.google.com.co/books?id=kR33ej859OEC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)

GIL VERA, Víctor Daniel y Gil Vera, Juan Carlos, “Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas”, Internet: (https://www.redalyc.org/articulo.oa?id=84953103011)

HERNÁNDEZ, Ramón Ventura Roque y Ibarra, Carlos Manuel Juárez, “Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios”, Internet: (http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072018000200005&lng=es&nrm=iso)

HUARAHUARA, Marisel Matilde Mendoza, “Delitos informaticos”, Internet: (http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442009000200002&lng=es&nrm=iso)

LEZAMA, Lugo, Estructura y funcionalidad de un sistema de seguridad informatica: Primera generacion de Sistemas de Seguridad. Modelado de dispositivos para un sistema de seguridad implementando tecnologia jini. Tesis de Licenciatura. Mexico, Universidad de las Americas Puebla, Ingenieria en Sistemas Computacionales, 2001

MARTELO, Raul y Tovar, Luis y Maza, Diego, “Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia”, Internet: (https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003&lng=en&nrm=iso&tlng=en)

MARTÍNEZ CLAVIJO, Edilson, “Sistema de Gestion de seguridad de la informacion” Internet: (https://www.ucundinamarca.edu.co/sgc/index.php/macroproceso-estrategico/proceso-gestion-sistemas-integrados/sgsi)

MARTÍNEZ, Jeimy Cano, “Ciberriesgo: Un riesgo sistematico”, Internet: (https://acis.org.co/archivos/Revista/Sistemasedicion151.pdf)

NAVARRO, Andrés, “La seguridad informática es una realidad en Colombia”, Internet: (http://www.icesi.edu.co/agenciadeprensa/boletines/2008/seguridad_informatica.html)

OJEDA PÉREZ, Jorge Eliécer y Rincón Rodríguez, Fernando y Arias Flórez, Miguel Eugenio y Daza Martínez, Libardo Alberto, “Delitos informáticos y entorno jurídico vigente en Colombia”, Internet: (http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_abstract&tlng=es)

PARRA MORENO, Duver Augusto, “Gestion del riesgo en la seguridad informatica: “Cultura de la auto-seguridad Informatica", Internet: (https://repository.unimilitar.edu.co/bitstream/handle/10654/6821/ParraMorenoDuverAugusto2012.pdf?sequence=2)

PULIDO, Julián Alberto Monsalve y Novoa, Fredy Andrés Aponte y Tamayo, David Fernando Chaves, “Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia)”, Internet: (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292014000200007&lng=en&nrm=iso)

RAMIREZ LIS, Yaned, “Manual de Normas y Políticas de Seguridad Informática”. Internet: (https://www2.sgc.gov.co/ControlYRendicion/TransparenciasYAccesoAlaInformacion/CircularesManuales/MO-TEC-001-I.pdf)

REAL ACADEMIA DE ESPAÑOL, “Diccionario”, Internet: (https://www.rae.es)

Revista Cientifica Dominio de las Ciencias julio, 2017, Vol. 3, Num 5. ISSN 2477-8818

ROMERO CASTRO, Martha Irene y Figueroa Moràn, Grace Liliana y Vera Navarrete, Denisse Soraya y Álava Cruzatty, José Efraín y Parrales Anzúles, Galo Roberto y Álava Mero, Christian José y Murillo Quimiz, Ángel Leonardo y Castillo Merino, Miriam Adriana. Introduccion a la Seguridad Informatica y el Analisis de

Vulnerabilidad. España: Área de Innovación y Desarrollo 2018 ISBN 978-84-949306-1-4

SANCHEZ, Kelly Gabriela Bermudez Molina y Edber Rafael Bailon. Analisis en Seguridad Informatica y Seguridad de la Informacion Basados en la Norma ISO/IEC 27001 - Sistema de Gestion de Seguridad de la Informacion Dirigido a una empresa de servicios financieros. Tesis. Guayaquil. Universidad Politecnica Salesiana, Ingeneria de Sistemas. 2015

SCOPUS, “Area por Profesion”, Intranet: (https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=5e796377ef0b4f8a373e902ee2e257b5&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Informatic+security%29&sort=plf-f&sdt=b&sot=b&sl=34&count=328&analyzeResults=Analyze+results&txGid=13005)
SCOPUS, “Índices de impacto”, Intranet: (https://www.recursoscientificos.fecyt.es/servicios/indices-de-impacto)

SCOPUS, “Publicaciones de Universidades de Estados Unidos”, Intranet: (https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=2f01071c0103fd57932ba979c535519f&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Informatic+security%29&sort=plf-f&sdt=cl&sot=b&sl=34&count=78&analyzeResults=Analyze+results&cluster=sco)

SCOPUS, “Publicaciones en Español”, Intranet: (https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=e7a4e3fee82f959193e3c395568969bc&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Seguridad+Informatica+%29&sort=plf-f&sdt=b&sot=b&sl=37&count=17&analyzeResults=Analyze+results&txGid=036)

SCOPUS, “Publicaciones en Seguridad Informatica”, Intranet: (https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=5e796377ef0b4f8a373e902ee2e257b5&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Informatic+security%29&sort=plf-f&sdt=b&sot=b&sl=34&count=328&analyzeResults=Analyze+results&txGid=13005)

SCOPUS, “Universidades de España con estudios de seguridad”, Intranet: (https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=e7a4e3fee82f959193e3c395568969bc&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Seguridad+Informatica+%29&sort=plf-f&sdt=b&sot=b&sl=37&count=17&analyzeResults=Analyze+results&txGid=036)

TICBEAT, Tecnologia, ”Las 10 grandes amenazas de seguridad en las bases de datos”, Internet: (https://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos)

TREJOS MOTATO, José Alfredo, “Grupo de investigación en Seguridad Informática Sapientiam”, Internet: (http://www.itc.edu.co/archives/sapientiamgruplac.pdf)

UNIVERSIDAD DE CUNDINAMARCA, “Política Global del Sistema de Gestión de Seguridad de la Información – SGSI”, Internet (https://www.ucundinamarca.edu.co/index.php/politica-de-tratamiento-de-datos)

UNIVERSIDAD DEL VALLE, “Políticas para el uso de recursos informáticos: Oficina de Informática y Telecomunicaciones”, Internet: (http://mafalda.univalle.edu.co/politicainformatica)

UNIVERSIDAD EXTERNADO DE COLOMBIA, “Centro de Investigación en Derecho Informático (CIDI)”, Internet: (https://derinformatico.uexternado.edu.co/centro-de-investigacion-en-derecho-informatico-cidi)

UNIVERSIDAD EXTERNADO DE COLOMBIA, Internet (https://www.uexternado.edu.co)

UNIVERSIDAD FRANCISCO JOSE DE CALDAS, ” Secretaria General”, Internet: (https://sgral.udistrital.edu.co/sgral)

UNIVERSIDAD FRANCISCO JOSE DE CALDAS, ”Politicas de Seguridad de la informacion Version 0.0.1.0.”, Internet: (https://funcionarios.portaloas.udistrital.edu.co/cit/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, “Gerencia de Innovacion y Desarrollo Tecnologico: GIDT”, Internet (https://gidt.unad.edu.co

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, UNAD, “Seguridad de la Informacion”, Internet: (https://gidt.unad.edu.co/seguridad-de-la-informacion)

UNIVERSIDAD NACIONAL DE COLOMBIA, Acuerdo 046 (10, abril de 2012). Por el cual se aprueba el Plan Estratégico de Tecnologías de Información y Comunicaciones, Bogota D.C., 2012

UNIVERSIDAD NACIONAL DE COLOMBIA, Acuerdo 228 (26, julio de 2016), Por el cual se expide política de seguridad informática y de la información. Bogota D.C., 2016

UNIVERSIDAD NACIONAL DE COLOMBIA. “Politicas de seguridad informatica y de la informacion”, Internet: (https://www.dntic.unal.edu.co/images/seguridad/PolticadeSeguridadInformaticaydelaInformacion.pdf)

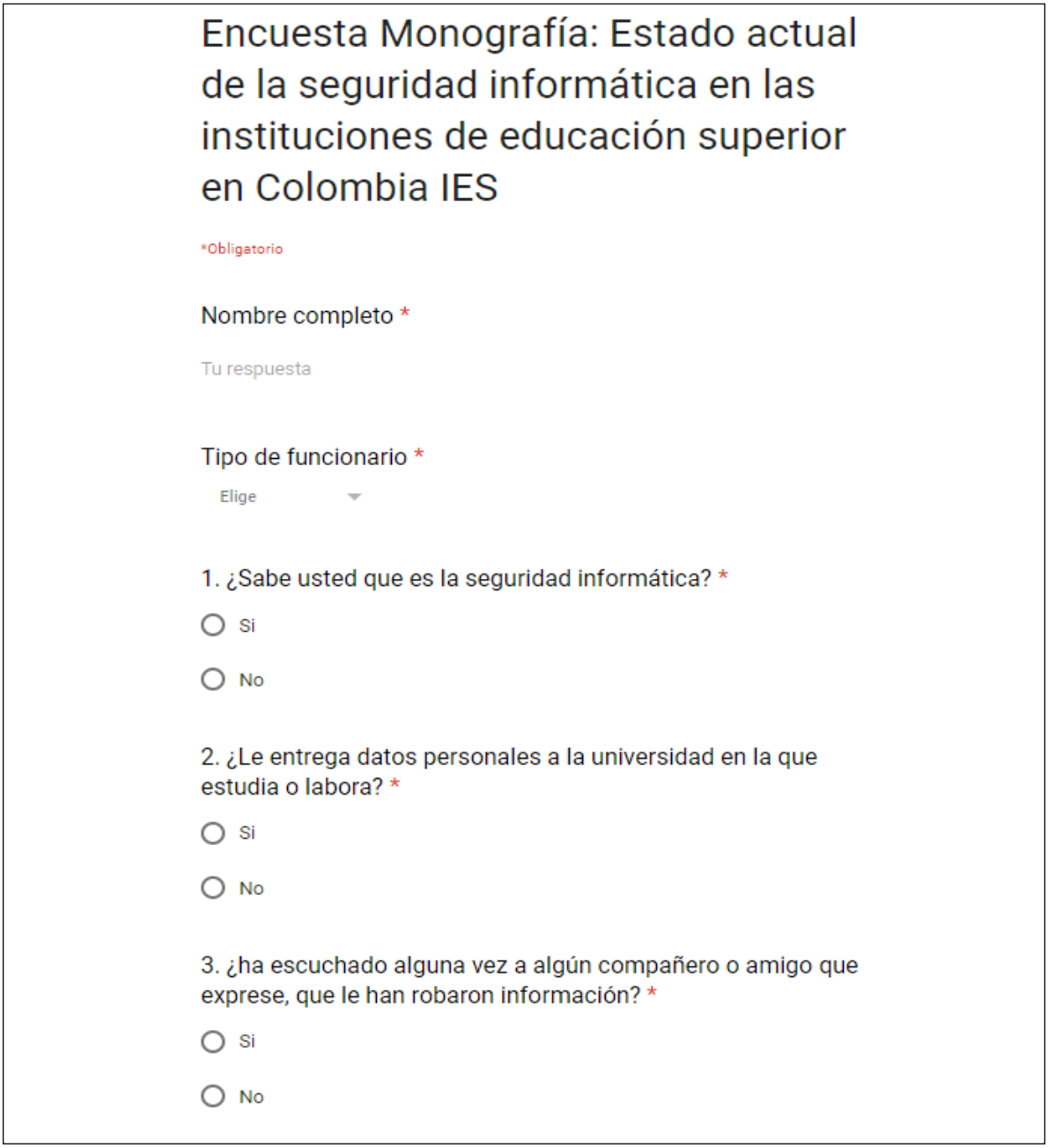
WIKIDOT, “Seguridad Informatica”, Internet: (http://seguridadinformatica.wikidot.com/seguridad-informatica)

WIKIPEDIA, “Información”; Internet: (https://es.wikipedia.org/wiki/Informaci%C3%B3n)

ANEXO

ANEXO A Encuesta diseñada para analizar el estado actual de la seguridad informática en las IES

Grafica No. 16 Modelo de la encuesta



Encuesta Monografía: Estado actual de la seguridad informática en las instituciones de educación superior en Colombia IES

*Obligatorio

Nombre completo *

Tu respuesta

Tipo de funcionario *

Elige

1. ¿Sabe usted que es la seguridad informática? *

Si

No

2. ¿Le entrega datos personales a la universidad en la que estudia o labora? *

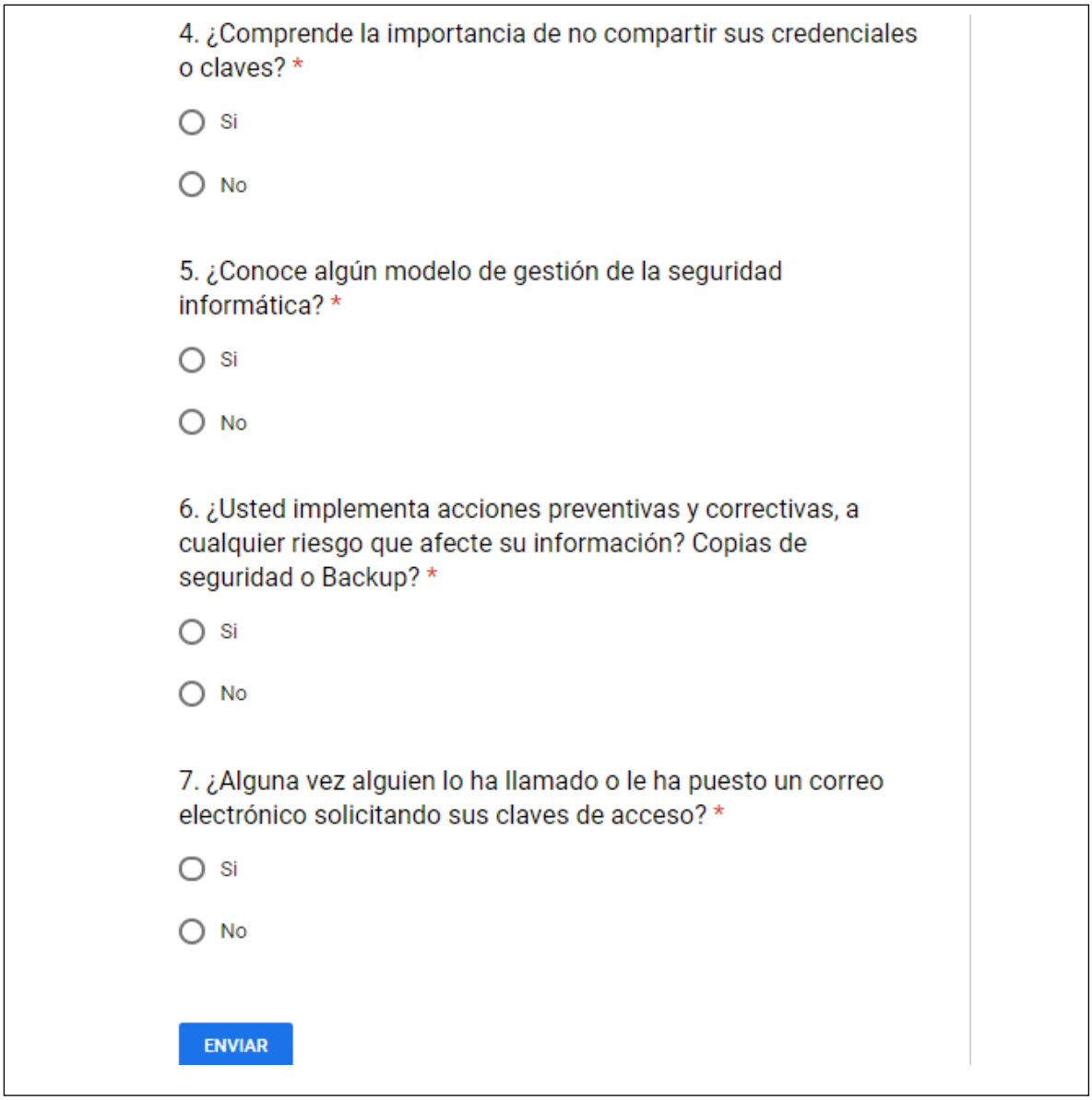
Si

No

3. ¿ha escuchado alguna vez a algún compañero o amigo que exprese, que le han robaron información? *

Si

No



Fuente del Autor

RESUMEN ANALITICO EDUCATIVO - RAE

Título del texto	Estado actual de la seguridad informática en las instituciones de educación superior en Colombia IES**.**
Nombres y Apellidos del Autor	Leonardo Montilla Malaver
Año de la publicación	2020

Resumen del texto:

Las entidades del sector educativo en el orden profesional son las salvaguardas de la información educativa de sus estudiantes activos y egresados y propenden por optar estrategias para evitar los delitos informáticos[58] y de esta forma garantizar que la información que certifican es legítima y veraz, siendo este el objetivo primordial de las autoridades y funcionarios a cargo de la información académica de las universidades colombianas.

La información que estas entidades salvaguardan, tienen que ver con registros académicos, calificaciones, hojas de vida de docentes, programas, archivos confidenciales y por tal razón su custodia es imprescindible para el buen funcionamiento de las IES su credibilidad y prestigio está en juego, con el fin de revisar los factores que se relacionan con la seguridad de la información a este nivel, se propone una investigación documental sobre la situación actual de la seguridad informática, en el sector educativo universitario en los siguientes temas: 1) Seguridad de la información e informática, 2) seguridad física y lógica, 3) servicios de seguridad, 4) Marco legal que normaliza la seguridad informática en las entidades Colombianas y Normas ISO relacionadas, 5) evaluación del análisis de riesgos, mediante el análisis de esta temática se establecerá la situación sobre la seguridad informática en las IES y se propondrán como conclusiones y recomendaciones los ajustes a seguir en cada uno de los factores revisados.

[58] Huarahuara, 2009

Palabras Claves	Ciberseguridad, IES, modelos de gestión, riesgo, seguridad informática, vulnerabilidad

Problema que aborda el texto:

Con el avance de las tecnologías y su influencia en la vida social, también han surgido los delitos informáticos, los cuales ponen en peligro al usuario que tiene acceso a una red, sea este un sujeto autónomo o una organización de educación superior. En Colombia existe una legislación acerca de los delitos informáticos: la Ley 1273 de 2009, que brinda a los usuarios un control legal sobre los incidentes que se pueden presentar y que en la actualidad son frecuentes. Esta legislación permite identificar y sancionar los delitos informáticos.

Grafica No. 17 Fallas de seguridad

Fuente: Sistemas CiberRiesgo: un riesgo sistematico [59]

De acuerdo con la información planteada en la figura 1, son diversos los tipos de incidentes que se suscitan en la actualidad a nivel informativo, siendo el

[59] Martínez, J. J. (29 - 30 de agosto de 2019). Ciberriesgo: Un riesgo sistemático. (J. J. Martínez, Ed.) doi:10.29236/sistemas p.24

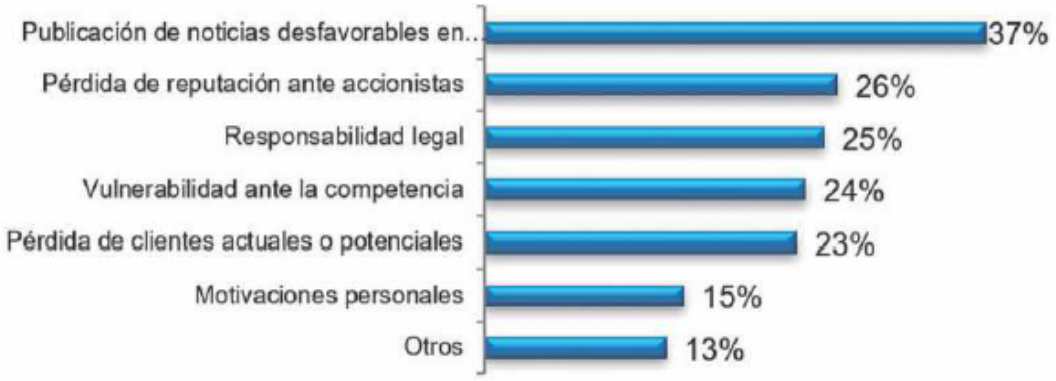
incidente que prevale con 41% se relaciona con los errores humanos y siendo el menor con 1% Pharming; desde esta perspectiva se plantea una pregunta de investigación.

Así entonces es pertinente comprender que “La evaluación de riesgo es el proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de importancia del riesgo.

El objetivo de esta evaluación es identificar y evaluar los riesgos. Los riesgos son calculados por una combinación de valores de activos y niveles de requerimientos de seguridad”[60].

Una encuesta realizada por Ciberriesgo, en el año 2019 en Colombia se determino el motivo por el cual las entidades no denuncian los incidentes contra ataques ciberneticos, ya que esto generalia perdidas economicas debido a la perdida de la imagen, reputacion y responsabilidad

Grafica No. 18 Motivos para no denunciar



Fuente: Sistemas Ciberriesgo: un riesgo sistematico [61]

[60] Freitas, 2009 Vidalina. Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Enlace* [online]. 2009, vol.6, n.1

[61] Martínez, J. J. (29 - 30 de agosto de 2019). Ciberriesgo: Un riesgo sistematico. (J. J. Martínez, Ed.) doi:10.29236/sistemas p.26

Objetivos del texto:

Objetivo General

Establecer el estado actual de las políticas y estrategias de control de seguridad informática como la legislación y normatividad vigente dirigidas hacia las instituciones públicas de educación superior (IES).

Objetivos Específicos

Reconocer los Modelos de gestión de la seguridad informática en las algunas Instituciones de educación superior IES.

Determinar las posibles causas de vulnerabilidad y el riesgo existente en los sistemas informáticos y bases de datos de las IES de las cuales se analizan los modelos de gestión de la seguridad informática.

Proponer estrategias de mejoramiento a implementar en las IES, como medidas preventivas en primera instancia a fin de salvaguardar de forma segura las bases de datos: registros académicos, calificaciones e historia académica, procesos académicos, programas e información docente, archivos administrativos información del sistema de investigación y demás información existente

Hipótesis planteada por el autor:

Todas las Instituciones de educación superior IES deben tener un modelo de gestión de la seguridad informática.

Tesis principal del autor:

Argumentos expuestos por el autor:

Tipos de seguridad: Dependiendo de las necesidades que tenga el lugar en el que se esté aplicando, sin embargo, en el caso de las universidades son la informática, la física y la lógica las que se deben tener presentes, estas podemos

determinarlas de la siguiente manera:

Seguridad Informática: Es el área del conocimiento que se dedica al diseño de normas, métodos y procedimientos que buscan conseguir un mejor. más seguro y confiable el sistema de información. (Aguilera, López,2010)

Seguridad Física: Su función primordial es lograr la protección del sistema de información mediante la utilización de limitaciones y formas de controlar físicamente el sistema evitando ataques físicos que puede provocar el hombre de forma voluntaria o accidental.

Seguridad Lógica: La seguridad lógica impide la vulneración del software sus programas y datos.

Análisis de Riesgos amenazas y Vulnerabilidades

Al momento de optimizar la seguridad informática de una organización se deben considerar varios factores como son:

- Los recursos
- Los riesgos
- Las amenazas
- Las vulnerabilidades

Conclusiones del texto:

Las universidades 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 los docentes y estudiantes 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.

Ninguna de las universidades analizadas en la presente monografía considera que la seguridad informática no es importante para el desarrollo de sus actividades y para enfrentar los retos de la sociedad de la información y el conocimiento.

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 la misma y de las múltiples posibilidades de mejora que la investigación proporcionan.

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.

Bibliografía citada por el autor:

A., C. A. (2001). *Metodologia para la Gestion de Riesgos*. Obtenido de http://www.ridsso.com/documentos/muro/207_1469148692_57916e1488c74.pdf

Acens, T. (marzo de 2015). *Bases de datos y sus vulnerabilidades más comunes.* Obtenido de https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

Almanza, A. R. (20 de 06 de 2013). *Revista Sistemas.* Obtenido de http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013

Anonimo. (s.f.). Capitulo 1 - Conceptos Basicos Networking.

Anonimo. (s.f.). Capitulo 2 - Seguridad Informatica.

Arévalo Moscoso, F. M., Cedillo Orellana, I. P., & Moscoso Bernal, S. A. (mayo - agosto de 2017). Metodologia agil para la Gestion de Riesgos informaticos. *Revista Killkana, 1*(2), 39-42. Obtenido de https://docplayer.es/127165258-Revista-killkana-tecnica-volumen-1-numero-2-mayo-agosto-2017-issn-impreso-issn-electronico.html

Barzanallana, R. (s.f.). *Introducción a la Seguridad Informática.* Obtenido de Gestión de la Seguridad en Sistemas de Información: https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf

Basaldua, L. D. (2005). Tesis Seguridad en Informatica (auditoria de Ssitemas). Mexico.

CANO M., J. J. (junio de 2019). *Ciberseguridad y ciberdefensa: Retos y perspectivas en un mundo digital.* Obtenido de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952019000200001&lng=pt&nrm=iso

Castro, R., & Irene, M. (2018). *introduccion a la seguridad informatica y el Analisis de Vulnerabilidad.* Área de Innovación y Desarrollo.

Catarina. (s.f.). *Capitulo 1 - seguridad informatica - conceptos básicos*. Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf

Cesar Duque & Asociados Consultores de Riesgos. (2011). *Metodologia para la Gestion de Riesgos.* Obtenido de Metodologia para la Gestion de Riesgos: http://www.ridsso.com/documentos/muro/207_1469148692_57916e1488c74.pdf

Colombia, C. d. (29 de noviembre de 1993). *Ley 87.* Obtenido de https://www.mininterior.gov.co/sites/default/files/ley_87_de_1993.pdf

Colombia, C. d. (27 de julio de 2000). *Ley 603 de 2000 .* Obtenido de http://derechodeautor.gov.co/documents/10181/182597/603.pdf/42c15f4a-afe5-4339-97ca-a61026450307

Colombia, C. d. (14 de julio de 2000). *Ley 594 de 2000.* Obtenido de https://www.mintic.gov.co/portal/604/articles-15049_documento.pdf

Colombia, C. d. (5 de febrero de 2002). *Ley 734 de 2002 .* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0734_2002.html

Colombia, C. d. (30 de julio de 2009). *Ley 1341 del 30 Julio de 2009.* Obtenido de https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

Colombia, C. d. (19 de junio de 2019). *Ley 1266 de 2008*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Colombia, C. d. (15 de junio de 2019). *Ley 1581 de 2012* . Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Colombia, C. d. (15 de junio de 2019). *Ley 527 de 1999*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Colombia, U. E. (s.f.). Obtenido de https://www.uexternado.edu.co/

Colombia, U. N. (s.f.). Obtenido de http://unal.edu.co/

Comunicaciones, M. d. (24 de septiembre de 2014). *Manual de Normas y Políticas de Seguridad Informática.* Obtenido de https://www2.sgc.gov.co/ControlYRendicion/TransparenciasYAccesoAlaInformacion/CircularesManuales/MO-TEC-001-I.pdf

CSIRT-cv. (s.f.). *12 medidas básicas para la seguridad Informática.* Valencia: Generalitat Valenciana.

Cundinamarca, U. (17 de mayo de 2017). *Política Global del Sistema de Gestión de Seguridad de la Información – SGSI*. Obtenido de

https://www.ucundinamarca.edu.co/index.php/politica-de-tratamiento-de-datos

Cundinamarca, U. (31 de mayo de 2018). *Establece política de tratamiento de protección de datos*. Obtenido de https://www.ucundinamarca.edu.co/index.php/politica-de-tratamiento-de-datos

Daccach, J. C. (s.f.). *Ley de Delitos Informáticos en Colombia*. Obtenido de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Digitales, T. (2017). Estructira y funcionalidad de un sistema de seguridad informatica. Puebla Mexico: Universidad de las Americas .

Distrital Francisco Jose de Caldas, U. (8 de junio de 2011). *Politicas de Seguridad de la informacion Version 0.0.1.0.* Obtenido de https://funcionarios.portaloas.udistrital.edu.co/cit/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

Distrital Francisco Jose de Caldas, U. (s.f.). *Secretaria General*. Obtenido de https://sgral.udistrital.edu.co/sgral/

Externado de Colombia, U. (3 de junio de 2015). *Centro de Investigación en Derecho Informático (CIDI)*. Obtenido de https://derinformatico.uexternado.edu.co/centro-de-investigacion-en-derecho-informatico-cidi/

FBI, F. B. (23 de marzo de 2018). *IRANI UNA MABNA HACKERS*. Obtenido de https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers

Fernandez Laviada, A. (2010). *La Gestión del Riesgo Operacional: De la teoría a su aplicación.* Madrid, España: Limusa Noriega Editores. Obtenido de https://books.google.com.co/books?id=kR33ej859OEC&printsec=frontcover

&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Freitas, V. D. (abril de 2009). *Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolíva.* Obtenido de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1690-75152009000100004&lng=es&nrm=iso

Hernánde, R. V., & Ibarra, C. M. (marzo de 2018). *Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios*. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072018000200005&lng=es&nrm=iso

Huarahuara, M. M. (2009). *Delitos informaticos*. Obtenido de http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442009000200002&lng=es&nrm=iso

Macías-Valencia, S. M.-Z. (2017). Seguridad en informática: consideraciones. *Revista Cientifica: Dominnio de las Ciencias, 3*(4), 13.

Martha Irene Romero Castro, G. L. (2018). *Introduccion a la seguridad informatica y el Analisis de Vulnerabilidades.* Área de Innovación y Desarrollo,S.L.

Martínez Clavijo, E. (s.f.). *Sistema de Gestion de seguridad de la informacion*. Obtenido de https://www.ucundinamarca.edu.co/sgc/index.php/macroproceso-estrategico/proceso-gestion-sistemas-integrados/sgsi

Martínez, J. J. (29 - 30 de Agosto de 2019). *Ciberriesgo: Un riesgo sistematico.* (J. J. Martínez, Ed.) doi:10.29236/sistemas

Nacional de Colombia, U. (10 de abril de 2012). *Acuerdo 046 de 2012 or el cual se aprueba el Plan Estratégico de Tecnologías de Información y Comunicaciones PETI*. Obtenido de

http://www.legal.unal.edu.co/rlunal/home/doc.jsp?d_i=47356

Nacional de Colombia, U. (11 de octubre de 2015). *Politicas de seguridad informatica y de la informacion.* Obtenido de https://www.dntic.unal.edu.co/images/seguridad/PolticadeSeguridadInformaticaydelaInformacion.pdf

Nacional de Colombia, U. (26 de julio de 2016). *Acuerdo 228 de 2016 Por el cual se expide política de seguridad informática y de la información*. Obtenido de http://www.legal.unal.edu.co/rlunal/home/doc.jsp?d_i=87116

Navarro, A. (14 de enero de 2009). *La seguridad informática es una realidad en Colombia*. Obtenido de http://www.icesi.edu.co/agenciadeprensa/boletines/2008/seguridad_informatica.html

Ojeda Pérez, J. E., Rincón Rodríguez, F., Arias Flórez, M. E., & Daza Martínez, L. A. (Enero - Junio de 2010). Delitos informáticos y entorno jurídico vigente en Colombia. Bogota, DC, Colombia: Cuadernos de Contabilidad.

Parra Moreno, D. A. (2012). *Gestion del riesgo en la seguridad informatica: "Cultura de la auto-seguridad Informatica".* Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/6821/ParraMorenoDuverAugusto2012.pdf?sequence=2

Pulido, J. A., Novoa, F. A., & Tamayo, D. F. (20 de mayo de 2014). *Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia)*. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292014000200007&lng=en&nrm=iso

Quiroz, S. M. (5 de julio de 2017). Seguridad informática: Consideraciones en Revista Científica Ciencias .ISSN:2477-8818.Vol 3,num 5,julio 2017,pp.676-

688. *Científica Ciencias, 3*(5), 676-688.

RAE. (2001). *Diccionario de la real academia de Español* (22 ed.). Madrid: ESPASA CALPE, S.A.

Raul J. Martelo, L. C. (Febrero de 2018). *Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia*. Obtenido de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003&lng=en&nrm=iso&tlng=en

Raúl J. Martelo, L. C. (2018). *Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia.* Obtenido de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003&lng=en&nrm=iso&tlng=en

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (Octubre de 2018). *Introducción a la seguridad informática y el Análisis de vulnerablidades.* Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Sanchez, K. G. (marzo de 2015). Tesis Analisis en seguridad informatica y seguridad de la informacion basados en la norma ISO/IEC 27001 - Sistema de Gestion de Seguridad de la Informacion Dirigido a una empresa de servicios financieros. Guayaquil.

Scopus. (12 de mayo de 2020). *Area por Profesion*. Obtenido de https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=5e796377ef0b4f8a373e902ee2e257b5&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Informatic+security%29&sort=plf-

f&sdt=b&sot=b&sl=34&count=328&analyzeResults=Analyze+results&txGid=13005

Scopus. (12 de mayo de 2020). *Publicaciones de Universidades de Estados Unidos*. Obtenido de https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=2f01071c0103fd57932ba979c535519f&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Informatic+security%29&sort=plf-f&sdt=cl&sot=b&sl=34&count=78&analyzeResults=Analyze+results&cluster=sco

Scopus. (12 de mayo de 2020). *Publicaciones en Español del 2014 al 2019*. Obtenido de https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=e7a4e3fee82f959193e3c395568969bc&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Seguridad+Informatica+%29&sort=plf-f&sdt=b&sot=b&sl=37&count=17&analyzeResults=Analyze+results&txGid=036

Scopus. (12 de mayo de 2020). *Publicaciones en Seguridad Informatica*. Obtenido de https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=5e796377ef0b4f8a373e902ee2e257b5&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Informatic+security%29&sort=plf-f&sdt=b&sot=b&sl=34&count=328&analyzeResults=Analyze+results&txGid=13005

Scopus. (12 de mayo de 2020). *Universidades de España con estudios de seguridad*. Obtenido de https://www-scopus-com.bibliotecavirtual.unad.edu.co/term/analyzer.uri?sid=e7a4e3fee82f959193e3c395568969bc&origin=resultslist&src=s&s=TITLE-ABS-KEY%28Seguridad+Informatica+%29&sort=plf-

f&sdt=b&sot=b&sl=37&count=17&analyzeResults=Analyze+results&txGid=036

Scopus. (s.f.). *Índices de impacto.* Obtenido de https://www.recursoscientificos.fecyt.es/servicios/indices-de-impacto

Senado, S. d. (13 de mayo de 2019). *Ley 1273 de 2009*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Senado, S. d. (15 de junio de 2019). *Ley 599 de 2000.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

TICbeat, R. (17 de abril de 2013). *Las 10 grandes amenazas de seguridad en las bases de datos*. Obtenido de https://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos/

Trejos Motato, J. A. (2015). *Grupo de investigación en Seguridad Informática Sapientiam*. Obtenido de http://www.itc.edu.co/archives/sapientiamgruplac.pdf

UNAD. (s.f.). Obtenido de www.unad.edu.co

Universidad Nacional Abierta y a Distancia, U. (2014). *Seguridad de la informacion - Gerencia de Innovacion y Desarrollo Tecnologico*. Obtenido de https://gidt.unad.edu.co/seguridad-de-la-informacion

Valle, U. (s.f.). *Políticas para el uso de recursos informáticos*. Obtenido de Oficina de Informática y Telecomunicaciones: http://mafalda.univalle.edu.co/politicainformatica/

Víctor Daniel Gil Vera, J. C. (junio de 2017). *Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas.* Obtenido de https://www.redalyc.org/articulo.oa?id=84953103011

Wikidot. (26 de mayo de 2015). *Seguridad Informatica.* Obtenido de

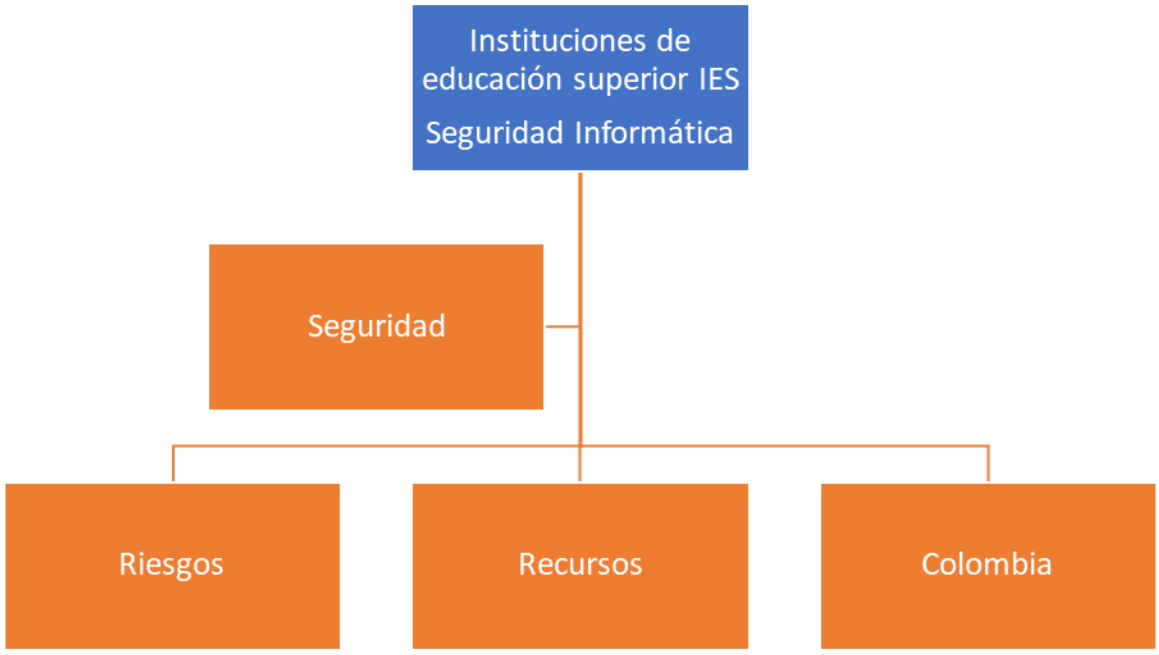
http://seguridadinformatica.wikidot.com/seguridad-informatica

Wikipedia. (25 de junio de 2019). *Información*. Obtenido de https://es.wikipedia.org/wiki/Informaci%C3%B3n

Nombre y apellidos de quien elaboró este RAE	Leonardo Montilla Malaver
Fecha en que se elaboró este RAE	Junio 04 de 2020

Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:

Grafica No. 19 Mapa conceptual de la seguridad informática en las IES



Fuente del Autor

Comentarios finales:

Todos los procesos aquí realizados y los objetivos planteados tienen como función personal, brindar un mejoramiento en mi trabajo.