MODELO DE CIBERSEGURIDAD PARA LA UNIVERSIDAD DE CARTAGENA.

JOSÉ DAVID PÉREZ GONZÁLEZ

UNIVERSIDAD SIMÓN BOLIVAR
MAESTRÍA EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
BARRANQUILLA - COLOMBIA
2020

Tesis de Maestría

MODELO DE CIBERSEGURIDAD PARA LA UNIVERSIDAD DE CARTAGENA.

JOSÉ DAVID PÉREZ GONZÁLEZ

Tesis de Maestría presentada como requisito parcial para optar el título de Magister en Ingeniería de Sistemas y Computación

DIRECTOR:

Paul Sanmartín Mendoza PHD.

UNIVERSIDAD DE SIMÓN BOLÍVAR

MAESTRÍA EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

BARRANQUILLA - COLOMBIA

2020

ÍNDICE

MODELO DE CIBERSEGURIDAD PARA LA UNIVERSIDAD DE CARTAGENA..... 1
LISTADO DE TABLAS 6
INTRODUCCION..... 7
1 IDENTIFICACIÓN (DESCRIPCIÓN) Y FORMULACIÓN DEL PROBLEMA..... 8
2 JUSTIFICACIÓN DEL PROBLEMA Y/O DE LA PROPUESTA..... 11
3 OBJETIVOS DE LA INVESTIGACIÓN Y/O DEL PROYECTO 12
3.1 OBJETIVO GENERAL..... 12
3.2 OBJETIVOS ESPECÍFICOS 12
4 METODOLOGÍA 13
4.1 ENFOQUE DE LA INVESTIGACIÓN 13
4.2 TIPO DE INVESTIGACIÓN..... 13
4.3 DISEÑO DE LA INVESTIGACIÓN..... 13
4.4 MÉTODOS DE INVESTIGACIÓN 13
4.5 TÉCNICAS PARA LA RECOPILACIÓN DE INFORMACIÓN..... 14
5 MARCO REFERENCIAL / TEÓRICO / CONCEPTUAL 15
5.1 MARCO CONCEPTUAL 15
5.2 LA CIBERSEGURIDAD Y CIBERESPACIO 15
5.3 LA CIBERSEGURIDAD EN COLOMBIA..... 18
5.4 EL RIESGO EN EL CIBER ESPACIO..... 20
5.5 DE LOS ATAQUES CIBERNÉTICOS, SUS CARACTERÍSTICAS Y GENERALIDADES..... 23
5.5.1 LOS CIBERATAQUES..... 23
5.5.2 LOS ATAQUES CIBERNÉTICOS..... 25
5.6 ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN Y EL PORQUÉ DE SU IMPORTANCIA 28
5.7 OBJETIVOS GENERALES DE LA SEGURIDAD 30
5.8 FUNDAMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN..... 31
5.9 ITIL Y SU ROL EN LA SEGURIDAD DE INFORMACIÓN. 31
5.10 METODOLOGÍA DEL COBIT EN LAS GSSI (GESTIÓN DE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN). 32
5.11 NORMATIVA ISO/IEC 27000 33

5.12 NIST CYBERSECURITY FRAMEWORK 35
5.13 REVISIÓN DE ESTADO DEL ARTE 37
6 DESARROLLO DE LA PROPUESTA 40
6.1 DIAGNOSTICO EL ESTADO DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CARTAGENA. 40
6.2 LA RED DE UN VISTAZO 41
6.3 APLICACIÓNES, ANCHO DE BANDA Y TECNOLOGÍA 41
6.4 CONCLUSIONES DEL DIAGNÓSTICO 45
6.4 CATEGORÍAS QUE INTERVIENEN EN LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD DE CARTAGENA. 46
6.5 MODELO PROPUESTO 47
6.5.1 GESTIONAR LA SEGURIDAD 65
6.5.2 GESTIONAR SERVICIOS DE SEGURIDAD 65
6.5.3 IDENTIFICACIÓN 66
6.5.4 PROTECCIÓN 66
6.5.5 DETECTAR 66
6.5.6 RESPONDER 67
6.5.7 RECUPERACIÓN 67
7 CONCLUSIONES 68
8 RECOMENDACIONES 68
BIBLIOGRAFÍA 70
ANEXOS ..... ¡Error! Marcador no definido.
ANEXO 1: NIST ..... ¡Error! Marcador no definido.
ANEXO 2: ISO 27002:2013 ..... ¡Error! Marcador no definido.
ANEXO 3: ISO 27002:2013 ..... ¡Error! Marcador no definido.

LISTA DE FIGURAS

Ilustración 1.Conmutador de banda de internet internacional. 25
Ilustración 2.ITIL 32
Ilustración 3.Principios de cobit 5. 33
Ilustración 4.Funciones del framework NIST. 35
Ilustración 5.Demanda de ancho de banda en la universidad de Cartagena 42
Ilustración 6.top de aplicaciones por categorías y número de sesiones. 43
Ilustración 7.Categoría de la aplicación y su nivel de riesgo 44
Ilustración 8.comparación con el movimiento total de volumen de datos en la universidad vs volumen de datos den aplicaciones SaaS. 44
Ilustración 9.Aplicaciones SaaS más utilizadas en la universidad de Cartagena. 45
Ilustración 10.Cantidad de EXPLOIT encontrados en la universidad de Cartagena. 45
Ilustración 11.Aplicaciones con más EXPLOIT en la universidad de Cartagena. 46
Ilustración 12.Categorías que conforman el modelo. Fuente. Autores del proyecto 47
Ilustración 13.Modelo de ciberseguridad propuesto Fuente. Autores del proyecto 48

LISTADO DE TABLAS

Tabla Recomendaciones Técnicas 23
Tabla Funciones y Categorías de NIST 35
Tabla Comparativo de estándares de seguridad de la información 64
Tabla Funciones, categorías, subcategorías y normativas de NIST 76
Tabla Objetivos ISO 27002:2013 98
Tabla Dominios ISO 27002:2013 102

INTRODUCCION

Conforme avanza el siglo XXI, los desarrollos tecnológicos atados a Internet y al campo de la computación han penetrado todos los aspectos de la vida diaria. Este nuevo escenario ha traído consigo el surgimiento de nuevas amenazas que pueden poner en riesgo a la arquitectura tecnológica. Con el aumento de la superficie de ataque vía la conectividad, la movilidad y la convergencia, los atacantes cuentan con un espacio de interacción y experimentación más amplio y este escenario se vuelve atractivo debido a que brinda un anonimato y dificulta la trazabilidad del delito, la red se ha vuelto llamativa para cometer ilícitos

El avance de las nuevas tecnologías ha traído consigo nuevos retos en materia de seguridad, es importante que se mantengan los principios de confidencialidad, integridad y disponibilidad para mantener los procesos en la organización, una cosa es clara y es que algunas características comunes, entre ellas el que no es necesario tener recursos para cometer ciertos delitos; la posibilidad de anonimato que ofrece internet y la dificultad técnica que requiere rastrear un ataque ha hecho que estas modalidades sean atractivas.

La universidad de Cartagena –UdeC- es una institución de educación superior OFICIAL y su carácter académico es el de Universidad, entidad con naturaleza jurídica pública y de estado laico, con autonomía administrativa y financiera, que ofrece una formación integral a sus estudiantes, sin distinción de sexo, raza, religión o política; por tal razón la admisión de su personal académico es realizada por la capacidad intelectual de sus candidatos aspirantes.

Existen estándares que sirven como modelos referentes para hacer frente a las nuevas exigencias de las tecnologías en cuanto a seguridad, un modelo de seguridad sirve como apoyo para lograr mitigar las amenazas y vulnerabilidades.

Esta investigación es importante toda vez que permita minimizar las amenazas y vulnerabilidades que pudieran provenir de agente tantos externos como internos, a través de un modelo que sirve como referente para salvaguardar los procesos sensibles en una organización para mitigar posibles ataques cibernéticos en los sistemas de información de la

UdeC. Es de recalcar que cada organización desde su particular posicionamiento y circunstancia tecnológica deba abordar las tareas de la implementación de ciberseguridad en sus actividades, e incluso en la de los clientes o proveedores con los que realiza intercambio de información.

1 IDENTIFICACIÓN (DESCRIPCIÓN) Y FORMULACIÓN DEL PROBLEMA

Los procesos de globalización en el mundo han jalonado diversos cambios en relación con los avances tecnológicos y sistemas de información. Estas comprenden el activo de mayor relevancia hacía un crecimiento estratégico y su seguridad debe resaltar objetivos comunes en cada proceso dentro de las instituciones. Ante este nuevo escenario los estados extienden la seguridad nacional hasta estos nuevos ámbitos.

Es así como los estados hacen frente a esta amenaza con estrategias de seguridad y por esto se planean y definen unas líneas o acciones estratégicas desde la defensa territorial, la defensa aérea, la defensa de las fronteras, la defensa económica y la ciberdefensa (Mañas, 2006). Este último, contempla la responsabilidad de proteger todo el ciberespacio y garantizar la ciberseguridad.

Sin embargo, después de dos décadas de evolución, la economía del ciberespacio parece no alcanzar los niveles de seguridad suficientes y están hoy día en jaque. Más aun, la ciberseguridad se ha convertido en la principal amenaza al comercio en el ciberespacio por lo que las naciones del mundo se enfrentan a la necesidad de dar respuesta a la problemática, no solo desde lo tecnológico, sino desde lo político y lo legal. Esta nueva realidad queda evidenciada por diferentes eventos mundiales como lo muestra la Organización para la Cooperación y el Desarrollo (OECD).

Organizaciones como Kaspersky detectaron más de 100 millones de ataques a dispositivos inteligentes en el primer semestre de 2019 Esta cifra es nueve veces mayor que la cantidad encontrada en el primer semestre de 2018, cuando solo se detectaron alrededor de 12 millones de ataques procedentes de 69.000 direcciones IP. Aprovechando la débil seguridad de los productos de IoT, los ciberdelincuentes están intensificando sus intentos de crear y monetizar botnets de IoT. Este y otros resultados son parte del informe "Internet of Things (IoT): a

malware story" (Internet de las Cosas, una historia de malware), sobre la actividad de los *honeypots* en el primer semestre de 2019 (kaspersky, 2019).

En Europa, según el Informe del Estado de la Unión 2017, el 80% de las compañías europeas sufrieron al menos un incidente de seguridad en 2016 y estos incidentes en el sector industrial crecieron un 38% respecto de 2015 (Figura 2). Además, en algunos Estados miembros el año 2016 el 50% de todos los delitos son ya Ciberdelitos, habiéndose multiplicado por cinco en los últimos cuatro años (Informe Estado de la Unión, 2017).

En América latina Kaspersky registra 45 ataques por segundo en América Latina En el último año (julio 2018- julio 2019) nuestras tecnologías bloquearon 45 intentos de infección en América Latina cada segundo. Eso significa que cada segundo, un usuario en América Latina sufre un ataque. Las principales amenazas a las que se enfrentan los usuarios en América Latina son las infecciones que ocurren con la piratería en Windows de 64 bits y el adware que invade la privacidad del usuario con anuncios invasivos durante la navegación (Latamkaspersky, 2019).

Colombia no ha sido ajena a los ciberataques, uno de los casos a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley "por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet". Este grupo ha atacado indistintamente entidades públicas y privadas, entre las que se cuentan PayPal, el banco suizo Post Finance, MasterCard, Visa y páginas web del gobierno suizo. (Información tomada del documento CONPES 3701).

Para el contexto de esta investigación, la UdeC está en proceso de realizar una gran inversión en recursos y servicios tecnológicos los cuales se materializarán con la implementación de un Datacenter de triage 2, facilitando no solamente la vida cotidiana de su cuerpo administrativo y estudiantil, sino el medio de trabajo, desarrollo y

producción de todas las personas; sin embargo, hoy en día los robos y atentados informáticos se han caracterizado por usar la innovación tecnológica con fines delictivos; estos son cada vez mayores, y el accionar de dichos ataques no solo generan pérdidas económicas, ya que sus otros intereses actualmente se encuentran enfocados en los daños contra las personas, empresas, gobiernos y sociedad en general.

En la actualidad, la información de la UdeC se encuentra en un estado de vulnerabilidad, Al no poseer un orden sistemático para afrontar este tipo de ciberataques, y se emprende un camino hacia el fortalecimiento de la arquitectura física informática y de personal humano, encontrando necesario y de prioridad reforzar este campo. En lo que hace referencia a la seguridad en los entornos digitales es importante tener en cuentes los beneficios que brinda el uso de las tecnologías de la información a la sociedad; sin embargo, es fundamental prestar especial cuidad a los riesgos que genera la utilización de ellos y, en algunos casos, la sobreexposición a los recursos mediáticos. Es, en este punto donde se formula la pregunta.

¿Cómo mejorar los procesos de seguridad de la información frente a los ciberataques en la UdeC?

¿Qué modelos y mecanismos se pueden implementar para responder a los ciberataques?

2 JUSTIFICACIÓN DEL PROBLEMA Y/O DE LA PROPUESTA

La presente investigación es importante toda vez que permita potencializar las herramientas e instrumentos operacionales a fin de propiciar herramientas clave para proteger diversos tipos de información, dada la problemática de constantes ataques cibernéticos a las bases de datos de organizaciones sociales, políticas, entre otras.

En este sentido, se proyecta el incentivo a todas las instituciones, públicas y privadas para que concentren sus esfuerzos en generar las capacidades necesarias para detectar las amenazas, identificar los ataques y prevenir que se materialicen en una afectación de sus sistemas de la información (Castro, 2018).

Por otro lado, la UdeC se beneficiaría con la construcción de una datacenter que ayuda a garantizar el manejo adecuado de la información tanto administrativa como del estudiante y así cumplir con las normas de seguridad establecidas por el ministerio de las telecomunicaciones, incentivando la expansión del portafolio de servicios. En un caso más específico la universidad podría monitorear el incremento del tipo y número de amenazas informáticas, monitorear el incremento del tipo y número de amenazas informáticas y determinar normas y regulaciones orientadas a la protección de la información.

En realidad, este tipo de proyectos fomenta la consciencia cibernética a toda la comunidad académica garantizando que su productividad intelectual esta resguardada con altos estándares de seguridad, por lo tanto, es menester que los usuarios de servicios combinen la voluntariedad y la sensibilidad para definir una actitud de privacidad frente a los servicios digitales (Fundación telefónica, 2006). De esto se puede aseverar que al aumentar el número de usuarios que acceden al portafolio de servicios la universidad podría extender la cobertura estudiantil con programas no presenciales y virtuales. En un sentido más amplio tomar este

modelo de seguridad cibernética posibilita fomentar una red bidireccional universitaria que contribuya con el desarrollo de área de ciberseguridad, que tendría como misión el análisis y propagación de incidentes en toda la comunidad universitaria, creando nuevos modelos de seguridad de la información.

3 OBJETIVOS DE LA INVESTIGACIÓN Y/O DEL PROYECTO

3.1 OBJETIVO GENERAL

Proponer un modelo de seguridad informática para mitigar posibles ataques cibernéticos en los sistemas de información de la Universidad de Cartagena.

3.2 OBJETIVOS ESPECÍFICOS

1. Diagnosticar el estado de los procesos de seguridad de la información de la universidad de Cartagena.
2. Definir teóricamente las categorías que intervienen en los procesos de seguridad de la información en la Universidad de Cartagena.
3. Diseñar una estructura relacional de categorías para la implementación de procesos de seguridad informática en la Universidad de Cartagena

4 METODOLOGÍA

4.1 ENFOQUE DE LA INVESTIGACIÓN

Se pretende alcanzar los objetivos mediante la realización de una investigación en sitio. El modelo de investigación será sistémico estructural y a su vez un enfoque holístico en investigación que surge como respuesta a la necesidad integradora delos diversos enfoques, métodos y técnicas, que desde diversas disciplinas científicas han permeado el desarrollo del conocimiento científico, buscando analizar las mejores políticas de ciberseguridad partiendo desde la situación actual de los modelos de respuestas tempranas a incidentes de seguridad informática que ya se hayan puesto en marcha y que se tomaran como casos exitosos.

4.2 TIPO DE INVESTIGACIÓN

En el vigente trabajo se utilizará un tipo de investigación proyectiva. Según (de Barrera & Morales, 2000) "consiste en la preparación de una propuesta o de un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y las tendencias futuras".

4.3 DISEÑO DE LA INVESTIGACIÓN

Estudios que incluyen la investigación holística han validado que dichas investigaciones permitan desarrollar una clasificación coherente de los diseños de investigación. El diseño hace referencia a las decisiones que se toman en cuanto al proceso de recolección de datos lo que garantiza la validez interna de la investigación, es decir, tener un alto grado de confianza de que las conclusiones son correctas (Hurtado, 2007).

4.4 MÉTODOS DE INVESTIGACIÓN

El método de investigación que se utilizará para el desarrollo del objetivo central será sistémico estructural dando un enfoque holístico. Que conlleva a contemplar el eje problemático como un todo.

El Método Sistémico Estructural expresa la lógica o sucesión de procedimientos seguidos por el investigador en la construcción del conocimiento, a través del esquema de categorías,

sus definiciones, relaciones y funciones asociadas con la seguridad de la información. Por otra parte, el modelo holístico proporciona una visión compleja para el desarrollo de la investigación, con un proceso global, integrador, evolutivo, concatenado y organizado reforzado el primero método ya mencionado (de Barrera & Morales, 2000).

Su meta no se limita a la recolección de datos, sino a la predicción e identificación de cual serán las mejores políticas de seguridad que se amoldarían al entorno socio cultural de nuestra región, para lograr alcanzar cada uno de los objetivos.

Se recogerá los datos sobre la base de los paradigmas investigativos y problemáticas planteadas previamente, se expondrá y resumirá la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de proponer el modelo (políticas) más propicio (Van Dalen & Meyer, 2006).

4.5 TÉCNICAS PARA LA RECOPILACIÓN DE INFORMACIÓN

Inicialmente se acudió a las técnicas de observaciones (recolección de datos) que permitan formar una idea sólida del estudio de la investigación que se está planteando, de allí la necesidad de utilizar la técnica de clasificación que permitió agrupar las políticas que mejor se amolden a nuestros objetivos y por último la técnica de definiciones, ésta no proporcionara las estructuras finales de nuestro objetivo principal.

5 MARCO REFERENCIAL / TEÓRICO / CONCEPTUAL

5.1 MARCO CONCEPTUAL

Ciberseguridad. La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber-entorno.

Seguridad de TI. La seguridad de TI protege la integridad de las tecnologías de la información (como los sistemas informáticos, las redes y los datos) de los ataques, los daños o el acceso no autorizado. Una empresa que intenta competir en un mundo de transformación digital debe comprender cómo adoptar las soluciones de seguridad que comienzan con la etapa de diseño. A eso nos referimos con "desplazar la seguridad a la izquierda" (shift left): hacer que la seguridad sea parte de la infraestructura y del ciclo de vida del producto lo antes posible. Esto permite que la seguridad sea proactiva y reactiva (Redhat, 2020).

Seguridad de la información. La seguridad de la información está definida como todas las medidas preventivas y de reacción del individuo, la organización y las tecnologías, para proteger la información; buscando mantener en esta la confidencialidad, la autenticidad e Integridad (unilibre, 2015).

Gobierno de TI.

Este dominio brinda directrices para implementar esquemas de gobernabilidad de TI y para adoptar las políticas que permitan alinear los procesos y planes de la institución con los del sector (Mintic, 2020).

5.2 LA CIBERSEGURIDAD Y CIBERESPACIO

La ciberseguridad es un ámbito que es transversal en todos los procesos de los sistemas y comunicaciones tales como: redes, bases de datos, autenticación, desarrollo de aplicaciones, entre otros, de ello se desprende la búsqueda de contextos seguros para hablar finalmente

hablar de ciberseguridad (Díaz et al., 2018). Por eso las organizaciones son más conscientes de los impactos que les pueden generar los riesgos referentes a las Tecnologías de Información dado las perdidas por los ataques a sus sistemas.

Según(Galán & Cordero) en su artículo destaca que "La ciberseguridad pública como garantía del ejercicio de Derecho & Sociedad", el término "Ciberseguridad", exponen un concepto ambiguo sobre su definición, y cito: "no es un concepto de fronteras perfectamente definidas; muy al contrario, en su configuración intervienen, se superponen, se integran y, en ocasiones, se erosionan mutuamente, conceptos, métodos, procedimientos, herramientas y regulaciones que construyen una realidad multiforme y multidisciplinar (p.25)." Adicionalmente estos autores agregan que el ciberataque es en si la convergencia de muchas actividades de la contraparte, pero no especifican un concepto como tal.

La ciberseguridad parece tener muchas definiciones una de ellas es la aportada por la Unión Internacional de Telecomunicaciones (ITU, 2010):

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno (p.)

En el mismo sentido, la ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información) expone que la ciberseguridad puede entenderse como la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (p.18).

La ITU (unión internación de telecomunicaciones), propone que la ciberseguridad requiere un esfuerzo sistemático y coordinado en la organización, y establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cualquier sector, sea industrial, académico, bancario o gubernamental.

Todo lo anterior complementándolo con un marco legal para las acciones, desarrollo y aplicación de medidas técnicas, procedimientos, diseños y aplicación de estructuras

organizacionales requeridas, que posibiliten la implementación de aplicaciones (software), e incentivando de una cultura de ciberseguridad y la cooperación regional. (Schjolberg, 2008).

En realidad, con muchos los autores los que proponen en sus trabajos de investigación que la ciberseguridad en los sistemas de información de las universidades es primordial. Es así, como Ibarra & Nieves (2016) exponen sobre la cantidad de trabajo faltante que hay que hacer sobre la ciberseguridad y sobre uno de los desafíos más importantes que sería el lograr un compromiso real de los Estados en la generación de políticas públicas específicas, y en la construcción de una cultura de ciberseguridad.

Según Betancourt (2017) para alcanzar este propósito, primero deben realizarse articulaciones y llegar a puntos de convergencias desde las organizaciones internacionales afines, el sector público y privado, de manera de ofrecer a los Estados herramientas efectivas, tanto de protección y cuidado de los individuos, como de lo que se considera información crítica para los gobiernos.

Se podría asegurar que la ciberseguridad es un componente crucial actualmente en la seguridad nacional de los países, pues si no se controla el ciberespacio, desde allí pueden darse acciones amenazantes que dejen en vilo la seguridad de toda una nación (Feliu, 2012). Por lo tanto, es importante focalizar las acciones sistemáticas sobre el "ciberespacio" dado que es un lugar estratégico para planear la defensa nacional. Por consiguiente, se debe definir desde estas algunas medidas de prevención, disuasión, protección y reacción.

Desde un punto de vista estrictamente tecnológico según Pérez (s.f) el ciberespacio serían las infraestructuras técnicas de un conjunto de un conjunto interconectado de redes de información tato públicas como privadas incluyendo internet. A esto se le adicionan enlaces físicos y protocolos y controladores de comunicaciones, los sistemas de ordenadores, entre otros aspectos que afectan la función tecnológica en el espacio.

En realidad, la complejidad de esta infraestructura global va extendiéndose en diferentes aspectos tales como: televisores, teléfonos inteligentes, electrodomésticos, los sistemas de control remoto para la supervisión y mantenimiento de sistemas industriales, las redes compartidas.

5.3 LA CIBERSEGURIDAD EN COLOMBIA

De acuerdo con Agudelo, (1997) Colombia se han presentado muchos avances en esta materia con la aplicación de un marco normativo y acciones desde el Estado para la protección de la seguridad nacional y de los sistemas de información, he aquí un recuento.

- Desde el manual 3.0 del Gobierno en línea, el ministerio de las TICs. El ministerio de las TICs genero una serie de directrices en temas de seguridad de la información basadas en estándares internacionales.
- En Colombia se presentó una disminución de los delitos cibernéticos en 2012.
- El grupo de respuestas a emergencias cibernéticas participo del ejercicio de gestión de crisis organizado por el comité interamericano contra el terrorismo.
- Colombia se posiciona como líder en latino américa dado que posee una política nacional de seguridad cibernética.
- Colombia elaboró el DOCUMENTO CONPES 3701, el cual establece parámetros de seguridad nacional cibernética y establece políticas de ciberseguridad y ciberdefensa.

El último aspecto en mención fue una gran evolución en términos de colocar al país a la vanguardia al plantear una Política de Seguridad Digital que articulo a través de un modelo eficiente la visión integral de todos los sectores que en el país giran alrededor de las instituciones públicas del Estado Nacional.

En respuesta a estos ataques que atentaron contra la seguridad nacional en el año 2011 el gobierno colombiano, elaboró el CONPES 3701 (Consejo Nacional de Política Economía Social), máximo organismo de coordinación de la política económica en Colombia. El CONPES 3701 el 14 de julio del 2011, que trata sobre los “Lineamientos De Política Para Ciberseguridad Y Ciberdefensa” de Colombia, el cual busca generar lineamientos de política en ciberseguridad y ciberdefensa tendiente a desarrollar una estrategia nacional para contrarrestar el crecimiento de las amenazas informáticas que afectan significativamente al país. Asimismo, recopila antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

El resultado de esta nueva línea de ciberdefensa fue muy sólida, innovadora, creativa y siempre actualizada, no solo para prevenir ataques informáticos contra instituciones estatales, sino para poder estructurar una ciberdefensa activa, algo que se debe hacer para la defensa del TI gubernamental. La ciberdefensa que se implemente debe ser proactiva, dinámica y al día con las amenazas que puedan llegar. Debe ser un laboratorio con un radar digital que permita ver en forma oportuna las posibles amenazas.

En este sentido el CONPES 3701(2011) tiene varios propósitos:
a. Fortalezca la capacidad institucional, normativa, administrativa y de gestión con el fin de abordar los temas de seguridad digital desde el más alto nivel, concientizando y capacitando a todos los actores de interés.

b. Construya una estrategia nacional de seguridad digital que genere confianza y fomente el uso del entorno digital, en línea con sus valores fundamentales, y desarrolle un modelo de cooperación eficiente involucrando a todos los actores de interés en el marco de la gestión de riesgos de seguridad digital, con el objetivo de maximizar los beneficios económicos y sociales en todos los sectores económicos.

c. Proteja los derechos fundamentales y las actividades económicas y sociales que realicen sus ciudadanos en el entorno digital, incremente el combate al crimen y la delincuencia en el entorno digital e implemente mecanismos de asistencia a víctimas de delitos en ese entorno.

d. Asegure la defensa de sus intereses fundamentales y refuerce la seguridad digital de sus Infraestructuras Críticas Nacionales con un enfoque de gestión de riesgos.

e. Participe activamente a nivel nacional e internacional en la promoción de un entorno digital abierto, estable y confiable, y en la cooperación, colaboración y asistencia respecto de la gestión de riesgos de seguridad digital.

Desde la creación del CONPES 3701 de 2011, Colombia empezó a estructurar una ciberdefensa sólida, innovadora, creativa y siempre actualizada, no solo para prevenir ataques informáticos contra instituciones estatales, sino para poder estructurar una ciberdefensa activa. La ciberdefensa que se aplique debe ser proactiva, dinámica y al día con las amenazas que puedan llegar. Debe ser un espacio de prácticas y pruebas que permita ver en forma anticipada las posibles amenazas (Benavides, & Flor, 2019).

Adicionalmente, dentro de los aspectos más resaltantes del CONPES 3701 (2011), está la conformación de la Comisión Intersectorial, con representación del Ministerio de Defensa Nacional con el ColCERT, el Comando Conjunto Cibernético (CCOC) en el Comando general de las FFMM y finalmente el Centro Cibernético Policial (CCP) a cargo de la Policía Nacional:

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert), encargado de coordinar a escala nacional los aspectos de ciberseguridad y ciberdefensa.

a. El Comando Conjunto Cibernético de las Fuerzas Militares, (CCOC) que tendrá la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio.

b. El Centro Cibernético Policial, (CCP) que estará a cargo de la prevención e investigación y apoyará la judicialización de los delitos informáticos. Para ello, contará con un comando de Atención Inmediata Virtual (CAI Virtual), para recibir las denuncias de los ciudadanos.

5.4 EL RIESGO EN EL CIBER ESPACIO

El surgimiento de Internet y los medios informáticos instauró un antes y un después en la accesibilidad de los sistemas de información, donde cada acción se halla reflejada, pues la red es un nuevo espacio donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día (García, 2015). Por lo tanto, el impacto en las relaciones sociales, económicas y políticas no pasan desapercibidas y esto merece del mayor de los cuidados para mantener y surgir en el nuevo orden social.

Por tal motivo a este inicio el uso del Internet generó comportamientos tanto positivos como negativos. Durante el periodo de crecimiento de las redes informáticas, los denominados ciberdelincuentes progresaron a pasos agigantados desarrollando técnicas y métodos para vulnerar los sistemas de seguridad, aún inmaduros, tomando ventaja sobre las autoridades y su escasa preparación para abordar este nuevo problema.

La apertura del ciberespacio hace que deba realizarse una reconceptualización de la seguridad en sus diferentes niveles, nacional, regional, y global. La gestión de riesgos se consolida como una herramienta estratégica de la ciberseguridad destinada a reducir la incertidumbre y la impredecibilidad definida por las relaciones y las tensiones internas y externas.

La gestión de riesgos es un proceso que posibilita el tratamiento y la disminución de las vulnerabilidades frente a las amenazas existentes. (Mosso, 2015).

Por otra parte "digitalización de la sociedad" exige garantizar que las herramientas tecnológicas utilizadas tienen la capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas prestan o hacen accesibles (Galán & Cordero, 2016).

Pero alrededor de todos aspectos siempre surgen incomodidades y dificultades relacionados con la ciberseguridad, sin embargo, gran parte de los internautas piensan que la mayor amenaza en la red es que te roben datos personales y las claves, pero lo cierto es que un atacante puede querer acceder a los recursos del usuario para aprovecharse del poder de procesamiento con el fin de realizar tareas que requieran gran poder de computación, o bien puede robarle su ancho de banda para que su sistema actúe como un zombi dentro de una *botnet* y poder realizar ataques masivos. (Rodríguez, Flores, López, &)

El hecho de conocer los marcos de referencias para el análisis de riesgo no asegura que el proceso se lleve a cabo en forma exitosa. Por lo tanto, se requiere de una metodología que en forma eficaz y eficiente aplique los marcos de referencias exitosamente en la labor del análisis de riesgos de TI. Lo anterior conlleva a que se identifiquen y prioricen exhaustivamente los diferentes riesgos para definir planes de acción y de protección, acordes con cada uno.

En este sentido del análisis del riesgo en el ciberespacio Gómez, Pérez, Donoso, & Herrera (2010) plantean que la labor en general no es una tarea fácil, ya que involucra un estudio detallado de todas las áreas de la organización y un análisis crítico que garantice la adecuada identificación y priorización de los riesgos y vulnerabilidades. Se hace necesario, entonces, contar con metodologías que faciliten el logro de estos objetivos de altos volúmenes de información.

Ahí mismo Gómez et al., (2010) en su artículo "*Methodology and Governance of the IT Risk Management"* expone que en las organizaciones hoy en día son conscientes de la necesidad de identificar los riesgos asociados a TI, pero también es claro que al tener esta

preocupación y no aplicar una metodología adecuada para cada negocio es imposible lograr que estas metodologías alcancen sus metas de minimizar los riesgos.

Por estos autores, bajo este mismo parámetro, tocan un punto primordial para la gestión de riesgo general, y que la estrategia aplicada en una organización puede ser que no funcione para otra. Para ejercer bien la metodología se debe tener en cuenta la misión de la organización, tenga ánimo de lucro o no, además de eso el saber aplicar las normativas mínimas que están estandarizadas, y para ello es válido conformar políticas o gestionar con apps o software.

Pero García, (2017) hace una breve exposición de técnicas que facilitan esta actividad basadas en la ISO 31010 es un estándar sobre gestión de riesgos codificado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, ofrece recomendaciones sobre la selección de técnicas de valoración del riesgo. Ver tabla 1

Tabla. Recomendaciones Técnicas

TECNICA	SIGLAS	OBJETIVO
Check-lists		Esta técnica proporciona una lista de las incertidumbres típicas a considerar. Los usuarios se refieren a una lista previamente desarrollada, códigos o normas.
Structured SWIFT		Técnica estructurada "¿Y si...?"). Plantea las perspectivas de lo que pasaría si determinado riesgo se transforma en problema. Elabora soluciones anticipadas a riesgos detectados en el *brainstorming* .
ANÁLISIS DE ÁRBOL DE FALLAS		Esta técnica se inicia con un evento no deseado y determina todas las maneras en las que podría ocurrir. Estos eventos se muestran gráficamente en un diagrama de árbol lógico. Una vez que el árbol de fallas se ha desarrollado, debe considerarse la posibilidad de formas de reducir o eliminar las posibles causas/fuentes.
Diagrama causa-efecto		Un efecto puede tener un número de factores que se pueden agrupar en distintas categorías. Estos factores se identifican a menudo a través del intercambio de ideas y se muestran en una estructura de “espina de pescado”. Permite conocer la raíz del problema y cuellos de botella en procesos.
Análisis Modal de Fallos y Efectos	AMFE	Esta técnica identifica y analiza los fallos potenciales, mecanismos y los efectos de esos fallos. Entre otros, se utiliza para el diseño de componentes y productos, sistemas, procesos de fabricación y montaje, servicio y software.
Análisis funcional de operatividad	HAZOP	Se trata de un proceso general de identificación de riesgos para definir posibles desviaciones del rendimiento esperado o deseado. Se utiliza para detectar situaciones de inseguridad en plantas industriales, debido a la operación o a los procesos productivos.
Análisis de capas de protección	LOPA	Permite la evaluación de controles, así como su eficacia.

Fuente: tomado textualmente de: (GARCÍA, 2017) https://www.ealde.es/herramientas- evaluacion-de-riesgos/

5.5 DE LOS ATAQUES CIBERNÉTICOS, SUS CARACTERÍSTICAS Y GENERALIDADES

5.5.1 LOS CIBERATAQUES

El surgimiento del internet en 1969 nace al mismo tiempo la terminología que conocemos en informática como el conjunto descentralizado de redes de comunicación que están interconectadas y que utilizan la familia de protocolos TCP/IP (trasmisión control

protocolo/internet protocol), aquellas las cuales garantiza que las redes físicas híbridas que la componen formen una red lógica única de alcance mundial. Es interesante recordar que "la red de redes nació de la idea y de la necesidad de establecer múltiples canales de comunicación entre ordenadores" (Gamon, 2017) (Chicharro Lázaro, 2009).

Según Carlini (2016) la aparición del internet y su expansión ha demostrado ser una de las revoluciones tecnológicas más importantes de la historia contemporánea, puesto que ha acoplado todos los ámbitos de las sociedades, en el que queda muy difícil no adoptarla para los procesos de ejecución de tareas. Sin embargo, las tareas que allí se realizan desde diversas fuentes algunas poseen alto valor y confidencialidad lo que hace surgir redes e intentos criminales para aniquilar o romper la seguridad digital de un país, persona individual o una organización.

Por consiguiente, es menester hacer referencia a varias definiciones importantes como es el ciberataque, así: un delito informático, es toda aquella acción ilícita que se da por diferentes factores informáticos el cual tiene como objetivo dañar todo tipo de hardware, software y redes de Internet. (KasperskyLab, 2018a)

De otra parte, la (*Federal Bureau of Investigación*) FBI lo define como el" ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos." (FBI, 2016)

Para poder ahondar en estas definiciones es necesario partir de que el mismo ciberespacio propicia la clandestinidad, el anonimato, fácil acceso, poco o ningún control gubernamental, rápido flujo de información, indetectable, bajos costos, bajos riesgos y alto impacto por el poder en términos de la capacidad de destrucción, disrupción, mal funcionamiento o toma de control de sistemas tecnológicos y sus consecuencias (Villanueva Méndez, 2015).

En lo más directo la amenaza cibernética en una preocupación presente y futura para los Estados, más aún, cuando la dependencia tecnológica es una realidad inevitable, con la cual necesariamente tendrán que convivir los ciudadanos y la sociedad, y sobre la que se soporta cada vez más la actividad económica y social de los países (Villanueva Méndez, 2015).

Leiva (2015) sintetiza que, al aumentar la dependencia de las TICs, la protección y la disponibilidad de estos activos críticos se convierten cada vez más en un tema de interés nacional. En sí, el ciberespacio seguro se ha convertido en uno de los retos más importantes del siglo, y por lo tanto la seguridad informática se considera cada vez más como una cuestión nacional a nivel estratégico que afecta a todos los niveles de la sociedad.

5.5.2 LOS ATAQUES CIBERNÉTICOS

La globalización del ciberespacio, en el hábitat delictivo ha crecido exponencialmente, pues la era de la información acrecienta las oportunidades de los delincuentes (Pons, 2017). El aumento de la conectividad a Internet provoca que cada vez más personas estén conectadas en un espacio público y transaccional, como lo confirma Brahima Sanou director de la (ITU) exponiendo que el uso de la Internet creció en todo el mundo en un 32% entre 2015 y 2016.

África es el continente con un aumento del 72% durante este período, el más alto de todas las regiones. Señalando el de crecimiento que permite el avance de la comunicación, la colaboración y la innovación; sin embargo, los ataques cibernéticos y el robo de información crítica se han convertido en una gran amenaza derivado de las consecuencias económicas y sociales que conllevan (López, 2015).

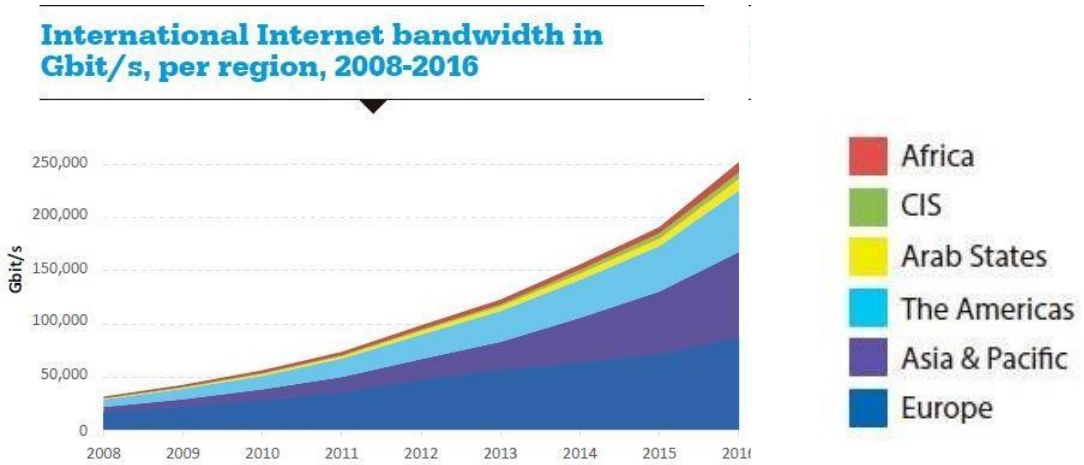

Ilustración 1.Conmutador de banda de internet internacional. Fuente: tomado textualmente de: (ITU, 2017) Disponible en: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

De acuerdo a Machín & Gazapo (2016) los ataques cibernéticos a nivel internacional, han hecho que la ciberseguridad está cobrando unos marcados matices de relevancia y de urgencia, a medida que la economía digital se ha ido desarrollando en los últimos 15 años, las empresas, así como los consumidores son más dependientes que nunca de los sistemas de información.

Así mismo, la relevancia de la ciberseguridad sigue viéndose incrementada debido a la aparición de una nueva ola de sistemas ciber-físicos como son los dispositivos "inteligentes" para el hogar, vehículos autónomos y sistemas aéreos no tripulados, el internet de las cosas; sin embargo, en este contexto de transformación digital, es cada vez más claro que tanto el público como el sector privado no pueden seguir el ritmo de las amenazas de ciberseguridad.

Es por ello que dependiendo de la meta que se desee alcanzar o el daño que se desee provocar, veremos que los ciberataques pueden presentarse de diferentes maneras. Para alcanzar sus objetivos, el ciberdelincuente o los ciberdelincuentes utilizan una serie de técnicas básicas, las cuales se aplican individualmente o de forma combinada. Entre las técnicas más habituales (Urueña Centeno, 2015), se podrían citar:

Por otro lado, los virus informáticos, que comúnmente son conocidos como programas de carácter malicioso, que pretenden infectar a otros archivos contenidos en el sistema, con el objeto de producir modificaciones o daños en el sistema informático que han infectado. El archivo infectado con el virus se denomina “víctima”. El virus introduce en los archivos infectados una secuencia de código malicioso, dirigida fundamentalmente a los archivos ejecutables del sistema atacado. A cada ejecución de estos archivos, se produce una propagación del virus, infectando a nuevos archivos y multiplicando sus efectos. (Urueña Centeno, 2015)

En correspondencia con lo anterior, un segundo tipo podría estar clasificado como los programas de Spam, (KasperskyLab, 2018b), el cual se define en la teoría como un anónimo, correo electrónico masivo no solicitado. Siendo así se dan diferentes formas de ataques que dañan o destruyen información, a continuación, algunos de ellos:

Spoffing: IP Spoofing es una técnica que permite que un atacante adopte la identidad de un host "confiable" (modificando su dirección IP por la dirección de éste) y obtenga de este modo accesos no autorizados a otros sistemas. En numerosos sitios (bajo Unix o Linux), existe un archivo denominado rhosts que contiene una lista de nombres de hosts que se consideran de confianza. Si un atacante se hace pasar por una de esas direcciones, puede llegar a ejecutar comandos en forma remota o iniciar sesión en el sistema aún sin disponer de una contraseña. (pandasecurity, 2007).

El envío o instalación de archivos espías o Keyloggers: como su nombre indica un Keylogger es un programa que registra y graba la pulsación de teclas y, algunos, también los clicks del ratón. La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware o bien aplicaciones (software) que realizan estas tareas. (Urueña Centeno, 2015).

El uso de Troyanos para el control remoto de los sistemas o la sustracción de información: troyano oculta software malicioso dentro de un archivo que parece normal. Hay una gran cantidad de virus troyanos en Internet que pueden realizar diversas tareas. La mayoría de los troyanos tienen como objetivo controlar el equipo de un usuario, robar datos e introducir más software malicioso en el equipo de la víctima. Como ejemplos de troyanos tenemos Back Orifice 2000, SubSeven, Cybersensor, DeepThroat v2, Dolly Trojan, Girlfriend, nCommand v1.0, NetSpher. (Symantec, 2018).

El uso de Rootkits: el objetivo principal de un rootkit es ocultar programas y datos. La amenaza surge cuando los ciberdelincuentes hacen uso de esta técnica y logran ocultar su presencia en el sistema durante un período de tiempo prolongado, generalmente mayor que cualquier programa maligno de los conocidos hasta el presente. (Gil, 2018)

Mediante el uso de las técnicas mencionadas, los ciberdelincuentes hacen uso de alguna de ellas o la combinación de varia convirtiéndolas en ciberataques consiguiendo una serie de efectos que perjudican, inhabilitan o provocan intrusiones en los sistemas de información, dentro de los ciberataques más conocidos están los siguientes:

Cambios en las direcciones de dominio (DNS): el cambio de dominio significa que la página web o un servicio determinado al que quiere acceder, va a tener otra dirección, por

lo que los usuarios o el mismo propietario no tendrían acceso a un determinado recurso, provocando un grave perjuicio, dependiendo del ámbito de dicho servicio. (Urueña Centeno, 2015).

Los ataques por denegación de servicio (DoS, Denial of service): hacen que sea imposible el acceso a los propios recursos y servicios de una organización o empresa y posteriormente solicitan un rescate para detener los ataques. (Gamon, 2017). Con ellas se pueden crear muchas conexiones simultáneas o enviar paquetes alterados para multiplicar los accesos. También permiten modificar los paquetes poniendo como IP de origen una IP falsa, de forma que no pueden detectar quién es el atacante real. (Urueña Centeno, 2015)

Todas estas técnicas y ataques describen de forma global los aspectos ilícitos cometidos en el ciberespacio están compuestas por cuatro características específicas: "se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, debido a su nula voluntad política de tipificar y sancionar estas conductas". (Subijana Zunzunegui, 2008).

Los ciberataques actualmente son conformados por grupos de personas con conocimiento en informática que no necesariamente deben estar en un lugar geográficamente para conformar un ataque masivo, es tan solo lograr un acuerdo para realizar una serie de ataques combinados utilizando las estrategias mencionas u otras, de acuerdo al nivel de seguridad que la organización tenga, o el tipo de daño que quieran ejecutar.

5.6 ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN Y EL PORQUÉ DE SU IMPORTANCIA

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los inconvenientes más grandes desde la aparición y globalización del Internet. Dado el impacto mediático del internet en la sociedad y sus innumerables aplicaciones y usos, encaminaron las personas y las organizaciones a considerar la necesidad de expandir servicios,

conocimientos, sentimientos, productos, etc. A adherirse a este mundo. (Gómez Fernando, 2007)

La tendencia cada vez es imperiosa hacia la interconectividad y la interoperabilidad de las redes, de los equipos computacionales, de las aplicaciones e incluso de las empresas, ha situado la seguridad de información como elemento primordial en todo el desarrollo de la sociedad. (Bertolín, 2008)

Ciertamente, la palabra Seguridad (denominación que se refiere a una disciplina amplísima que abarca los sistemas de protección física, la prevención de accidentes, o la prevención de actividades desleales por parte de los empleados), no es una función desconocida de las empresas, ni una necesidad sobrevenida por el uso de Redes Telemáticas, pero sí es cierto que recientemente merece mayor atención por parte de los administradores de redes. (Gómez Fernando, 2007)

Al analizar la normativa según la **ISO27001,** la seguridad de la información se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes de una organización (ISO, 2013), dicha información se debe manejar con la importancia que le pertenece independientemente del formato que se maneje, estos pueden ser: Electrónicos, en papel o audio y vídeo, etc. La seguridad de la Información se ha desarrollado mucho en estos últimos tiempos, además ha evolucionado considerablemente. Se ha convertido en una carrera acreditada mundialmente (ISO, 2013).

Revisando varias definiciones expuestas por los autores citados; concuerdo con los mismos. Debido que en la actualidad nuestra sociedad y su globalización informática cada vez más dependiente, involucra muchos factores que de carácter personales (individuo) u organizacionales (estado, empresa) importantes para ambos bandos, que conciben como elementos importantes el área de la seguridad informática y todo lo que en ella se maneja.

Sin menospreciar los temas personales, la Gestión de la Seguridad en los Sistemas de Información (GSSI) refiriéndonos a las organizaciones, denota más relevancia debido a los avances tecnológicos continuos que tenemos día a día. La fuga de información en la empresa en el siglo XXI es habitualmente la ruina de estas mismas. Estos hechos generan que expertos

en las áreas de gestión de información (GSI) unidos al área de seguridad informática, de en aras de minimizar estas vulnerabilidades desarrollan nuevas normativas de seguridad para preservar y resguardar la información, no solamente con dispositivos de hardware y software. Sino con interconexión del personal organizacional y políticas estratégicas que conllevan a disminuir los problemas en los ámbitos de desarrollo empresarial.

5.7 OBJETIVOS GENERALES DE LA SEGURIDAD

Dejando claro que la seguridad de los sistemas de información es una disciplina en continua evolución. Esta tiene como objetivo final permitir que una organización cumpla con su misión, implementando estrategias sistémicas que tengan un especial cuidado y consideración hacia los riesgos relativos a las TIC de la organización, a sus socios comerciales, clientes, administración pública, suministrados, etc. (Bertolín, 2008)

La seguridad en los sistemas de información debe cumplir con 3 objetivos primordiales como lo es la confidencialidad, que está definida como la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados. La Integridad, siendo la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada, y finalmente la disponibilidad, siendo una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones. (Gómez Fernando, 2007).

El no mantener una figura de en el esquema organizacional que se encargue de cumplir con estos principios, certifica que la Seguridad en los Sistemas de Información está viciada y se convierte en un sistema no confiable, (ANDRES, 2018) en su tesis “Equipo de respuesta ante incidentes de seguridad informáticos para la universidad regional autónoma de los andes “unidades” habla que sobre la falta de coordinación y el no cumplimiento de estos objetivos, evidenciando la inexistencia de control acarreando un crecimiento no dimensionado de problemáticas en la perdida de información, denominadas “incidentes”.

5.8 FUNDAMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

Toda organización para su crecimiento y valoración, requieren como factor importante de producción el desarrollo de tecnologías y metodologías que permitan el control del portafolio de servicios. Existen algunos modelos de metodologías ágiles que permiten el correcto funcionamiento de la gestión de servicios informáticos (Armendáriz, 2017).

Al hablar del enfoque que se le ha trasmitido a la gestión de seguridad de los sistemas de información, es natural para un individuo que no esté inmiscuido en el área de sistemas, que la primera idea que le viene en mente sea una solución o soluciones operativas, que trate los retos presentados por las TI (tecnologías de información) de esa forma. Pero si se logra cambiar esa a perspectiva a nivel organizacional mejoraremos el desempeño y obtendremos una ventaja estratégica como es el apoyar en prevenir incidencias futuras en nuestros SI.

La seguridad de información ha sido regulada por organismos internacionales como la ISO/IEC 27000, metodologías agiles como el COBIT v5 nos permiten realizar la evaluación de la gestión de tecnología de información a través del entorno de auditoría y estrategias como como ITIL que permiten optimizar nuestras prácticas en Gestión de servicios de tecnología de la información (ITSM) y garantizar un correcto funcionamiento del modelo de gestión de las Tecnologías de Información.

Analizaremos los tres fundamentos que coadyuvan a desempeñar una buena gestión de la seguridad de la información.

5.9 ITIL Y SU ROL EN LA SEGURIDAD DE INFORMACIÓN.

Es un marco de trabajo público de las mejores prácticas destinadas a gestionar la entrega de servicios de tecnologías de información (TI) sistemáticamente alineados y en concordancia con el negocio.

Nos da una información detallada de los procesos más trascendentales que debe llevar a cabo cualquier organización de TI, así como, procedimientos y métodos para la implantación de ITSM (IT Service Management). Estos procesos componen el Ciclo de Vida del Servicio, y se ponen en marcha en función de cada organización, su actividad, objetivos, etc…

Por tal motivo ITIL está acorde a nuestras metodologías ya que especifica un método sistemático que garantiza la calidad de los servicios de TI. (ItSMF, 2012).

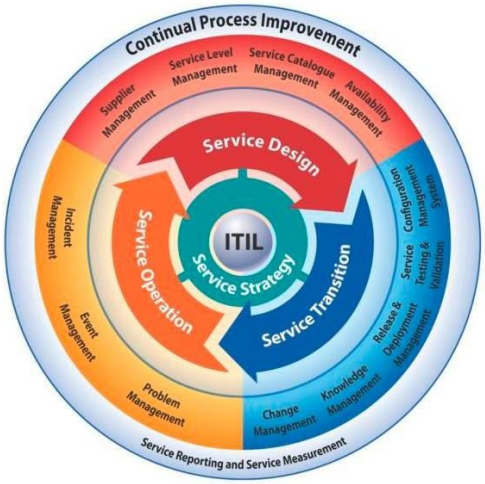

*Ilustración 2.ITIL*FUENTE: tomado textualmente de: (Armendáriz, 2017; Orr & Britain, 2011) Disponible en *: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/581*

5.10 METODOLOGÍA DEL COBIT EN LAS GSSI (GESTIÓN DE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN).

Sus siglas significan Control Objectives for Information and related Technology (Objetivos de Control para la información y tecnología relacionada), el cual es un marco de referencia creado por ISACA (Information Systems Audit and Control Association (Asociación de Control y Auditoria de Sistemas de Información) para la gestión de la TI y el Gobierno de TI. Es un acumulado de herramientas de soporte que permite a la gerencia de las organizaciones el cerrar la brecha entre los requerimientos de control, problemas técnicos y los riesgos del negocio. (Institute, 2007)

La metodología COBIT se enmarca en un modelo holístico permitiendo que las TI ser administradas y gestionadas de todo para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. La metodología posee 5 principios que evalúan las necesidades, condiciones y opciones de las partes interesadas para

determinar que se alcanzan las metas corporativas equilibradas y acordadas optimizando la inversión en tecnología, así como su uso en beneficio de las partes interesadas (Armendáriz, 2017) ver ilustración 3.

Ilustración 3.Principios de cobit 5. FUENTE: tomado textualmente de: (Armendáriz, 2017; Orr & Britain, 2011) Disponible en : http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/581

5.11 NORMATIVA ISO/IEC 27000

La norma ISO 27002 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) especifica los requisitos genéricos que pueden ser aplicables a todas las organización para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información(SGSI) permitiendo la evaluación del riesgo de las organizaciones y especifica los controles de seguridad para mitigarlos o eliminar los riesgos de los activos de la información; teniendo como objetivo principal la conservación de la confidencialidad, integridad y disponibilidad de la información . La norma se encuentra establecida con un enfoque basado en procesos para la gestión de la seguridad de la información, a su vez permite la integración y alineación con sistemas de gestión como la ISO 9001 e ISO 14001 y el SGSI. ISO 27001; está compuesta por 11 secciones (obligatorias y no obligatorias) y el anexo A que contiene 114 controles que se implementan siempre y cuando la organización lo determine para la certificación. Teniendo en cuenta que las secciones de la 0 a 3 son introductorias ósea no son obligatorias para la implementación y las secciones obligatorias son de la 4 a 10 eso quiere decir que las

organizaciones deben implementar los requerimientos de la norma; a continuación, se describen la estructura del estándar (Isotools, 2019).

La normativa de la ISO 27002 puede ser observada en el (Anexo 2)

Cobit5 y el framework NIST

Según (ISACA, 2017) al seguir la guía de implementación tanto en COBIT como en NIST, se logró gobernar y administrar eficazmente los riesgos y recursos de seguridad cibernética. ¿Cuáles fueron los beneficios clave de adoptar estos dos marcos juntos? Estas son las tres razones principales para una organización:

1. Ambos tienen una sólida guía de implementación. Aunque cada marco tiene una metodología de implementación sugerida, se pueden mapear fácilmente entre sí y se utilizarían mejor juntos para la adopción de la seguridad cibernética. El método de implementación de COBIT ofrece un enfoque paso a paso para adoptar buenas prácticas de gobernanza, mientras que la guía de implementación del Marco de Seguridad Cibernética del NIST se enfoca específicamente en las prácticas relacionadas con la seguridad cibernética.

2. Los marcos se refieren entre sí. Cada uno de estos marcos señala dónde el otro los complementa. COBIT se refiere a las publicaciones NIST apropiadas a nivel de proceso, y NIST se refiere a las prácticas COBIT como referencias informativas. Esto permite un mejor mapeo, una duplicación reducida y una visión más amplia de un programa de seguridad cibernética como parte de una iniciativa general de GEIT.

3. Ambos proporcionan un enfoque holístico. Uno de los principios de COBIT se llama "Aplicación de un enfoque holístico" y se centra en un conjunto de habilitadores. Piense en estos habilitadores como los ingredientes para un programa integral de GEIT. El Marco de Ciberseguridad NIST, por otro lado, es lo que se

considera un enfoque holístico para un programa de seguridad cibernética sólido al proporcionar un núcleo de marco que consta de cinco funciones (Identificar, Proteger, Detectar, Responder y Recuperar), e incluye actividades, resultados deseados y referencias aplicables.

5.12 NIST CYBERSECURITY FRAMEWORK

El Marco fue concebido bajo las premisas de identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica, proporcionando un enfoque flexible y repetible, que permite la priorización de actividades y apunta a obtener un buen rendimiento de las infraestructuras, manteniéndose rentable para el negocio. (NIST, 2109).

Las cinco funciones incluidas en el Framework Core son:

1. Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar

Ilustración 4.Funciones del framework NIST. Fuente. (NIST, 2109)

Las Funciones son el nivel más alto de abstracción incluido en el Marco. Actúan como la columna vertebral del Framework Core en el que se organizan todos los demás elementos.

Estas cinco funciones fueron seleccionadas porque representan los cinco pilares principales para un programa de ciberseguridad exitoso y holístico. Ayudan a las organizaciones a expresar fácilmente su gestión del riesgo de ciberseguridad a un alto nivel y posibilitan decisiones de gestión de riesgos.

Tabla. Funciones y Categorías de NIST

FUNCION	CATEGORIA
IDENTIFICAR	Gestión de activos
	Entorno de negocio
	Gobierno
	Evaluación de riesgos
	Estrategia de gestión de riesgos
	Gestión de riesgos de la cadena de suministro
PROTEGER	Gestión de identidad y control de acceso
	Concientización y capacitación
	Seguridad de datos
	Procesos y procedimientos de protección de información
	Mantenimiento
	Tecnología de protección
DETECTAR	Anomalías y eventos
	Monitoreo continuo de seguridad
	Procesos de detección
RESPONDER	Planificación de respuesta
	Comunicaciones
	Análisis
	Mitigación
	Mejoras
	Planificación de recuperación

RECUPERAR	Mejoras
	Comunicaciones

Para el desarrollo del proyecto y como eje fundamental del desarrollo del modelo se hace referencia al NIST, dentro del modelo este framework es el eje vertical para mantener niveles de ciberseguridad apropiados dentro de la institución, a continuación, se explica cada una de sus funciones.

5.13 REVISIÓN DE ESTADO DEL ARTE

En la revisión del estado del arte, quisimos dar un vistazo desde America Latina y se encontró un estudio documental llamado: *Análisis de los Ciberataques Realizados en América Latina* (2018). Realizan en detalle un análisis del nivel de riesgo y preparación en ciberdefensa que tiene la región, como resultado se obtuvo que tiene la mayor cantidad de redes de comunicaciones dependientes de Estados Unidos. La mayoría de los países latinoamericanos tienen o están trabajando en algún tipo de autoridad de protección de datos y privacidad, pero no cuentan con los recursos necesarios para atender prevenciones.

Sin embargo, en Colombia un estudio realizado sobre la Ciberdefensa y la ciberseguridad (2015) en el sector de defensa, cuyo objetivo era una serie de planes y programas de capacitación en seguridad concluye con sugerencias alrededor de la implementación de estrategias de defensa que esté alienada con la seguridad y cumpla con la normatividad. Por otro lado, lograr amoldar el campo jurídico al nuevo sistema tecnológico de cara a una mejor defensa del ciberespacio y ciberseguridad.

Otro trabajo importante es el estudio de Patrones de intentos de “ciberataques asociados a las vulnerabilidades del complemento Revslider (2018)” desde el cual analizan los registros de acceso a internet en varios momentos y se pudo evidenciar ataques contra aplicaciones web basadas en WordPress. La solución para evitar que estos ciberataques sean efectivos consiste en mantener la base tecnológica actualizada, no solamente el núcleo del CMS base con WordPress o Drupal, sino también los restantes componentes de la aplicación web.

Reyna y Olivera (2016), en su estudio sobre amenazas cibernéticas publicado en México,

realizan un resumen de los ataques más comunes que se realizan y citan ejemplos específicos. Estos ataques pueden ser a correos electrónicos, con la intención de obtener información; redes sociales, para robo de información personal o usurpación de identidad; banca en línea, para estafas a través de la manipulación a las víctimas para obtener códigos de acceso; comercio electrónico, para estafas por pagos en línea; y, juegos en línea, en los cuales se piden claves de tarjetas para acceder a dichos juegos.

Raudales (2017) señala que los ataques cibernéticos no sólo suceden en países desarrollados o con tecnologías de primer nivel. Indicó que América Latina ha sido víctima en numerosas ocasiones de delitos cibernéticos. En América Latina y el Caribe, los ciberataques tienen costos muy altos debido a la carencia de una política orientada a la seguridad.

En un estudio sobre modelos para proveer ciberseguridad. Modelos y enfoques de seguridad en las redes sociales (2013). Se establece que está compuesto por varios niveles y cada uno de ellos se organiza en procesos y subprocesos de gestión de la privacidad. Cada subproceso contiene una serie de áreas clave de procesos y cada área se mide en prácticas clave. Además, cada Área clave del proceso, que puede ser evaluada por las diferentes prácticas clave, tiene una correspondencia con una serie de requisitos que deben de cumplirse.

Es fundamental señalar mencionar que la civilización hoy en día está inclinada a ser más dependientes de las tecnologías de la información por razones de eficacia y agilidad, en un mundo tecnológico que avanza a pasos agigantados. Por tal razón con el fin de lograr el cumplimiento de su desarrollo misional, el análisis y entendimiento de los riesgos de TI debe estar inmerso directamente a las directrices de las instituciones de educación superior.

Por lo anterior, Gómez Fernando (2007) declara que la política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios. Las amenazas a la seguridad en una red tienen como particularidad un flujo de información desde una fuente.

Por otro lado, Cisneros (Cisneros, 2018) realizo un modelo de Seguridad para Garantizar la Integridad de Pagos Móviles sobre Near Field Communication (NFC), dentro de su investigación concluyo que el modelo de seguridad NRioSec establece tres niveles de protección con un alto grado de compatibilidad y fácil integración en el desarrollo de

aplicaciones de pago móviles. Sus componentes permiten controlar la autenticación con certificados digitales, la unicidad de transacciones mediante la tokenización y el cifrado de datos mediante algoritmos robustos, y que sumados a las normas de seguridad de aceptación de pagos móviles del PCI SSC, determinan la eficacia de su aplicación para mitigar las vulnerabilidades analizadas.

De acuerdo a lo expuesto por Velásquez, Pérez, & Messino Sossa, (2016) para obtener un modelo adecuado a cada empresa es necesario conocer con detalle cada uno de sus procesos y cuáles son los que tienen prioridad para la continuidad del negocio en cada nivel de gobernanza; según los resultados arrojados por las diferentes auditorias de sistemas realizadas en la región, se toman tres estándares los cuales son alineados para trabajar a la par cubriendo de extremo a extremo la organización con un Sistema de Gestión de Seguridad de la Información que será adaptable a todo nuevo criterio o reto al que se enfrenten, tomando como referentes COBIT 5.0 y la ISO 27001:2013.l

Mantener la confidencialidad, la integridad, la disponibilidad y la usabilidad autorizada de la información cobra especial relevancia y plantea la necesidad de disponer de profesionales idóneos y capaces de asegurar, gestionar y mantener la seguridad de los datos en sus sistemas ante amenazas presentes y futuras.

Arias & Celis (2015) realizaron un modelo experimental de ciberseguridad y ciberdefensa para Colombia cuyo objetivo radico en Construir el modelo de referenciación que garantice al estado colombiano parametrizar las condiciones de protección en el ciberespacio como respuesta a los ataques producidos por guerra de la información. Con el desarrollo del proyecto concluyeron que la Ciberseguridad y Ciberdefensa definen y categorizan tanto las acciones, servicios y mecanismos de seguridad que requiere Colombia para blindar su ciberespacio minimizando el riesgo destructivo de los piratas de la información.

En Perú Zubiate & Linares (2018) realizaron una propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones, dentro de la investigación el autor determino que con la perspectiva de ciberseguridad y/o riesgo, adoptando el Marco del NIST para mejorar la ciberseguridad de las infraestructuras críticas, es un factor importante en la creación de valor para las empresas. La metodología de adopción para ejecutar el marco debe tener un enfoque de gobernanza coherente para adoptar una buena decisión. Este marco es un

modelo flexible que se pueden modificar para satisfacer las necesidades de la empresa y permite que cualquier organización tenga un marco central probado y repetible.

6 DESARROLLO DE LA PROPUESTA

6.1 DIAGNOSTICO EL ESTADO DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CARTAGENA.

Para dar cumplimiento al primer objetivo específico fue necesario realizar un diagnóstico del estado de los procesos de seguridad de la información de la UdeC. Cuando se piensa en diagnosticar se hace referencia al proceso de reconocimiento, análisis y evaluación de una cosa o situación para determinar sus tendencias, solucionar un problema o remediar una dificultad. Así mismo permite de igual manera determinar cuáles son los puntos fuertes y los puntos débiles. Ahora bien, el ciclo de vida de una revisión de seguridad informática resume los riesgos a los que se enfrenta un negocio. Los datos utilizados para este análisis fueron tomados mediante Firewall de Nueva Generación (PAN-PA-5220-ac) de Palo Alto Networks, que inspeccionó todo el tráfico en la capa 7 (incluso de aplicaciones, amenazas y contenido), y lo vincula con el usuario, sin importar la ubicación o el tipo de dispositivo en la trama de la red, el firewall es administrado por un ACC (Application Command Center) siendo esta la herramienta analítica que proporciona inteligencia procesable sobre la actividad dentro de la red. La representación gráfica le permite interactuar con los datos y visualizar las relaciones entre los eventos en la red, incluidos los patrones de uso de la red, los patrones de tráfico y la actividad sospechosa y las anomalías. Esto permitirá un análisis real de la situación que enfrenta la organización.

Utilizaremos el informe en aras de brindar inteligencia accionable en torno a las aplicaciones y las amenazas que recorren la red, evidenciando los procesos de seguridad de la información que necesitan ser intervenidos e incluyendo las recomendaciones que se pueden emplear para reducir la exposición de riesgo global de la organización a nivel informático.

6.2 LA RED DE UN VISTAZO

En esta sección se encuentra una descripción de alto nivel de la red, en el cual se evidencian las principales conclusiones sobre el volumen y tipo de aplicaciones, las amenazas y las vulnerabilidades observadas.

Se evidenció en la trama de red escaneada, un total de 301 aplicaciones vulnerables que están en uso, siendo ellas potenciales desafíos de seguridad en la organización. A medida que las funciones críticas como aplicaciones se muevan fuera de un control sistémico de la universidad, los empleados y estudiantes usaran con mucha más frecuencia estas aplicaciones vulnerables permitidas por la misma organización, abriendo la ventana desde adentro y generando un esquema propicio para ser usados por ciber atacantes.

De las aplicaciones vulnerables encontradas, se clasificaron 63 dentro de alto riesgo, ya que estas pueden introducir u ocultar actividad maliciosa, transfiriendo archivos fuera de la red local, o establecer conexión no autorizada. 69 aplicaciones SaaS (Software as a Service), para mantener el control administrativo y adoptar políticas de gestión por el equipo de TI.

De igual manera se observó un total de 248311 vulnerabilidades incluyendo fuerza bruta, fuga de información y anomalía de protocolos, y un total de 267088 amenazas que se encuentran en la red local, incluidos *exploits* conocidos y *malware* (programa malicioso), conexiones salientes y actividades fuera de control.

6.3 APLICACIÓNES, ANCHO DE BANDA Y TECNOLOGÍA

El primer paso para gestionar la seguridad y el riesgo empresarial es identificar qué aplicaciones pueden ser objeto de abuso para causar el mayor daño. En este análisis es prioridad evaluar detenidamente las aplicaciones en estas categorías para asegurarse de que no estén realizando malas prácticas, políticas, sistemas operativos o riesgo de seguridad cibernética.

A continuación, se muestra el gasto de ancho de banda en las categorías de tecnología, junto con las principales aplicaciones que consumen la mayor cantidad de ancho de banda (ver ilustración 5), de forma gráficas se mostraran las principales categorías de aplicaciones por

sesiones (ver ilustración 6) y nivel de riesgo (ver ilustración 7), sectorizando el análisis para su mejor compresión y así poder abordar directamente las falencias.

Ilustración 5.Demanda de ancho de banda en la UdeC 1 mes de escaneo en la red. El ancho de banda total: 1.17T• | Sesiones totales: 14575665 | Aplicaciones en total: 301

El monitoreo y administración de los anchos de banda o QoS en las aplicaciones es fundamental, para detectar posibles recursos que están siendo utilizados por agentes externos a nuestra red. Sostener un monitoreo y mantenimiento constante a el ancho de banda es optimiza los mecanismos para priorizar las operaciones más importantes en universidad, esta actividad es indispensable.

Durante el periodo escaneando la red de datos de la UdeC podemos ver que la demanda de ancho de banda es muy alto y permisivo en las aplicaciones y protocolos respecto a su uso, se evidencia la falta de mecanismos de control en la demanda de solicitudes por peticiones de dirección IP (PING) y accesos por NUST/NAT, protocolos que deben ser

controlados debido a que son las primeras herramientas que se utilizan para el diagnóstico de conectividad y ataques DoS, DDoS.

Además de ello, no se controlan la demanda de contenido multimedia, consumiendo un alto grado de ancho de banda, un exceso de tráfico en la red sin justificación aparente, suele ser un claro síntoma de un posible ataque, sea interno o externo. Es cierto que el tráfico con Internet es normalmente continuo, pero no se trata de una demanda excesiva, y menos que dicha demanda provoque un comportamiento extraño además de las disminuciones notables de velocidad en los canales.

En las IES (instituciones de educación superior) donde generalmente la misión suele ser académicas, las conexiones P2P (peer to peer) deben estar completamente controladas o en casos normales no permitidas, por su grado de vulnerabilidad.

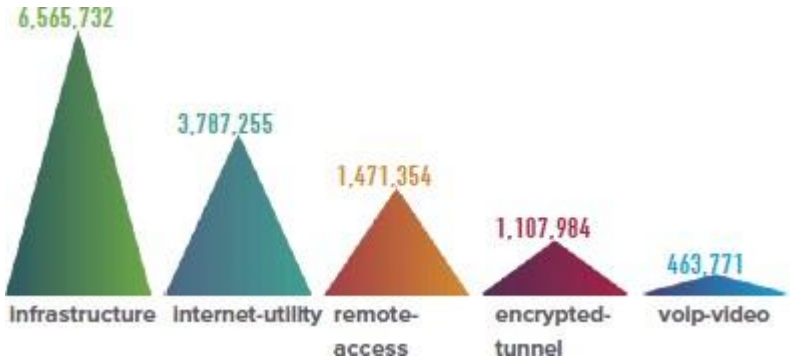

Ilustración 6.Top de aplicaciones por categorías y número de sesiones.

En la ilustración 6 se exponen las categorías de aplicaciones por el número de sesiones, evidenciando la falta de control en aplicaciones de alto contenido multimedia en primer lugar, seguido de peticiones P2P, accesos sin autorización de manera remota. De acuerdo al comportamiento de las aplicaciones, podemos calificar el riego de ellas del 1 al 5, siendo 5 el nivel más alto y 1 el más bajo como lo señala la (ilustración 7). Las variables que tomo para la cualificación de su comportamiento es asociada al número de sesiones realizadas y la cantidad de canal de ancho de banda que se requiere para su uso, también tenemos en cuenta los puertos utilizados y tiempo de sesión.

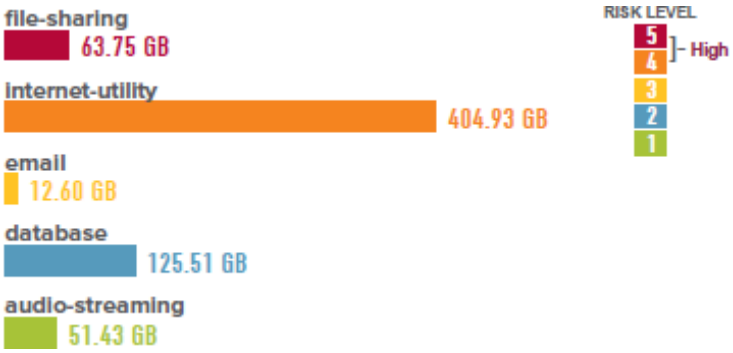

Ilustración 7.Categoría de la aplicación y su nivel de riesgo

Las aplicaciones basadas en SaaS siguen definiendo un contorno importante de la red, proporcionan funcionalidad crítica y la eficiente, pero al mismo tiempo introducen nuevos riesgos potenciales de seguridad y de datos, sino se controla adecuadamente. Normalmente el departamento de las TI, adoptan mucho de estos servicios, y otro son adquiridos directamente por los usuarios individuales llámense administrativos, docentes u estudiantes. Las aplicaciones podrían ser correo electrónico, los calendarios y las herramientas ofimáticas como las más comunes.

Con el fin de minimizar los riesgos de seguridad de los datos que necesita el control sobre las aplicaciones SaaS utilizadas en la red, se señala a continuación el movimiento de datos SaaS en comparación con el movimiento total de volumen de datos en la universidad y colocando en relieve las 5 aplicaciones de mayor consumo en ancho de banda.

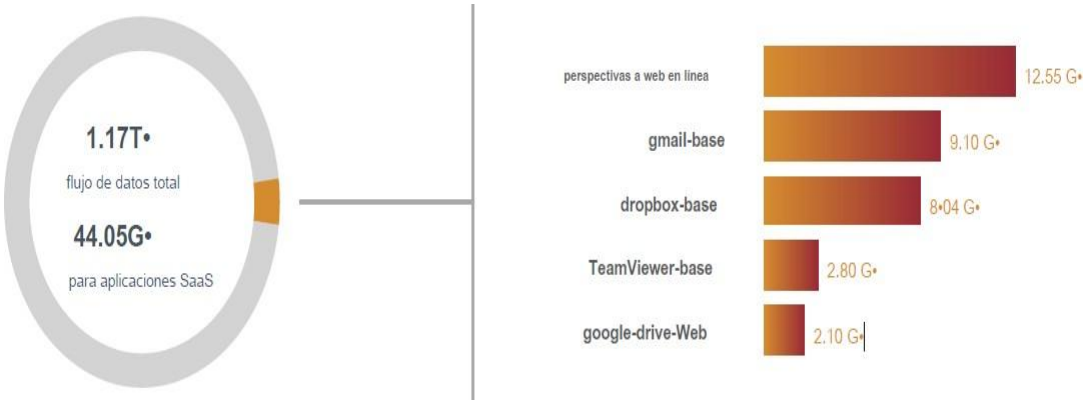

Ilustración 8.comparación con el movimiento total de volumen de datos en la universidad vs volumen de datos den aplicaciones SaaS.

La siguiente (ilustración 9) podemos evidenciar las aplicaciones SaaS más utilizas y así proyectar una buena política para el control de flujo de datos, cantidad de sesiones en uso y consumo de banda requerido para el buen desarrollo de actividades internas sin dejar atrás el constante monitoreo de los puertos y canales específicos.

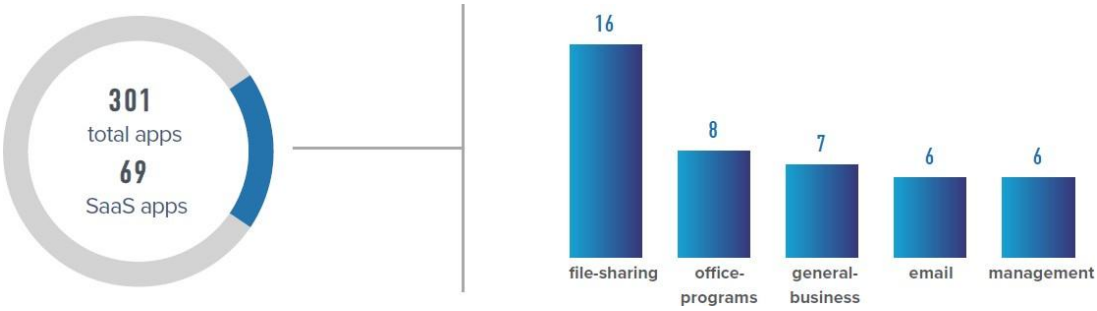

Ilustración 9.Aplicaciones SaaS más utilizadas en la UdeC.

6.4 CONCLUSIONES DEL DIAGNÓSTICO

La comprensión de la exposición al riesgo, y cómo ajustar su postura de seguridad para prevenir ataques, requiere de inteligencia sobre el tipo y volumen de amenazas utilizadas en contra de la organización. En este segmento se expone las amenazas a las que se encuentra expuesta la red de acuerdo con lo observado. Ver ilustración 10

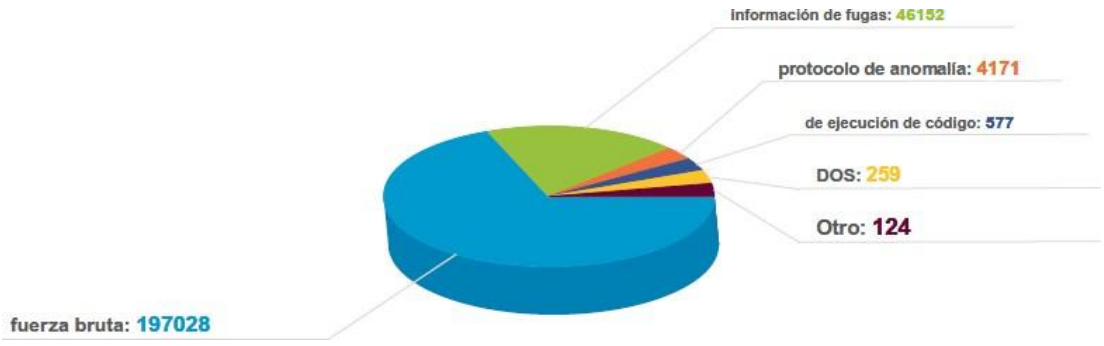

Ilustración 10.Cantidad de EXPLOIT encontrados en la UdeC.

La siguiente grafica muestra el volumen de ataques tipo exploit entregados en cada categoría incluyendo de fuerza bruta con el más alto porcentaje, fuga de información ocupando le segundo lugar y anomalías en protocolos en tercer puesto, luego están otras amenazas como la ejecución de códigos, ataques DoS y otros como ejemplo conexiones remotas.

Clasificamos las 5 categorías más encontradas en el escaneo de red y las aplicaciones que entregan la mayor cantidad de exploits en su red.

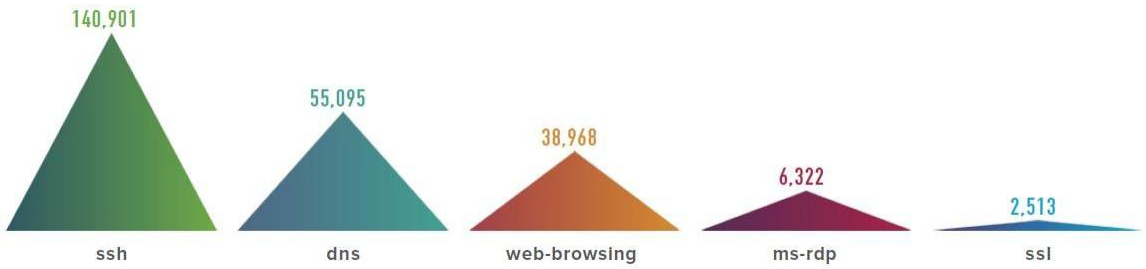

Ilustración 11.Aplicaciones con más EXPLOIT en la UdeC.

Las aplicaciones con más vulnerabilidad en la universidad se encuentran en aquellas que utilizan los protocolos SSH con 140.901 sesiones activas, con una cifra de 55.095 sesiones están las que utilizan DNS como los correos electrónicos, están los buscadores web en tercer lugar y de ultimas están las conexiones RDP (Remote Desktop Protocol) y los protocolos de protocolo para navegadores web y servidores autenticados.

En el análisis anterior de los datos solo se evidencio un malware no reconocido, pero además se reveló con información detallada la falta de políticas y procedimientos inexistentes o más bien existentes, pero no ejecutados, que evidentemente generan un aprovechamiento de agentes internos y externos de las vulnerabilidades del departamento de TI, del tramo de la red y de servicios utilizados por la comunidad en la universidad.

6.4 CATEGORÍAS QUE INTERVIENEN EN LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD DE CARTAGENA.

Para dar cumplimiento al segundo objetivo específico fue necesario realizar la revisión bibliográfica y el análisis documental teniendo en cuenta el enfoque de la seguridad de la información, para lo anterior se tomaron como referentes las categorías señaladas de la ISO 27002:2013 (Ver anexo 2) como guía de buenas prácticas, el marco de referencia integral de

gobierno y la gestión de Tecnologías de la Información COBIT 5 **(ver sección 5)** en sus procesos gestionar servicios de seguridad (DSS05) gestión de los servicios de seguridad y APO13 Gestionar la seguridad, métricas y metas de TI asociadas y las funciones del framework NIST (Ver anexo 1), que se explican en la siguiente sección donde se detalla el modelo propuesto. (Sanchez, 2015).

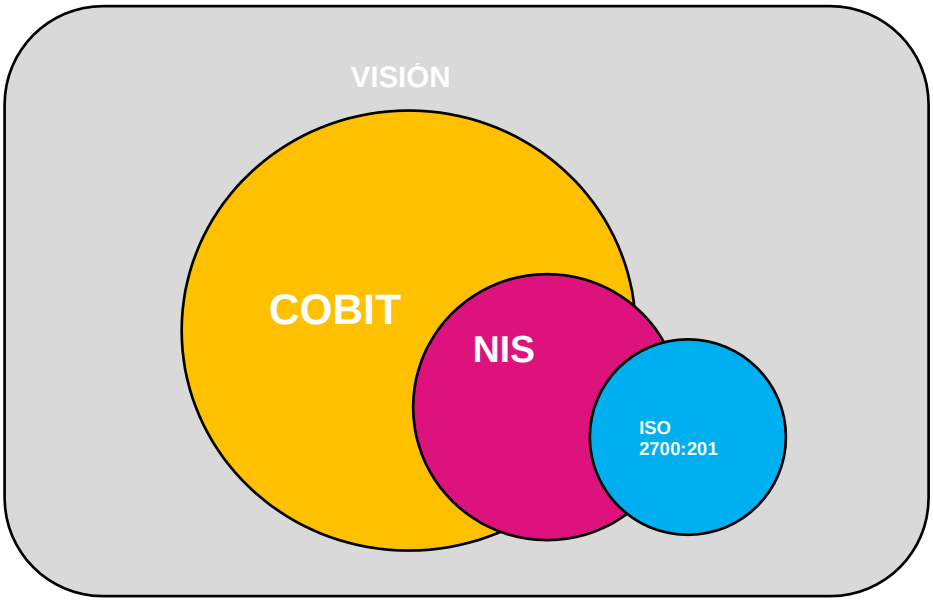

Ilustración 12.Categorías que conforman el modelo. Fuente. Autores del proyecto

La ilustración 12 muestra como el modelo propuesto utiliza estándares mundialmente reconocidos como: ISO 27002:2013, COBIT 5 y el marco de seguridad NIST, que en esta investigación serán renombradas categorías. Siguiendo el modelo propuesto (ver Ilustración 13) se tienen en cuenta los procesos de COBIT 5.0 APO13 gestionar la seguridad y DSS05 Gestionar los servicios de seguridad.

6.5 MODELO PROPUESTO

Desde una perspectiva holística el modelo inicia reconociendo el cuadro de Mando Integral presentado en la ilustración 13 el cual traduce la estrategia y la misión de una organización en un amplio conjunto de medidas de actuación, que proporcionan la estructura necesaria para un sistema de gestión y medición estratégica, teniendo en cuenta desempeño financiero, conocimientos internos del cliente, procesos de negocio y aprendizaje y crecimiento.

Como se puede observar en la siguiente ilustración se evidencian cuatros elementos importantes, el primero de ellos es la perspectiva financiera ¿Cómo ven los entes competentes a la Universidad? En ese sentido es importante mantener niveles de seguridad óptimos que permitan dan cumplimiento a los diferentes estándares para generar confianza.

Ahora bien, se tiene la perspectiva interna de la Universidad ¿En que se deben ser los mejores? Sin duda alguna brindar óptimos niveles de seguridad de la información permite la mejora continua en una búsqueda constante en ser cada día más competitivos, reconociendo el hecho de que la información es un elemento sensible de toda organización a la cual se debe prestar especial atención.

Como tercera perspectiva se tiene la innovación y el aprendizaje ¿Se puede continuar mejorando y creando valor? De por si la información permite la toma de decisiones y desde el desarrollo de este proyecto se propone salvaguardar la información a través del uso de estándares reconocidos permitiendo la mejora la continua.

Ilustración 13.Modelo de ciberseguridad propuesto Fuente. Autores del proyecto

El modelo presenta la perspectiva del cliente y en el caso específico de la UdeC son los

estudiantes, docentes y administrativos ¿Cómo ven los clientes a la Universidad? Mantener una excelente imagen ante el estudiante, el cuerpo administrativo y de docente al asegurar que toda su información está siendo gestionada de forma segura genera un voto de confianza por parte de las personas.

Tabla. Comparativo de estándares de seguridad de la información

	ISO 27000:2017	ISO 27001:2013	ISO ISO 27002:2013	ISO 27005:2011	ITILV3 2011	NIST	COBIT 5
DEFINICION	Proporciona una visión general de los Sistemas de gestión de seguridad de la información, así como los términos y definiciones de uso común	Es un estándar para la seguridad de la información, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la información	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendable en cuanto a seguridad de la información	Proporciona directrices para la gestión de riesgos de seguridad de la información. Brinda soporte a los conceptos generales que se especifican en la norma NTCISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad	Es un marco de trabajo de buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI	Es un conjunto de actividades de ciberseguridad, resultados esperados y referencias aplicables que son comunes a los sectores de infraestructuras críticas, en términos de estándares de la industria, directrices y prácticas que permiten la comunicación de actividades de ciberseguridad	Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute)

Dominios y Procesos	10 Dominios	14 Dominios 10 Procesos	N/A	14 Dominios	26 Procesos 5 Fases	5 funciones fundamentales	5 Fases 37 Procesos 7 Facilitadores 2 Dominios 5 Principio
Funciones	Marco de referencia de seguridad de la Información	Marco de Seguridad de la Información	Marco de referencia buenas prácticas de seguridad de la Información	Marco de Referencia de gestión del riesgo Seguridad de la Información	Mapeo de la Gestión de Niveles de Servicio de IT	Ayudar a los negocios de todo tamaño comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad.	Marco de Referencia de Gestión de Procesos - Mapeo de Procesos TI
Controles	N/A	114	114	N/A	N/A	20	N/A

6.5.1 GESTIONAR LA SEGURIDAD

Según COBIT para gestionar la seguridad se establecen 3 subprocesos basados en establecer y mantener un SGSI que proporcionan un enfoque estándar, formal y continúo a la gestión de seguridad para la información, la tecnología y procesos de negocio que esté alineados con los objetivos del proyecto. Los siguientes dos subprocesos se enfocan en mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información, de cómo mantener la comunicación constante de las necesidades y los beneficios de la mejora continua de la seguridad de información, esto con el fin de recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corrigiendo las no conformidades para prevenir recurrencias. Promoviendo una cultura de seguridad y de mejora continua.

6.5.2 GESTIONAR SERVICIOS DE SEGURIDAD

Según el proceso DSS05 de COBIT, el Gestionar Servicios de Seguridad (GSS) se basa en proteger la información de la organizacion con el propósito de mantener niveles moderados en cuanto a los riesgos en lo que hace referencia a la seguridad de la información de acuerdo con las políticas de seguridad. En este proceso también es necesario establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

Dentro de GSS se describen 8 subprocesos que se encargan de implementar y mantener efectivas medidas (especialmente parches de seguridad actualizados y control de virus), gestionar la seguridad de la red y las conexiones, gestionar la seguridad de los puestos de usuario final, Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio, procedimientos para conceder, limitar y revocar acceso a locales, gestionar documentos sensibles y dispositivos de salida; y se fundamenta en usar herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

Finalmente encontramos al núcleo del modelo propuesto (Ver Ilustración 13) que está basado en el marco de seguridad NIST y en la norma ISO 27002:2013. El núcleo del modelo está basado en 5 aspectos importantes, cada una de ellos se despliegan categorías y sub-categorías (Ver Tabla 2) con objetivos muy bien descritos, estas subcategorías son alimentadas con los 14 dominios que están descritos en la tabla de dominios (Ver Anexo 3), y cada uno ellos alineados a las necesidades de las subcategorías, siendo así 114 controles / referencias normativas de la ISO que se convertirán en los protocolos a plasmar en la implementación. A continuación, se relacionan los objetivos por los cuales se aplicaría cada dominio dentro del modelo se seguridad (Ver Anexo 2).

6.5.3 IDENTIFICACIÓN

La fase de identificación para su aplicación en la UdeC permitirá hacer un diagnóstico o reconocimiento de los procesos en los que se involucran las tecnologías de la información, partiendo de que se debe comprender cuales serían los posibles riesgos asociados a la organización a partir de un control que se tendría por medio de la gestión de los activos, a través de los inventarios de hardware y de software, todas estas funciones deber ser ejecutadas por el personal competente, para este caso el equipo auditor a través de una auditoria pasiva.

6.5.4 PROTECCIÓN

Para la segunda fase que hace referencia a la protección, en ella se tiene el objetivo de desarrollar medidas de control que permitan mitigar cualquier acción que pueda vulnerar los sistemas de seguridad de la UdeC, esto se logra a través de la Gestión de identidad, autenticación y control de acceso, la conciencia y capacitación, la Seguridad de datos, los Procesos y procedimientos de protección de la información, el Mantenimiento y las Tecnologías de protección.

6.5.5 DETECTAR

La tercera fase que hace énfasis en detectar y poder determinar anomalías y eventos, en el cual se trabaja con monitoreo continuo de seguridad y procesos de detección, para esta fase el profesional de seguridad debe estar vigilando los sistemas y las redes, preferiblemente debe ser un especialista certificado en el área de seguridad.

6.5.6 RESPONDER

En la cuarta fase que hace referencia a responder, se debe realizar una planificación en la cual los procesos y procedimientos de respuesta se ejecutan y mantienen para garantizar la respondan a incidentes de seguridad cibernética detectados, de igual manera las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de las agencias de aplicación de la ley. Así mismo el análisis se realiza para garantizar una respuesta efectiva y apoyar las actividades de recuperación, luego se realizan las actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente, y por último las actividades de respuesta en la universidad se mejoran al incorporar las lecciones aprendidas de las actividades de detección / respuesta actuales y anteriores.

6.5.7 RECUPERACIÓN

Por último, se tiene la recuperación, en la cual los procesos y procedimientos de recuperación se mantenienen y se ejecutan para mantener y garantizar la reparación de los sistemas que han sido afectados por cualquier tipo de incidentes de ciberseguridad. De igual manera la planificación y los procesos de recuperación se optimizan al añadir las lecciones aprendidas en actividades posteriores y las actividades de restablecimiento se regulan y se coordinan con partes internas y externas.

Como se evidencio en el desarrollo de la investigación, el modelo propuesto consta de una serie de estándares mundialmente reconocidos como COBIT 5, el framework NIST yla ISO 27002, los cuales partiendo de las necesidades que se observaron en la universidad, se complementan creando un modelo guía que puede ser aplicado en próximas investigaciones para determinan en cierto grado un nivel de confidencialidad, no obstante y desde la experiencia, es válido afirmar que este marco permitiría fortalecer ciertas falencias que

podrían existir en los procesos propios de la organización.

Es de recalcar que el framework NIST permite ayudar a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos, así mismo el marco tomó como estrategia basarse en estándares de la industria ya aceptados por el ecosistema de ciberseguridad como COBIT 5, en ese orden de ideas los elementos utilizados en el modelo resultan ser complementarios toda vez que permita mitigar cualquier amenaza y vulnerabilidad sin que se afecten los procesos de la universidad, proporcionando un enfoque flexible y repetible, que permite la priorización de actividades y apunta a obtener un buen rendimiento de las infraestructuras, manteniéndose rentable para la organización.

7 CONCLUSIONES

Para concluir, con el diagnóstico realizado en la UdeC, se logra obtener una perspectiva o evaluación de cómo estaban funcionando los procesos relacionados con las tecnologías de la información y la seguridad de la información, permitiendo tomar decisiones para el desarrollo de la investigación, al comprender desde el reconocimiento, análisis y evaluación, las tendencias de uso de la red y de esa manera solucionar un problema o remediar una dificultad. De igual manera determinar cuáles son los puntos fuertes y los puntos débiles y comprender con que elementos se contaba y las posibles vulnerabilidades a las que se podría estar expuesto.

Se definen teóricamente las categorías seleccionadas evidenciando la importancia que tienen los estándares escogidos, en ese sentido COBIT 5, NIST y la ISO 27002 en conjunto con los cuales se permiten mantener niveles óptimos de confidencialidad, integridad y disponibilidad de la información debido a su complementariedad.

El modelo permite evidenciar que las categorías escogidas se complementan de tal manera que brindan las herramientas necesarias para mitigar y/o contrarrestar vulnerabilidades y amenazas, debido a que, con ellas, se encuentra un apoyo en el uso de las normativas al comprender que herramienta o estrategia usar para cada caso en específico, teniendo en cuenta cada fase presente dentro de una posible materialización de algún ataque.

8 RECOMENDACIONES

Se recomienda que el equipo de sistemas implemente o tome las consideraciones que en este proyecto se estipulan tomando la sinergia de estándares como una referencia para salvaguardar la información a través del uso de modelos o estándares que brindan las normativas necesarias para cada caso o suceso en específico.

Es posible que para futuras investigaciones el modelo sea nutrido con otros estándares y pueda ser implementado en la UdeC y en otras instituciones de educación superior ya que compartirán los mismos objetivos institucionales, creando así la primera red académica de colaboración de información, relacionada con incidentes de seguridad informática, y en la medida en que el desarrollo tecnológico vaya avanzando, debido a las nuevas y diferentes técnicas de ataque que surgen cada día, en ese orden de ideas debe existir una constante actualización del modelo.

BIBLIOGRAFÍA

Andres, p. S. P. (2018). *"equipo de respuesta ante incidentes de seguridad informática para la universidad regional autónoma de los andes "uniandes"*. Universidad regional autónoma de los andes -uniandes-, ambato-ecuador. Retrieved from http://dspace.uniandes.edu.ec/bitstream/123456789/8158/1/piuasis011-2018.pdf

Diseñar los controles de acceso aplicables a la empresa Spytech S.A.S para su posterior implementación, de acuerdo con el dominio A9 de la norma ISO 27001:2013.

Agudelo, S. F. (1997). Violencia y salud en Colombia. *Pan American Journal of Public Health*, *1*, 93-103

Armendáriz, D. N. L. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica-ESPOL*, *30*(1).

Arquitectura TI Colombia. G.INF.06 Guía Técnica - Gobierno del dato, Versión 1.0, 30 de diciembre de 2014

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*: Editorial Paraninfo.

Betancourt, C. E. A. (22 de agosto de 2017). Ciberseguridad en los sistemas de información de las universidades. In (Vol. 3, pp. 200-217).

Betancourt, C. E. A. (2017). Ciberseguridad en los sistemas de información de las universidades. In (Vol. 3, pp. 200-217).

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *bie3: Boletín ieee*(2), 950-966.

Benavides Gaviria, D. F., & Flor García, G. A. (2019). *Pilares estratégicos en la transición de la banca tradicional a la banca digital en una filial del Banco de Occidente y una filial del Banco BBVA Colombia* (Master's thesis, Universidad EAFIT).

Center, P. M. (2017). Los mayores ciberataques de 2017 hasta la fecha. Retrieved from

https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/

Chicharro Lázaro, A. (2009). La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas. *IDP. Revista de Internet, Derecho y Política*(9).

CONPES 3854, (2016).

de Barrera, J. H., & Morales, M. F. B. (2000). *Metodología de la investigación holítisca*: Instituto Universitario de Tecnología Caripito.

DigiNews's. ¿A qué amenazas cibernéticas se enfrentará el sector educativo con la transformación digital? Retrieved from http://www.digiware.net/?q=es/blog/a-que-amenazas-ciberneticas-se-enfrentara-el-sector-educativo-con-la-transformacion-digital

DigiNews's. (2018). ¿A qué amenazas cibernéticas se enfrentará el sector educativo con la transformación digital? Retrieved from http://www.digiware.net/?q=es/blog/a-que-amenazas-ciberneticas-se-enfrentara-el-sector-educativo-con-la-transformacion-digital

Díaz, F. J., Molinari, L. H., Venosa, P., Macia, N., Lanfranco, E. F., & Sabolansky, A. J. (2018). *Investigación en ciberseguridad: un enfoque integrado para la formación de recursos de alto grado de especialización.* Paper presented at the XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).

FBI. (2016, 2016/05/03 -). Delito cibernético - FBI. Retrieved from https://www.fbi.gov/investigate/cyber

Galán, C. M., & Cordero, C. G. La ciberseguridad pública como garantía del ejercicio de derechos. *Derecho & Sociedad*(47), 293-306.

Galán, C. M., & Cordero, C. G. (2016). La ciberseguridad pública como garantía del ejercicio de derechos. *Derecho & Sociedad*(47), 293-306.

Gamon, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO: Revista Latinoamericana de Estudios de Seguridad*(20), 80-93.

GARCÍA, D. (2017). 7 herramientas para la evaluación de riesgos. Retrieved from https://www.ealde.es/herramientas-evaluacion-de-riesgos/

García, J. A. (2015). *Derecho penal y redes sociales*: Aranzadi-Thomson Reuters.

Gil, M. A. M. (2018). La amenaza de los Rootkits. Retrieved from http://www.bvs.hn/cu-2007/ponencias/SEG/seg021.pdf

Gómez Fernando, S. E. (2007). *Seguridad de la información.* Retrieved from http://cybertesis.uni.edu.pe/handle/uni/9764

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de ingeniería*(31), 109-118.

Institute, I. G. (2007). *COBIT Mapping: Mapping of TOGAF 8. 1 with COBIT 4. 0*: ISACA.

Sistema de Gestión de la Seguridad de la Información, (2013).

ItSMF, U. (2012). *ITIL foundation handbook*: The Stationery Office.

Isootols, (2019). *ISO 27002. La importancia de las buenas prácticas en los Sistemas de Seguridad de la Información*. https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/

ITU. ICT FACTS AND FIGURES 2017. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

ITU. (2010). *Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación*. Paper presented at the Actas finales de la **Conferencia de Plenipotenciarios**, Guadalajara. http://handle.itu.int/11.1002/pub/80366152-en

ITU. (2017). ICT FACTS AND FIGURES 2017. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

kaspersky. (2013). ¿Qué es un botnet? Retrieved from https://www.kaspersky.es/blog/que-es-un-botnet/755/

KasperskyLab. (2018a). Que es la ciber seguridad en internet? Retrieved from https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

KasperskyLab. (2018b). ¿Qué es el spam? Retrieved from https://encyclopedia.kaspersky.com/knowledge/what-is-spam/

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software, 3*(4), 161-176.

Martínez, J. (2012). Seis pasos para el Gobierno de Datos ¿Qué es y cómo se implementa un programa de Gobierno de Datos? *IBM DeveloperWorks*, 1-5.

Morales, S. D. T. (2014). Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". Especial referencia al ámbito universitario. *Revista Icade. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales*(92), 13-47.

Mosso, J. M. R. (2015). Ciberseguridad Inteligente. *arXiv preprint arXiv:1506.03830*.

Orr, A. T., & Britain, G. (2011). *Introduction to the ITIL service lifecycle*: The Stationery Office.

pandasecurity. (2007). ¿Qué es IP Spoofing? Retrieved from https://encyclopedia.kaspersky.com/glossary/spoofing/

Recio, j. (2012). de la seguridad informatica a la seguridad de la informacion. *asociación española para la calidad*, 14-19.

Rodríguez, C. H., Flores, , M. C., López, & , T. G. LA UNIVERSIDAD Y SU RELACIÓN CON LA CIBERSEGURIDAD. *Memorias del Coloquio:"Ciberseguridad. Desde el ámbito legal, empresarial y tecnológico"*, 94.

Schjølberg, C. J. S. (2008). ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG). *Report ofthe Chairman ofHLEG. Genf: ITU. Online verfügbar unter https://www. itu. int/en/action/cybersecurity/Documents/gca-chairman-report. pdf, zuletzt geprüft am, 1*, 2016.

Subijana Zunzunegui, I. J. (2008). El ciberterrorismo: Una perspectiva legal y judicial.

Symantec. (2018). ¿Qué es un troyano? Retrieved from https://co.norton.com/internetsecurity-malware-what-is-a-trojan.html

Urueña Centeno, F. J. (2015). Ciberataques, la mayor amenaza actual. *Documento de Opinión*, *9*(2015), 16.

Van Dalen, D. B., & Meyer, W. J. (2006). Síntesis de" Estrategia de la investigación descriptiva. *Manual de técnica de la investigación educacional*.

Vicente, E., Mateos, A., & Jiménez-Martín, A. (2014). Risk analysis in information systems: A fuzzification of the MAGERIT methodology. *Knowledge-Based Systems, 66*, 1-12. doi:https://doi.org/10.1016/j.knosys.2014.02.018

Villanueva Méndez, J. C. (2015). *La ciberdefensa en Colombia.* Universidad Piloto de Colombia, Retrieved from http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2812/00002646.pdf?sequence=1

Organization for Economic Co-operation and Development (OECD). Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy (2012).

http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Informe Estado de la Unión 2017. Cybersecurity. Resilience, Deterrence and Defence. Building strong cybersecurity in Europe. http://europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity. en.pdf (consultado en agosto de 2018). [En línea] [Citadoel: 25 de agosto de 2018.] http://europa.eu/rapid/attachment/ P-17-3193/en/Cybersecurity.en.pdf.

Reyna, D., & Olivera, D. (2016). Las Amenazas Cibernéticas. REVISTA ELECTRÓNICA DE INVESTIGACIÓN DE LA UNIVERSIDAD DE XALAPA. Ciberseguridad. Desde el ámbito legal, empresarial y tecnológico. 35 - 55.

Raudales, C. (2017). LA BRECHA EXISTENTE EN LA CIBERSEGURIDAD EN HONDURAS. Innovare Ciencia y Tecnología, 58 - 73.

REPUBLICA DE COLOMBIA, departamento Nacional de planeación, consejo nacional de política económica y social-COMPES 3701, Bogotá 14 de Julio del 2011.