MODELO EXPERIMENTAL DE CIBERSEGURIDAD Y CIBERDEFENSA PARA COLOMBIA

Realizadores:

Nicolás Alfredo Arias Torres Cód. 066041023

Jorge Alberto Celis Jutinico Cód. 066082102

UNIVERSIDAD LIBRE

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

BOGOTÁ, D.C. 2015

MODELO EXPERIMENTAL DE CIBERSEGURIDAD Y CIBERDEFENSA PARA COLOMBIA

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OBTENER EL TITULO PROFESIONAL DE INGENIEROS DE SISTEMAS

Nicolás Alfredo Arias Torres
Jorge Alberto Celis Jutinico

Director:
Eduardo Triana M.
Ingeniero de Sistemas

UNIVERSIDAD LIBRE
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
BOGOTÁ, D.C. 2015

AGRADECIMIENTOS

Nicolas Alfredo Arias Torres

Les agradezco a todas las personas que con su ayuda han colaborado en la realización de este proyecto de Grado, en especial al Ingeniero Eduardo Triana M. director de esta investigación, por la orientación, seguimiento y supervisión continua de la misma.

Le doy gracias a mi madre por apoyarme en todo momento e incluso en los momentos más difíciles de mi vida y darme la fuerza necesaria para superar las etapas de debilidad, por enseñarme que el estudio es lo más importante en la vida y estar a mi lado a lo largo de este gran logro.

Jorge Alberto Celis Jutinico

Primero que todo me gustaría darle gracias a Dios por bendecirme y permitir llegar adonde estoy y esperando que me siga bendiciendo para seguir alcanzando mis metas, y por qué hizo realidad este deseo de convertirme en Ingeniero. A la UNIVERSIDAD LIBRE DE COLOMBIA por darme la oportunidad de estudiar y ser un profesional. A mi director de tesis, Ing. EDUARDO TRIANA por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito, y como no a mi amigo y compañero de tesis NICOLAS ARIAS.

También me gustaría agradecer a los docentes que me trasmitieron parte de sus conocimientos durante toda mi carrera profesional y han aportado con un granito de arena a mi formación.

De igual forma y muy importante, agradecer el apoyo de toda mi familia y novia, quienes estuvieron presentes durante todo este proceso y quienes me motivaron para llevar adelante este proyecto de vida y me impulsan a seguir por mas, a mis familiares que me vieron arrancar pero que en este momento no están presentes les agradezco de corazón.

Son muchas las personas que han formado parte de mi vida profesional a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí vida, por todo lo que me han brindado y por todas sus bendiciones.

DEDICATORIA

Nicolas Alfredo Arias Torres

Inicialmente quiero dedicar este trabajo de grado a todas las personas que creyeron en mis capacidades, y de una u otra forma me apoyaron para lograr este objetivo.

A mi hija que es lo más importante en mi vida y por ser un ejemplo para ella

A mi familia por apoyarme en todo momento.

Jorge Alberto Celis Jutinico

Esta tesis se la dedico a Dios quién fue mi guía durante este camino, y me brindo las fuerzas necesarias para seguir adelante y no desmayar en los problemas que se presentaron en el transcurso de este recorrido, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mi familia quienes por ellos soy lo que soy.

Para mi padre Hugo Alberto Celis (QEPD), mi madre Gloria Jutinico y abuela Alicia Jutinico (QEPD) que por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para estudiar. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

A mis hermanos y sobrinos por estar siempre presentes, acompañándome y brindarme sus consejos para que hoy en día esté a punto de cumplir uno de mis tantos proyectos.

A mi novia quien ha sido y es una mi motivación, inspiración y felicidad, que con sus concejos y palabras me cambiaron la forma de ver y afrontar este tipo de retos.

TABLA DE CONTENIDO

Pagina

LISTADO DE FIGURAS

Página

Página

LISTADO DE TABLAS

Pagina

GLOSARIO

ALGORITMO RSA: Es un algoritmo para cifrar como para firmar digitalmente.

ATAQUE: Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

AMENAZA: Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información.

AUTENTIFICACIÓN: La autenticación es el acto o proceso para el establecimiento o confirmación de algo o alguien como real.

AUDITORIA: Es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

BOMBA LÓGICA: Una bomba lógica es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones pre programadas, en ese momento se ejecuta una acción maliciosa.

CABALLO DE TROYA: E**s** un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

CIBERDEFENSA: Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas.

CIBERSEGURIDAD: Conjunto de acciones de carácter preventivo que tiene por objeto el uso de las redes propias y negarlo a terceros.

CONFIABILIDAD: La información disponible en la red presenta una serie de características que la hacen en extremo variable, por lo que su calidad no puede ser definida per segura. Entre los factores que determinan esta variabilidad

CONGELACIÓN: Se produce cuando un programa de computadora, o todo el sistema dejan de responder a las entradas.

CRIPTOGRAFÍA: Se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

CRACKER: Un hacker es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

DENEGACIÓN: Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

EMP: PULSOS ELECTROMAGNÉTICOS Una emisión de energía electromagnética de alta intensidad en un breve período de tiempo.

GUERRA ELECTRÓNICA: Consiste en una actividad tecnológica y electrónica con el fin de determinar, explotar, reducir o impedir el uso hostil de todos los espectros de energía

GUSANO: Es un malware que tiene la propiedad de duplicarse a sí mismo.

HACKER: Es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo, que considera que poner la información al alcance de todos constituye un extraordinario bien.

HERF: RADIOFRECUENCIA DE ALTA ENERGÍA Artefacto cuyas emisiones trastornan la operación normal de equipos digitales, tales como ordenadores y aparatos de navegación.

IAB: La "Internet Architecture Board" es un organismo responsable de definir la arquitectura general de Internet marcando guías y orientaciones al IETF. También actúa como grupo de asesoramiento tecnológico de ISOC.

IETF: "Internet Engineering Task Force" es un grupo abierto de trabajo para el desarrollo de Internet del que forman parte ingenieros informáticos, diseñadores de redes, proveedores e investigadores. Está abierto a cualquier individuo interesado. Sus grupos de trabajo están organizados por áreas, cada una de las cuales tiene un director que forma parte del "Internet Engineering Steering Group"**.**

MALWARE: Código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

MIDDLEWARE: Es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, o paquetes de programas, redes, hardware y/o sistemas

operativos. Éste simplifica el trabajo de los programadores en la compleja tarea de generar las conexiones y sincronizaciones que son necesarias en los sistemas distribuidos.

MODELO: Modelo informático Representación de la realidad por medio de abstracciones. Los modelos enfocan ciertas partes importantes de un sistema.

RELACIÓN: Una relación o vínculo entre dos o más entidades describe alguna interacción entre las mismas.

RFC 2828: Son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.

SET: Un comando para mostrar y asignar valor a las variables de entorno en sistemas operativos.

SEGURIDAD INFORMÁTICA: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

SERVIDOR: Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

SISTEMA DISTRIBUIDO: La computación distribuida o informática en malla es un modelo para resolver problemas de computación masiva utilizando un gran número de ordenadores organizados en clústeres incrustados en una infraestructura de telecomunicaciones distribuida.

VARIABLE: Una variable está formada por un espacio en el sistema de almacenaje (memoria principal de un ordenador) y un nombre simbólico (un identificador) que está asociado a dicho espacio.

VIRUS: Es un malware que tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario.

VULNERABILIDAD: Las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido.

X.800: Es una recomendación que describe las características básicas que deben ser consideradas cuando se quiere conectar una computadora con otras, ya sea conectarse a Internet o a una Red de área local, de forma segura.

X.509: Específica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

ZOMBI: Es la denominación asignada a computadores personales que, tras haber sido infectados por algún tipo de malware, pueden ser usados por una tercera persona para ejecutar actividades hostiles

RESUMEN

El incremento de los ataques destructivos a las redes de comunicación configuradas como soporte operacional de los estamentos del gobierno colombiano, reclaman la necesidad de contar como mecanismo y estrategia contra restadora de un modelo integral para la Ciberseguridad y la Ciberdefensa; el programa de ingeniería de sistemas buscando la consolidación de su imagen y compromiso con la alta calidad, definió como acción inmediata la construcción experimental de este modelo.

El modelo para la Ciberseguridad y Ciberdefensa colombiana (MCCPC), se configuran luego de segmentar espacialmente los marcos de acción logística tanto de los estamentos militares, de policía, como las unidades asesoras de gobierno previa validación de los documentos y referentes existentes que han liberado y difundido estados de trascendental importancia en la lucha contra el terrorismo cibernético.

El modelo presupuestado (MCCPC) deberá ser validado por la dirección académica que orienta a la línea de investigación de seguridad informática para entonces establecer un contacto con el MINTIC y el Ministerio de defensa y proceder a su socialización.

Palabras Claves: Ataque; Amenaza; Ciberseguridad; Ciberdefensa; Malware; middleware

ABSTRACT

The increase in destructive attacks on communication networks configured and operational support of the estates of the Colombian government, demanding the need for a mechanism and strategy against subtracting a comprehensive model for Cybersecurity and Cyber Defence; the systems engineering program seeking to consolidate its image and commitment to high quality, prompt action defined as the construction of this experimental model.

The model for Cybersecurity and Cyber Colombia (MCCPC), then spatially configured logistics segment frames action both military establishments, police, counselors and government units prior validation of existing documents and references which have been released and released states of paramount importance in the fight against cyber terrorism. The budget model (MCCPC) must be validated by the academic leadership that guides the research of security then establish contact with the MINTIC and the Ministry of Defense and proceed to socialization.

Keywords: Attack; Threat; Cybersecurity; Cyber defense; Malware; middleware

INTRODUCCIÓN

Un modelo de Ciberseguridad y Ciberdefensa como resultado del proceso de planeación estratégica para construir un verdadero escudo de protección para el país, se constituye en el instrumento formal con completa operacional, que asegurara al estado Colombiano un blindaje total frente a la posibilidad de ataques respectivos de los hacker y piratas de la información que abordan continuamente el ciberespacio.

El MCCPC, determina la acción logística mediante la segmentación geográfica, la catalogación esquemática de referentes operacionales propios de cada ministerio, como resultado de haber consultado e indagado documentos especializados que sobre este tema a construido la unión europea, Canadá, Australia y estados unidos; la guerra de la información con sus potentes herramientas (EMP y HERF). Se constituye una fuerza de alto poder destructivo, que inquieta a todos los estados del mundo y preocupa a los controladores de la controlacion en la nube.

La estructuración de este trabajo se realiza en tres ejes descriptivos, el primero corresponde al marco operacional de desarrollo, que presenta las características metodológicas, propias de todo trabajo de investigación, para luego proceder a describir el marco teórico, citando referentes textuales y tecnológicos y definiendo los ejes de manipulación analítica que requiere la construcción de un modelo finalizando entonces con la exposición de la solución ingenieril.

1. MARCO DESCRIPTIVO OPERACIONAL

Considerando la normatividad existente en el programa de ingeniería de sistemas de la Universidad Libre, para el desarrollo de trabajos de grado, se describen en este capítulo los referentes formales, sobre los cuales se constituye el marco analítico y estructural que define el escenario de trabajo para la construcción de la solución considerada como objetivo en este trabajo.

Se relacionan, para sus efectos, los aspectos de identificación, la justificación, los ejes de referenciación directa, la metodología ingenieril y el cronograma correspondiente.

1.1 IDENTIFICACIÓN PROYECTO

Modelo experimental de Ciberseguridad y Ciberdefensa para Colombia.

1.2 DESCRIPCIÓN MARCO PROBLEMICO

1.2.1 REFERENCIACIÓN DESCRIPTIVA

Los ataques recibidos por la república de Estonia en el año 2007, que bloquearon las plataformas computacionales de los entes gubernamentales, militares y económicos; la burla realizada en el 2009 al departamento de defensa de la casa blanca, el desvió monitoreado del porta aviones más poderoso de la armada norteamericana: "Ronald Reagan" y los ataques a las centrifugadoras nucleares Iraníes por parte del ejército Israelí; con su potente "FLAME"[1] ha motivado al gobierno Colombiano a proyectar el escenario de defensa y de respuesta, ante la presencia de un ataque en su ciberespacio, mediante la construcción de un modelo, que catalogue acciones determinantes para minimizar el riesgo y para anular la acción destructiva definida por los piratas de la información.

Las salidas del modelo, valorarían en forma efectiva y oportuna las vulnerabilidades detectadas en la infraestructura computacional disponible en las unidades militares,

[1] Solución informática construida por el ejército israelí para atacar instalaciones iraníes. https://es.wikipedia.org/wiki/Flame_(malware)

gubernamentales, financieras, educativas, de salud y de transporte, para establecer acciones reguladoras y modificadoras del contexto, proyectarían el seguimiento y ubicación espacial de los agresores, bloquearían los puntos de los posibles objetivos y validarían la integridad y sincronismo de las actividades de recuperación AUR el paso no controlable de una acción de desastre.

1.2.2 FORMULACIÓN DEL PROBLEMA.

¿Cómo asegurar y blindar el ciberespacio Colombiano, mediante un instrumento de formalización sistémica que defina acciones operaciones y controles de respuesta ante la presencia de un ataque?

1.3 PRESENTACIÓN DE OBJETIVOS

1.3.1 OBJETIVO GENERAL

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.

1.3.2 OBJETIVOS ESPECÍFICOS

- Valorar los proyectos que lideran en la actualidad el comando conjunto cibernético y el centro cibernético policial.
- Estudiar integralmente los esquemas de protección y respuesta que deben ser formulados y esgrimidos o manifestados ante un ataque cibernético, para su rechazo, filtrado y minimización de riesgo.
- Simular las condiciones de extensión de los vectores de ataque como proyectivas de defensa construidas y valoradas por las autoridades en el ciberespacio colombiano.

1.4 JUSTIFICACIÓN

La ingeniería de sistemas, constituye la base operacional proyectiva, que determinara para Colombia la infraestructura, logística y funcional requeridas para enfrentar con acierto la inseguridad existente en el ciberespacio, generada por los hackers, piratas y enemigos de la red.

El programa de ingeniería de sistemas, debe hacerse presente como constructor de soluciones de alto impacto para la sociedad colombiana. Dentro del marco de desarrollo del plan "vive digital". Generando referentes de validación directa dada su coherencia, integridad y valides por unidades de apoyo gubernamental, tales como el COMPES[2], COLCERT[3], COMANDO CONJUNTO CIBERNÉTICO[4], y EL CENTRO CIBERNÉTICO POLICIACO[5].

1.5 BASE REFERENCIAL

La elaboración esquemática, la definición de la plataforma operacional y el diseño estructural del modelo requerido para normalizar la Ciberseguridad y Ciberdefensa COLOMBIANA, será producto de la revisión consulta y evaluación del acuerdo documental con sus correspondientes productos, que se citan como núcleos del estudio a continuación.

1.5.1 NORMATIVIDAD LEGAL

El gobierno Colombiano para enfrentar los delitos informáticos, ha promulgado la base jurídica, señalada en la figura 1.

---

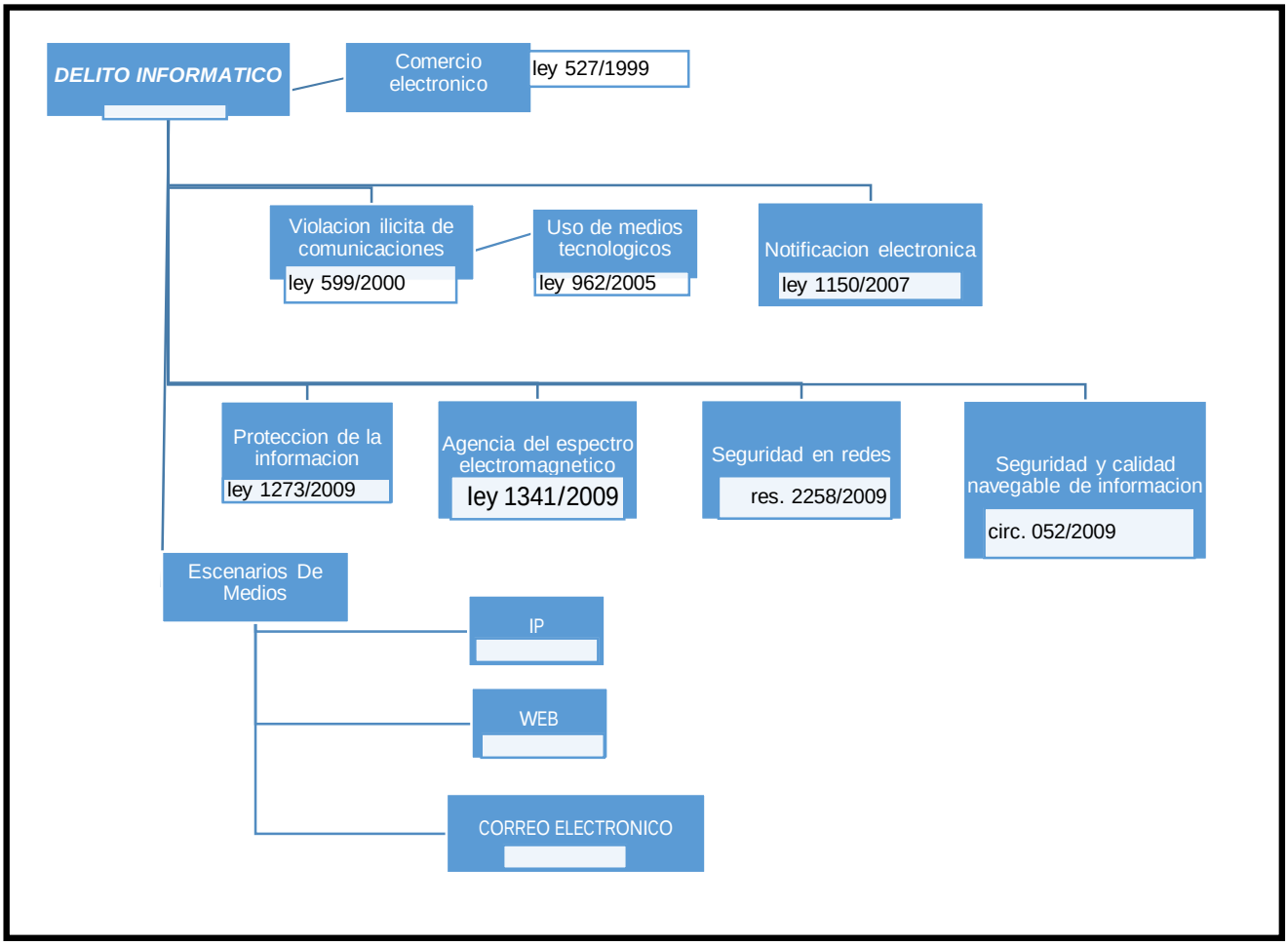
[2] Coordinación Nacional para la Planeación de la Educación Superior.
https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

[3] Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
http://www.colcert.gov.co/

[4] Estudio interdisciplinario de la estructura de los sistemas reguladores.
http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

[5] Aplicación con conexión directa al CAI Virtual de igual forma podrá realizar el reporte de delitos informáticos y hurto.
www.ccp.gov.co/ciberincidentes/tiempo-rea

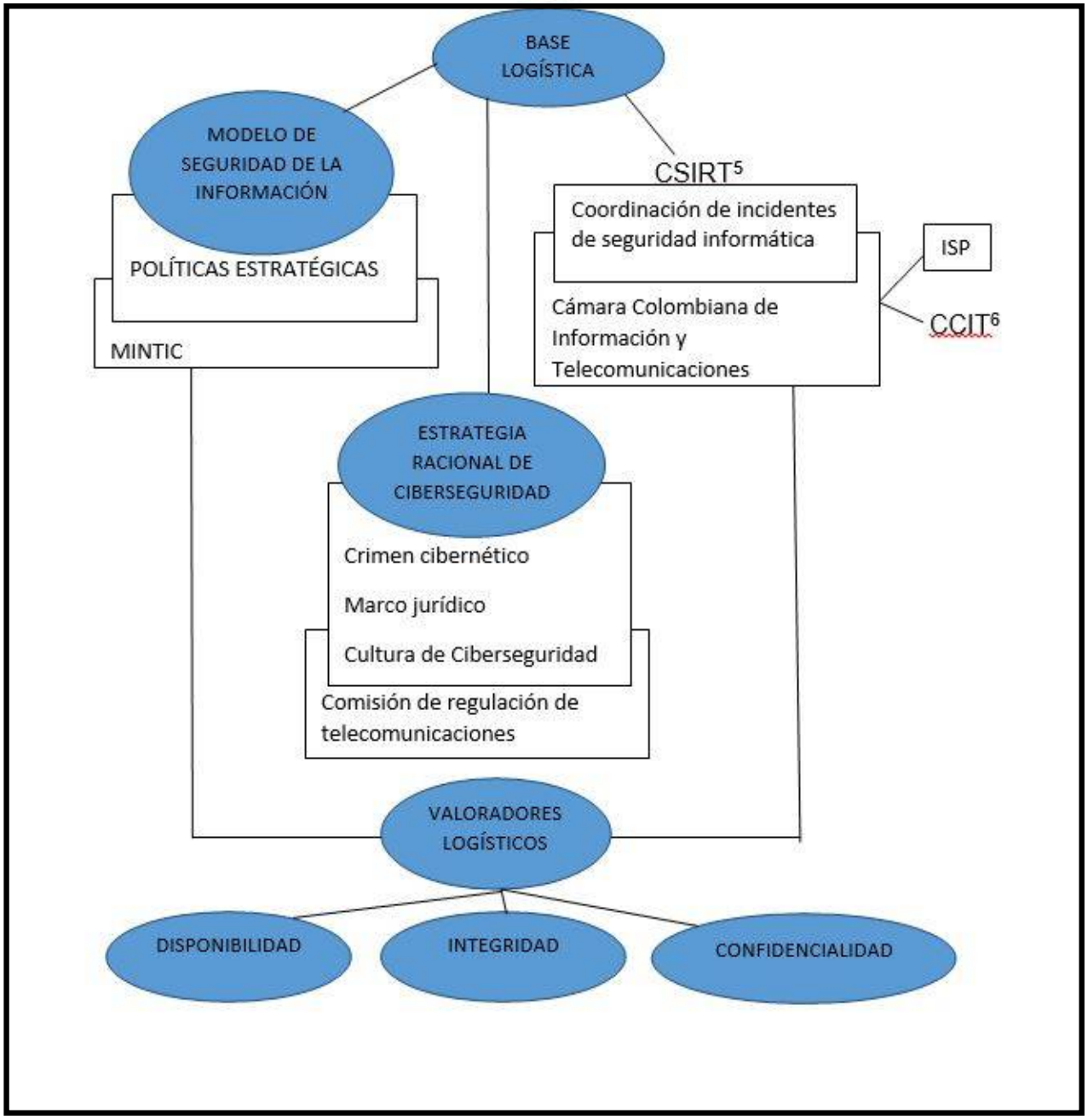
Figura 1: normatividad jurídica: delito informático



Fuente: aporte realizadores.

Con la figura 2, se presenta la base logística que enmarca el conjunto de acción legal considerado como fundamental por el COMPES.

Figura 2: Base logística de privatización conceptual de seguridad en Colombia



Fuente: Aporte realizadores

1.5.2 PARÁMETROS DE CONTEXTO UNIVERSAL

La participación de Colombia en reuniones de referenciación internacional, ha permitido acopiar experiencias, que reflejan acciones de carácter legal y tecnológico, siendo preciso citar por su importancia las siguientes.

- Convenio Sobre Cibercriminalidad De Budapest (CCC)[6]
  - Prevención conductas delictivas
  - Criminalización actos de xenofobia
  - Delincuencia en el ciberespacio
- Resolución OEA AG/RES 2004 (XXXIV-0/04) [7]
  - Creación de CSIRIT[8]
  - Definición arquitectónica de la seguridad en internet
  - Adopción de instrumentos jurídicos para protección
- Comunidad andina: Decisión 587
  - Políticas de seguridad
  - Prevención y erradicación de amenazas de seguridad
- Convenio de Ciberseguridad-UIT[9]

---

[6] Es la asociación más grande de Europa de los piratas informáticos.
https://www.ccc.de/en/

[7] REUNIÓN DE MINISTROS DE JUSTICIA O DE MINISTROS O PROCURADORES GENERALES DE LAS AMÉRICAS.
http://www.oas.org/juridico/spanish/ag04/agres_2040.htm

[8] Centro de coordinación de atención a incidentes de seguridad informática Colombiano.
http://www.csirt-ccit.org.co/

[9] La UIT es el organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación – TIC.
http://www.itu.int/es/pages/default.aspx

- Fortalecimiento sistema mundial de comunicaciones

- Resolución 64/25 de la ONU[10]
- Examen multilateral de amenaza
- Limitadores de amenazas
- Libre circulación de información

1.5.3 SIGNIFICACIÓN PARTICULAR DE LOS ESTADOS

Algunos países han conformado los llamados "CERTS[11]" cuya información se halla disponible en la URL Del "Cardegie Nellon". www.cert.org/csirts/masiouvil/coutach.
Países que con sus estrategias de seguridad, validan su interés por salvaguardar el ciberespacio, en los cuales se registran:

- Alemania
- Australia
- Canadá
- Estados unidos
- Estonia
- Francia

Cada estado se ha preocupado por definir acciones políticas, servicios y mecanismos, que con su utilización, blindan su ciberespacio operacional.

---

[10] Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.
http://www.un.org/es/ga/64/resolutions.shtml
[11] Investigar, desarrollar y difundir nuevos métodos, herramientas y tecnologías para proteger y mejorar la confiabilidad del sistema de energía eléctrica de Estados Unidos y la eficiencia de los mercados eléctricos competitivos.
https://certs.lbl.gov/

1.5.4 FACTORES POSICIONADORES DE CONTROL

Cada estrategia de seguridad cibernética interpreta lo pertinente a:

- Fortalecimiento, capacidad del estado para enfrentar la acción terrorista en el ciberespacio.
- Conformación de organismos de respuesta a emergencias cibernéticas.
- Gestión del conocimiento, en los escenarios, de la Ciberseguridad y Ciberdefensa.
- Desarrollo de estrategias de neutralización y reacción cibernética.
- Valoración, e identificación; de las vulnerabilidades existentes, en el ciberespacio.
- Dimensionamiento a nivel software y hardware, de herramientas generadoras de desastres y protectoras de ataque.

1.6 RESULTADOS PROPUESTOS

El entregable del proyecto, que construirá el programa de ingeniería de sistemas para el cumplimiento de su función de proyección social y dentro de sus políticas de mejoramiento continuo, garantizara a las entidades receptoras de la solución construida, la obtención de los resultados listados a continuación:

- Conformación estructural de los parámetros, lineamientos y políticas que consolidaran el modelo de Ciberseguridad y Ciberdefensa requerido para sus efectos por Colombia.

- Identificación funcional de los agentes de proceso de carácter proactivo con los que se considerara y eliminara la infraestructura de los vectores de ataque que se implementen para modificar y perturbar el ciberespacio Colombiano.

Validación de la confiabilidad y efectividad del modelo al simular cada despliegue operacional un vector de ataque sobre unidades aleatorias de infección.

1.7 FORMALIZACIÓN LOGÍSTICA OPERACIONAL

El modelo experimental de Ciberseguridad y Ciberdefensa de Colombia, surgen como factores diferenciadores. Los núcleos analíticos de relación conceptual, experimental y lógica trabajados dentro del marco teórico, los elementos de conocimiento primordial que determinaron los parámetros de aplicación (marco conceptual) y la base de infraestructura computacional, que cuantifica el marco tecnológico considerado como referente exigido de sustento operacional.

En la figura 3 se presenta esta formalización logística, denotando su espectro relacional y de mapeo funcional como referente de entrada, de proceso y de salida.

1.8 METODOLOGÍA

La construcción del entregable correspondiente a este proyecto, será el resultado de la utilización normativa de las fases que integran un proyecto de tecnología, calificado en el área de la teleinformática y específicamente en el entorno de la seguridad digital, la carta técnica acogida por los desarrolladores, comprende las fases siguientes:

- **FASE DE CONTEXTUALIZACIÓN:**
  Se procede a recolectar, analizar y clasificar la información, que constituye la base para la formulación e interpretación problemita, identificando de esta manera: ¿el que se quiere?, el ¿Cómo se hará?, ¿con que se hará?, ¿para qué se hará? Y ¿quién lo utilizara?

- **FASE DE DIMENSIONAMIENTO FUNCIONAL:**
  Se esquematiza y elabora el prototipo de análisis y valoración, identificando el conjunto de variables, relaciones a integrar y el soporte tecnológico a utilizar, señalando los

aspectos inherentes a la formulación de indicadores y al establecimiento de la ruta crítica para el desarrollo del proyecto.

- **FASE DE DISEÑO Y CONSTRUCCIÓN:**

  Tomando como referente de juicio y desarrollo el prototipo elaborado, se procede a realizar las actividades estructuradas modularmente, validando su efectividad, eficiencia y nivel de calidad, para categorizar la solución que proyectara la entrega del resultado esperado.

- **FASE DE VALIDACIÓN Y LIBERACIÓN:**

  Se definen los procedimientos de prueba a nivel de caja blanca y caja negra y se constata frente a una población experimentada, si los resultados encontrados, satisfacen planamente los requerimientos formulados, si se valida positivamente entonces el modelo puede ser socializado y liberado, en caso contrario deberá reformularse, corrigiendo las falencias detectadas.

1.9 CRONOGRAMA DE DESARROLLO

En la Tabla 1, se presentan las actividades a desarrollar según calendario operacional definido, este cronograma presenta las características siguientes:

- **CALENDARIO DE EJECUCIÓN**
  - Fecha De Inicio: Abril 20 2015
  - Fecha de terminación: Noviembre 15 de 2015

- **UNIDAD DE PROGRAMACIÓN:**

  La semana

- **HERRAMIENTA DE DESARROLLO:**

  Microsoft Project®

❖ **ASIGNACIÓN DE TIEMPOS**

En la tabla 1, se listan los tiempos estimados, los tiempos de holgura y los nombres de las actividades definidas por la estructura de la metodología seleccionada.

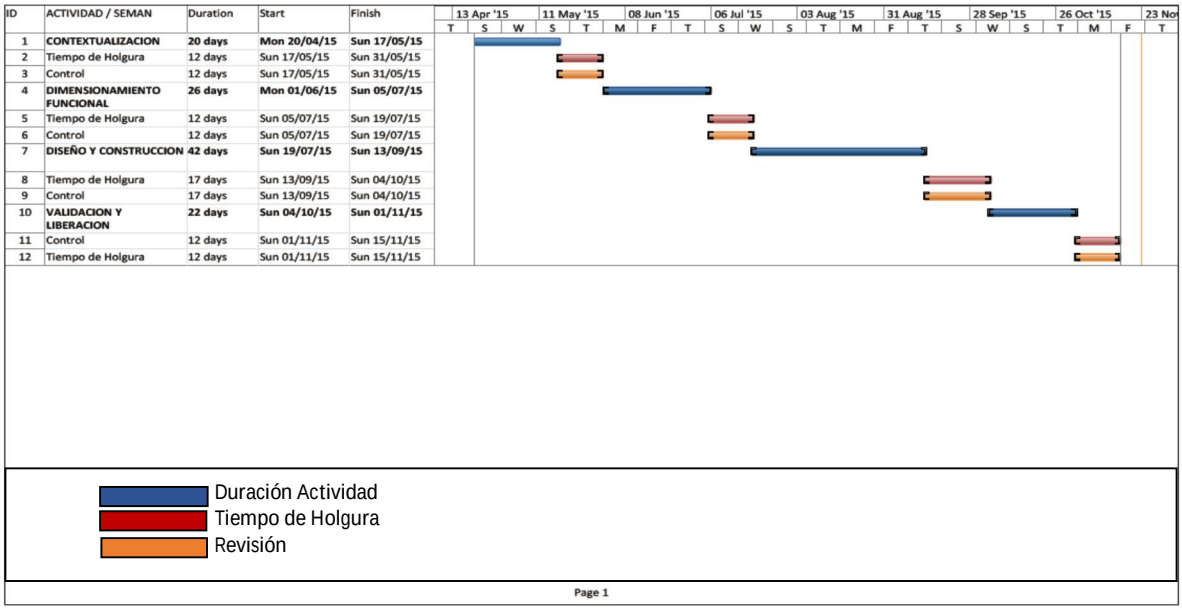
Tabla 1: Asignación de tiempos de desarrollo

ACTIVIDAD	TIEMPO ESTIMADO	TIEMPO DE HOLGURA
CONTEXTUALIZACIÓN	4	2
DIMENSIONAMIENTO FUNCIONAL	5	2
DISEÑO Y CONSTRUCCIÓN	8	3
VALIDACIÓN Y LIBERACIÓN	4	2
Total	**21**	**9**
DURACIÓN PROYECTO		**30**

Fuente: Aportes realizadores.

Su estructura grafica se presenta en la figura 3

Figura 3 Cronograma proyecto



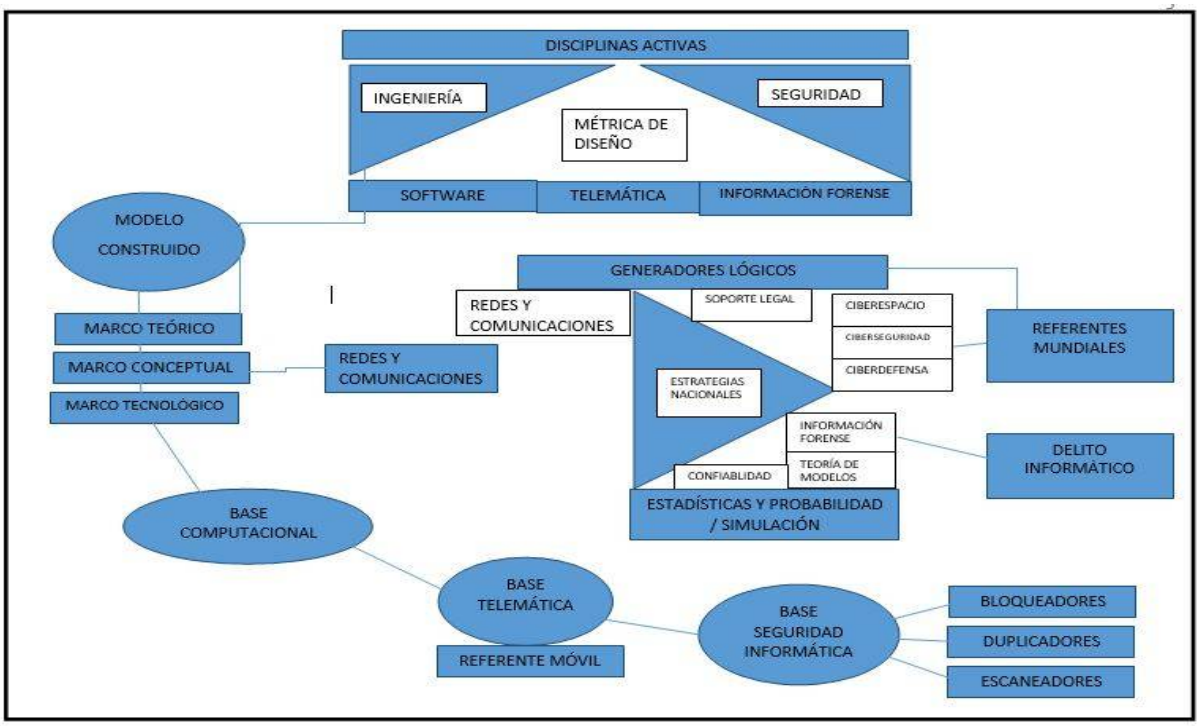
Fuente: Aporte realizadores

1.10 NORMATIVA DE ESPECIFICACIÓN CONCEPTUAL

El diagrama sincrónico señalado en la figura 4 muestra las unidades descriptivas de la esencia, dominio, imagen, y temporalidad de la solución. Formalizando este discriminador como la base operacional que determina la construcción de las respuestas a estos ejes de estructuración sistémica.

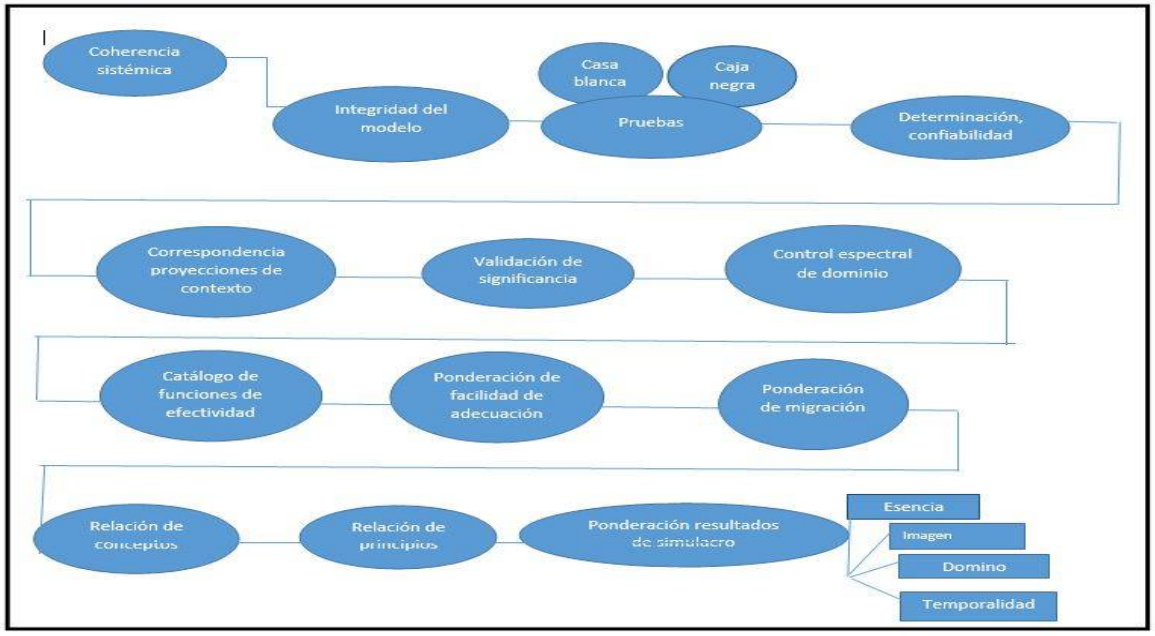
- ¿Que requiere el gobierno Colombiano?
- ¿Cómo se hará?
- ¿Con que se hará?
- ¿Cómo se valida su con finalidad?
- ¿Cómo se definirán su imagen y temporalidad?
- ¿Su nivel de coherencia e ingenuidad sistémica se coteja pos comprensión en el entorno universal?

Figura 4: Formalización logística operacional



Fuente: Aporte realizadores

Figura 5: Normatividad de Especificación conceptual



Fuente: Aporte realizadores

1.11 VALIDADORES DE CALIDAD

Con el fin de permitir a la dirección del programa, presentar el resultado de este trabajo ante el COMPES o que las unidades de control y Ciberseguridad conformadas, el interior de las fuerzas militares y de la policía. Los realizadores sugieren el seguimiento y cumplimiento de la agenda construida.

- Fase 1:
  - Validación funcional
  - Director proyecto
  - Jurado evaluador

- Fase 2:
  - Validación de integridad y pertinencia de la solución

- Director línea de investigación seguridad, información, seguridad importancia procesar los de sistemas universidad libre.

❖ Fase 3

- Validación de calidad, efectividad e
- Pares externos
- Calificación COMPES.

2. ESCENARIO DE REFERENCIACIÓN CONCEPTUAL

El diseño, estructuración y construcción del modelo experimental para la Ciberseguridad y Ciberdefensa en Colombia, requiere del conocimiento y manejo objetivo de un conjunto de conceptos y principios pertinentes a la seguridad digital, la informática forense, la teoría de modelos y la guerra de la información; dicha base teórica se expone para efectos de documentación e interpretación seguidamente.

2.1 TEORÍA DE MODELOS

Convencionalmente el modelo se define como la estructura representativa y escalizada sistémicamente que mapea integralmente un escenario referencial de estudio (Prawda 2008), de otro lado, la modelación como método científico general permite la elaboración del enfoque cibernético, la materialización de la complejidad y la referenciación esquematizada de un problema mediante el tratamiento de funciones significativas que translucen la esfera operacional del proceso que se estudia (Ramírez 2006), El modelo para la Ciberseguridad y la Ciberdefensa en Colombia, evidencia por su naturaleza, las funciones listadas.

- **FUNCIÓN ILUSTRATIVA**

  Representación de la esfera problemita, que categorizo el estudio mediador enunciado lógicas interpretados por estructuras matemáticas descriptivas.

- **FUNCIÓN TRASLATIVA**

  Proyección del escenario probélico a un eje de validación instrumental.

- **FUNCIÓN HEURÍSTICA**

  Genera un escenario elaborado de la complejidad relacional y asociativa del problema que dimensiona la vulnerabilidad del ciberespacio Colombiano.

❖ **FUNCIÓN APROXIMATIVA**

Funcionalidad con significancia y claridad de las estructuras de valoración integral con alto índice de exactitud.

❖ **FUNCIÓN EXTRAPOLARÍA**

Garantiza la elaboración de pronósticos de fundamentación estadística, sobre el comportamiento de las variables.

❖ **FUNCIÓN TRANSFORMADORA**

Identifica el nivel de optimización dinámica, que se requiere para validar su coherencia y confiabilidad.

Complementariamente se hace necesario estipular que el modelo que se proyecta estructurar y diseñar, será el resultado de integrar sistemáticamente estos diferenciadores lógicos a saber.

- ISOMORFISMO[12]
- HOMOMORFISMO[13]
- ISOFUNCIONALISMO[14]

Con base en la complejidad estructural de estos diferenciadores se puede definir como carta técnica de desarrollo, el conocido pentágono de la teoría de modelos que metodológicamente categoriza estas etapas o fases (Ramírez 2006).

- Fase de creación del modelo informativo del fenómeno estudiado.

[12] El concepto matemáticode isomorfismo pretende captar la idea de tener la misma estructura. Dos estructuras matemáticas entre las que existe una relación de isomorfismo se llaman **isomorfas**. https://es.wikipedia.org/wiki/Isomorfismo

[13] En matemáticas, un homomorfismo (o a veces simplemente morfismo) desde un objeto matemático a otro con la misma estructura algebraica, es una función que preserva las operaciones definidas en dichos objetos. https://es.wikipedia.org/wiki/Homomorfismo

[14] El termino isofuncionalismo refiere a aquellas propiedades que permiten que un modelo reaccione del mismo modo que el original frente a las mismas influencias exteriores.

- Fase descriptiva de la estructura relacional de las variables.
- Fase deductiva mediante el análisis lógico matemático.
- Fase de análisis sistémico para categorizar la estabilidad de las variables y enunciados que traducen el comportamiento del fenómeno de estudio.
- Fase de comprobación para validar los parámetros de confiabilidad, efectividad, sincronismo y coherencia.

Operacionalmente el modelo que se difundirá con la entrega de este trabajo, estará cualificado y cuantificado por los 6 principios de la cibernética (Strafford 2008) a saber:

- Principio de auto movimiento activo, reproducción regular y sistémica de los estados condicionados.

- Principio de jerarquía: Establece operadores variables y significación de flujo al interpretar los ejes del ecosistema tecnológico escondido.

- Principio de reflexión, Concordancia y coherencia proyectiva mediante procesos analíticos de comportamiento funcional de las variables.

- Principio de comunicación informativa, operación de la causalidad [15]en la presentación del principio de control y en la estructura de modificación y actualización de la fenomenología de estudio.

- Principio de retroalimentación: Reflexión de elementos ejecutores y controladores operacionales para configurar nuevas salidas de interpretación.

[15] El Estado y en general todos los agentes del sector de las Tecnologías de la Información y las Comunicaciones deberán colaborar, dentro del marco de sus obligaciones, para priorizar el acceso y uso a las Tecnologías de la Información y las Comunicaciones en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

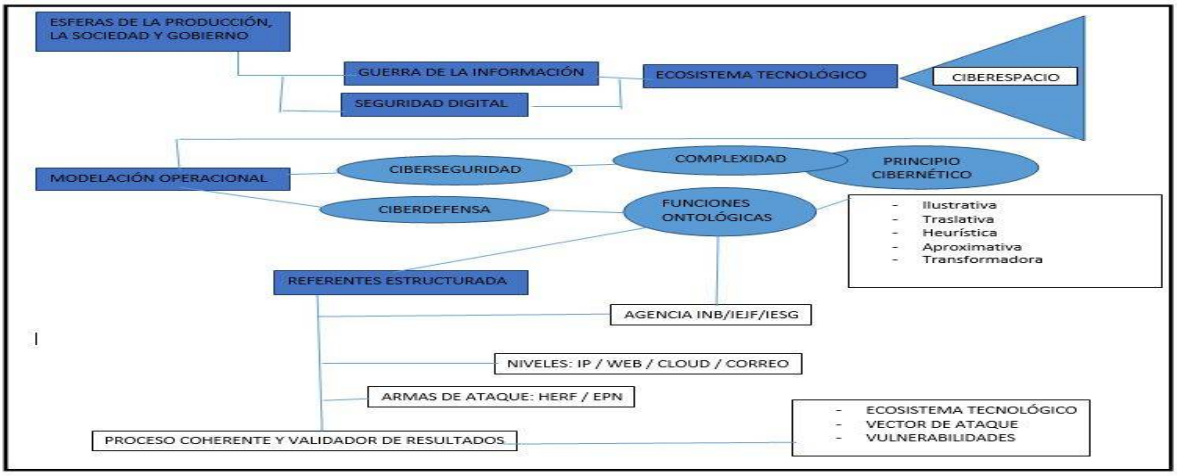
- Principio de adaptación: Mapeo situacional para estudiar el comportamiento operacional del modelo frente a un conjunto complejo de variables exógenas o endógenas, que resultan de asociar gradientes modificadores al entorno que se interpreta (Shannon 1996).

Con la figura 6, se puede interpretar las funciones de comunicación y comunicabilidad, los gradientes operacionales y el sincronismo servicio del modelo a liberar. Dicha figura describe implícitamente.

- Descriptores funcionales
- Ejes de valoración sistémica
- Principios reguladores
- Referentes tecnológicos

  - Ciberespacio
  - Seguridad
  - Control funcional

Figura 6 marco descriptivo del modelo proyecto



Fuente: Construcción propia HERP[16]/EPN[17]

[16] HERP
[17] EPN

2.1.1 SOPORTE MATEMÁTICO PARA EL MODELAMIENTO

La construcción de un modelo, conlleva la interpretación funcional de estos conceptos y estructuras matemáticas, con las cuales se soporta el proceso de simulación; el seguimiento de los resultados y su análisis prospectivo seria producto de la materialización correspondiente.

- **TEOREMA DE BAYES (STALLINGS 2012)**

$$p(A) = \sum_{1}^{n} p\,[p|\varepsilon_i]P[\varepsilon_i]$$

$$p[\varepsilon_i \,|\, A] = \frac{p(A|\varepsilon_i)p(\varepsilon_i)}{p(A)}$$

$$p(\varepsilon_i|A) = \frac{p(A|\varepsilon_i)p(e_i)}{\sum_1^n p(A|\varepsilon_j)p(\varepsilon_j)}$$

- **DISTRIBUCIONES DE PROBABILIDAD (OBREGON 2002)**

  - Binomial

    $g_B(n; np) = \left(\frac{p}{n}\right) p^n (1-p)^{N-n}$; n=0, 1, 2,3….N

    $T_b(Z; N; P) = \sum_0^p (N/n) Z p^n q^{N-n}$

  - Uniforme

$$fx(x; a, b) = \begin{cases} 0 & x < a \\ \frac{x-a}{b-a} & a \le x \le b \\ 1 & x > b \end{cases}$$

- Poisson

$$g(n) = e^{-a} \frac{a^n}{n!}$$

- Exponencial

$$F(t,a) = \begin{cases} 1 - e^{-at} & t \geq 0 \\ o & t < 0 \end{cases}$$

❖ FUNCIÓN DE ERROR [OBREGON 2002]

$$e(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-y^2} dx$$

$$= \frac{1}{2}\left[1 + e\left(\frac{x}{\sqrt{2}}\right)\right]$$

❖ VALOR EXPEDIDO FUNCIÓN DE (X,Y) [OBREGON 2002]

$$\mu|\bar{x} - \bar{y}| = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} |x - y| f_{xy}(x.y) dx dy$$

$$= ab \int_0^p e^{-by} \int_0^y (y - x) e^{-ax} dx\, dy + ab \int_0^{\infty} e^{-by} \int_y^{\infty} (x - y) e^{-ax}\, dx\, dy$$

$$= \frac{a^2 + b^2}{a^2 b + a b^2}$$

❖ VALIDADORES PREDICTIVOS) [Klein2012]

- Lineal

$$y = a_0 + a_1 x$$

$$\sum y = a_0 N + a_1 \sum x$$

$$\sum xy = a_0 \sum x + a_1 \sum x^2$$

- Parabólicos

$y = a_0 + a_1 x + a_2 x^2$

$\sum y = a_0 N + a_1 \sum x + a_2 \sum x^2$

$\sum xy = a_0 \sum x + a_1 \sum x^2 + a_2 \sum x^3$

$\sum x^2 y = a_0 \sum x^2 + a_1 \sum x^3 + a_2 \sum x^4$

- Logarítmica

$p\, v^k = c$

$\log p + k \log v = \log c$

$\log p = \log c - k \log v$

X=log v

Y= log p

$Y = a_0 + a_1 x$

$a_{0=Log\ c}$

$a_1 = -k$

2.1.2 PROCESO DESCRIPTIVO DEL MODELAMIENTO.

Configurar el modelo de Ciberseguridad y Ciberdefensa, será el resultado de las consideraciones o propiedad de estos escenarios.

- Principios de seguridad:
  - Mecanismos
  - Servicios

- Técnicas de criptografía:
  - Cifrado simétrico
  - Criptografía de clave publica

- Ejes de interpretación:

- I.P.
- Correo
- WEB

❖ Configuradores de ataque:
- Intrusos
- Software dañino
- Ecosistemas tecnológicos

❖ Computación forense:
- Técnicas de intrusión
- Infraestructura de seguridad
- Teoría de riesgos
- Análisis forense
- Tratamiento de evidencias digitales
- Trazo digital

❖ Normativas gobierno Colombiano:
- COMPES 3708
- Plan vive digital
- Legislación delito informático
- Marcos operacionales de unidades militares y de policía

❖ Herramientas tecnológicas:
- Recuperadoras
- Detectoras
- Contrarresta miento
- Firewall

Con este acuerdo documental se proceden a delimitar el eje de acción y a constituir sistemáticamente las variables de catalogación, las restricciones operacionales, los

escenarios de vulnerabilidad, las mecánicas y servicios funcionales de respuesta. Y se validara con prueba de carta negra y carta blanca, la integridad, confiabilidad y funciona de monitores del modelo construido.

2.2 GUERRA DE LA INFORMACIÓN

El capitán de navío de la armada peruana, José Luis Gaviria Arranscue, en su artículo publicado por la revista fuerzas armadas de la escuela superior de guerra Colombiana, definió la guerra de la información como "el escenario en donde un terrorista de la información, usando solamente un teclado y un ratón, accede ilegalmente a un computador y causa el choque de aviones, cortes de energía, o sabotea los suministros de alimentos (Gavidia 2012).

La guerra de la información conlleva:

- Guerra electrónica
- Espionaje electrónico
- Terrorismo cibernético

    - Satélites de baja orbita
    - Modificación posicional del referente espacial
    - Proyección de impacto financiero a la economía estatal

Formalmente, cualquiera de estos escenarios conlleva a la manipulación para obtener la superioridad y pleno dominio en el ciberespacio de un estado, para ello los bucaneros de la información explotan las ventajas de:

- Guerra de comando de control

  Bloqueo de comunicación, desvió de referencia espacial, anulación del envío y recepción de órdenes.

- Guerra basada en inteligencia

  Destrucción de la logística definida por acción de los GPS, los telecontroles y el mapeo de seriales desfasados de frecuencia, que definen la congelación de los equipos computacionales o elevan la tasa diferencial de sincronización de ajuste de control.

- Guerra electrónica

  Orientación al dominio total del espectro electromagnético al sabotear:

  - Frecuencias radio AM/FM
  - Tv y sistemas de radar
  - Enlaces por luz ultravioleta
  - Enlace con frecuencia cósmica

Esta guerra genera núcleos disipadores que actúan sobre los equipos computacionales de control, mediante ruidos progresivos y sincrónicos que se manifiestan y categorizan como (stallings 2012).

- Atenuación[18]: decaimiento de la señal por reducción de energía

  $$NF = -10\,log10\frac{PF}{PS}\frac{Potencia\ de\ salida}{Potencia\ de\ entrada}$$

- Distorsión de retardo

  Llegada de frecuencias en intervalos diferentes

- Ruido

  Modificación de la señal por distorsiones modificadoras, se clasifican como:

[18] "En telecomunicación, se denomina atenuación de una señal, sea esta acústica, eléctrica u óptica, a la pérdida de potencia sufrida por la misma al transitar por cualquier medio de transmisión." https://es.wikipedia.org/wiki/Atenuaci%C3%B3n

- Ruido térmico[19]
- Ruido de intermodulación[20]
- Diafonía[21]
- Ruido impulsivo[22]

Por ejemplo, la cantidad de ruido térmico en cualquier conductor está dado por.

N = KTW

N= Densidad de potencia de ruido

K= Constante de Boltzman $=1.3803 * 10^{-23}\, {}^{j}/_{k}$

T= Temperatura en grados kelvin.

La guerra electrónica, está orientada al uso de equipos especializados que actúan sobre infraestructuras computacionales parta modificar estos parámetros de toda señal periódica, a saber.

N=V N=V

$X(t) = \sum ancos\,(2mnfot) + \sum bnseo\,(2mnfot)$

$$au = \frac{\frac{i}{t}}{tx(E)de}$$

$$an = \frac{2t}{t}x(T)\cos(2\pi fot)de$$

$$bn = \frac{\frac{2}{t}}{tx(t)sen(2\pi fut)de}$$

$$x(e) = cot°cn\cos(2\pi fut + \emptyset n)$$

$$x(e) = s0\, x(t)e52\pi ft$$

[19] "Se genera por la agitación térmica de los portadores de carga (generalmente electrones dentro de un conductor) en equilibrio, lo que sucede con independencia del voltaje aplicado." https://es.wikipedia.org/wiki/Ruido_de_Johnson-Nyquist

[20] "Este tipo de ruido se produce en sistemas de transmisión no lineales produciéndose la inserción de nuevas frecuencias las cuales se adicionan o se restan con las frecuencias de la señal mensaje degenerándola." https://es.wikipedia.org/wiki/Perturbaciones_en_una_transmisi%C3%B3n#Ruido_de_Intermodulaci.C3.B3n

[21] Se dice que entre dos circuitos existe diafonía, cuando en parte una de las señales presentes en uno(1) de ellos, considerado perturbador, aparece en el otro, considerado perturbado. https://es.wikipedia.org/wiki/Diafon%C3%ADa

[22] Ruido cuya intensidad aumenta bruscamente durante un impulso. https://es.wikipedia.org/wiki/Ruido_impulsivo

En la figura 7, se representa la acción operacional de la guerra electrónica, sobre un objetivo, acción basada en la modificación del dominio periodo/frecuencia, que impide que los espectros no se solapen, echando por tierra la fundamentación de la señal muestreada e impidiendo su recuperación.

$$X_{(s)} = x(t) - p(t)$$

X(s)= señal de pulsos
X(t)= señal emitida
p(t)= señal de pulsos.

Cuantificándose potencialmente sobre enlaces satelitales para alterar cualquier parámetro de la ecuación de enlace (tonase) 2012, a saber:

- Potencia de salida del transmisor
- Perdida de respaldo
- Perdida de alimentadores en la estación terrena
- Potencia de salida del transmisor
- Ganancia de la antena
- Perdida de trayectoria
- Modificación de la temperatura

Que al modificarse actúa de manera directa sobre las ecuaciones de subida y bajada del satélite, a saber:

- Ecuación de subida

$$\frac{c}{no} = lo\ logAtPr - 20les\left(\frac{4\pi d}{x}\right) + 10\log\left(\frac{6}{te}\right) - 10\ loglp - locosk$$

10 Lo Log AtPr = EIRP estación terrea/

$20\log\left(\frac{4\pi d}{x}\right) = perdida\ de\ trayectoria$

$10 \log \left(\frac{6}{te}\right) = \frac{satelite6}{te}$

10 log (ln)= perdida atmosférica adicional

10 log k = constante de boltzman

- Ecuación de bajada

$$\frac{c}{no} = eirp(dew) - lp(db) + \frac{6}{te(dbk)} - 1\lg(de) - k(dbwk)$$

Con parámetros similares a la primera ecuación

- Guerra psicológica

Empleo de los computadores para generar mensajes por trasmisión de imagen

La guerra de la información explora con amplitud los problemas de la vulnerabilidad, para ello emplea

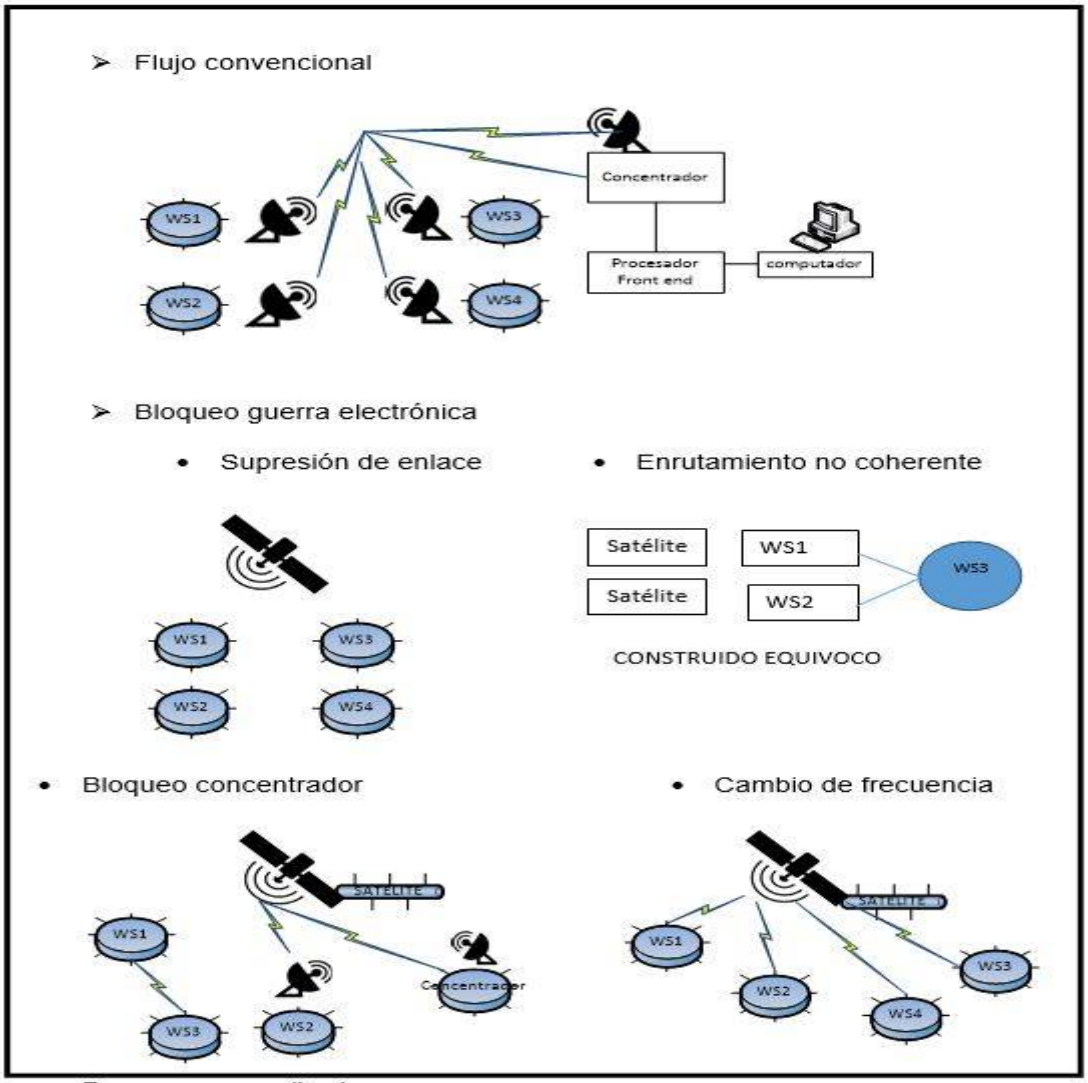
- Software malicioso
- Chipping
- Puertas traseras
- Armas electromagnéticas
- Herf (high energy radio frequency)[23]
- Emp (electromagnético pulse)[24]
- Microbios destructivos de hardware
- Nano máquinas
- Radiación VAN ECK[25]

[23] Arma de energía dirigida utilizada para interrumpir equipos digitales. https://en.wikipedia.org/wiki/Talk%3AHigh-energy_radio-frequency_weapons

[24] Método de ataque militar realizado con armas generadoras de importantes cantidades de energía electromagnética ambiental que destruyen total o parcialmente el equipamiento eléctrico y electrónico dentro de su radio de acción. https://es.wikipedia.org/wiki/Pulso_electromagn%C3%A9tico

[25] Proceso que se utiliza para espiar la información del contenido informático de un monitor https://es.wikipedia.org/wiki/Interferencia_de_Van_Eck

Figura 7. Esquema destructivo plataforma satelital



Fuente aporte realizadores

2.3 SEGURIDAD DIGITAL E INFORMÁTICA FORENSE

Siendo la seguridad digital, el escenario donde se estructura y valida la confiabilidad e integridad transaccional sobre una arquitectura computacional qué opera sobre un sistema tele informático, se hace preciso operar e interpretar el escenario de contextualización lógica, los factores definidores de implementación, el delito informático y la información forense , cuya fundamentación se expone a continuación.

2.3.1 CONTEXTUALIZACIÓN LÓGICA

La definición de la contextualización lógica se hace por el conocimiento de los factores relacionados con (stallings 2013)

- Arquitecturas de seguridad
- Amenaza/ataque
- Mecanismo y servicio de seguridad
- Normatividad reguladora

Que para los efectos se tratan separadamente

2.3.1.1 ARQUITECTURA DE SEGURIDAD

Enfoque sistémico, descriptivo y proyectivo qué estructura lógicamente los atributos referenciales y condiciones operacionales normativa en el despliegue que supervisa y regula la seguridad computacional entorno teleinformático, esta arquitectura se despliega y considera el recado recomendación x 800 [26] de la ITU[27]

2.3.1.2 AMENAZA Y ATAQUE LA NORMA X.800 ESPECÍFICA

- Amenaza: Posibilidad de violación de la seguridad que materializa un posible peligro.

- Ataque: Asalto deliberado a la infraestructura computacional que genera una acción destructiva tipificada por el delito informático.

[26] Recomendaciones básicas que se requieren para comunicar una computadora con otras. https://es.wikipedia.org/wiki/X.800

[27] Organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación – TIC http://www.itu.int/es/pages/default.aspx

2.3.1.3 MECANISMO Y SERVICIO DE SEGURIDAD

Según la recomendación que Define la arquitectura de seguridad OSI (X.800), estos términos poseen la siguiente significación.

- Mecanismo. Entidad que detecta y previene el ataque definiendo su proceso de restablecimiento Integra los núcleos operacionales citados

  - Cifrado
  - Firma digital
  - Control de acceso
  - Integridad de datos
  - Intercambio de autentificación
  - Relleno de tráfico
  - Control de enrutamiento
  - Notarización

- Servicio de seguridad.
  Entidades contrarrestaditas de los ataques a la seguridad mediante

  - Autentificación
  - Control de acceso
  - Confidencialidad
  - Integridad
  - No repudio

2.3.1.4 NORMATIVIDAD REGULADORA

Especificaciones que determinan controlan y regulan la definición de un sistema de seguridad (Stallings 2013) este conjunto de normativas se expresan en los documentos siguientes.

- X 9.17: gestión de claves
- RFC 1321: mensaje MD5
- RFC 2040: algoritmo RC 5- CTS
- RFC 2046: MIME[28]
- RFC 2406: carga útil de seguridad IP
- RFC 2104: HMAC[29]
- RFC 2571: gestión SNMP
- RFC 2573: aplicaciones SNMP
- RFC 2630: sintaxis criptográfica
- RFC 3156: seguridad MIME
- X.509: marco de clave pública
- X.800: arquitectura de seguridad OSI
- FIPS: operación DES
- FIPS 180-1: estándar HASH
- FIPS 197: cifrado avanzado.

❖ La figura 8 explícita la contextualización lógica de la seguridad.

2.3.2 DEFINIDORES DE IMPLEMENTACIÓN

El definidor de implementación es el eje de grabador de validación del servicio de seguridad que se aplica a sus referentes funcionales son:

❖ Cifrado simétrico. DES[30]/AES[31]/CBC[32]/CFB[33].

[28] PROTOCOLO MIME (extensiones multipropósito de correo de internet), serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos.
https://es.wikipedia.org/wiki/Internet_Message_Access_Protocol
[29] Construcción específica para calcular un código de autentificación de mensaje (MAC).
https://es.wikipedia.org/wiki/HMAC
[30] Descifrado de la clave secreta.
http://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des
[31] Esquema de cifrado por bloques
https://es.wikipedia.org/wiki/Advanced_Encryption_Standard

- Criptografía de clave pública. RSA[34]/DIFFIE[35]/HELLMAN[36].
- Firma digital y gestión de claves.
- Autorización KERBEROS[37]/X.509 [38]
- Seguridad en correo PGP/S-MIME.
- Comprensión de datos ZIP/RADIX 64[39].
- Seguridad IP IPSEC/ESP/ISAKMP.
- Seguridad web SSL/TLS/SET/ALERT.
- Gestión de redes SNMP[40]/PROXY.

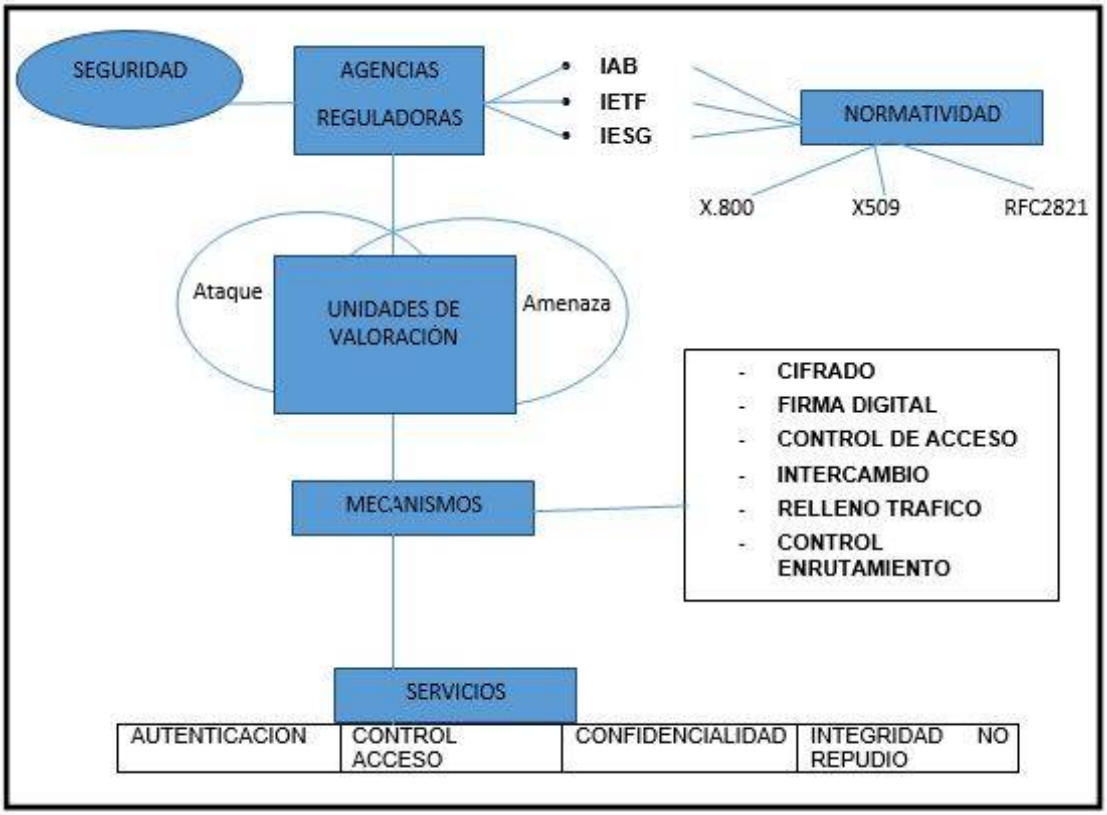
Gracias a estos definidores es posible interpretar al interior de la seguridad en la web con alertas relacionados con:

- Mensajes inesperados
- Mac de registro
- Fallo de descomposición

---

[32] A cada bloque de texto plano se le aplica la operación XOR con el bloque cifrado anterior antes de ser cifrado.
https://es.wikipedia.org/wiki/Cifrado_por_bloques
[33] Hacen que el cifrado en bloque opere como una unidad de flujo de cifrado.
https://es.wikipedia.org/wiki/Cifrado_por_bloques
[34] Primer algoritmo valido, tanto para cifrar como para firmar digitalmente.
https://es.wikipedia.org/wiki/RSA
[35] Protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autentificada).
https://es.wikipedia.org/wiki/Diffie-Hellman
[36] https://es.wikipedia.org/wiki/Diffie-Hellman
[37] Protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.
https://es.wikipedia.org/wiki/Kerberos
[38] Un certificado en el entorno electrónico de seguridad, conjunto estructurado y estandarizado de datos
https://msdn.microsoft.com/es-es/library/aa354512(v=vs.110).aspx
[39] Formato de compresión sin pérdida, muy utilizado para la compresión de datos como documentos, imágenes o programas.
https://es.wikipedia.org/wiki/Formato_de_compresi%C3%B3n_ZIP
[40] Protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
https://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

Figura 8 Contextualización lógica de la seguridad



Fuente: aporte realizadores

- Fallo de negociación
- Certificado revocado
- Certificado caducado

Como también el poder interpretar el encapsulamiento de la carga útil de seguridad, el conocer la estructura del formato es porque comprende:

- Índice de parámetros de seguridad
- Número de secuencia
- Datos de carga útil
- Relleno
- Cabecera siguiente

- Datos de autentificación “un definidor de implementación como el ipsec proporciona estos valoradores de control
- Conexión segura
- Acceso seguro
- Establecimiento conexión extranet
- Seguridad en el comercio electrónico

Para ello se poseen estas recomendaciones:

- RFC 2401 requerimiento de seguridad.
- RFC 2402 extensión de autenticación IPV4/ IPV5
- RFC 2408 gestión de clave6

La funcionalidad ipsec se evalúa gracias a la concurrencia de estos agentes.

- Protocolo ESP
- Protocolo AH
- Algoritmo de cifrado
- DOI[41]
- Gestión de claves

2.3.3 DELITO INFORMÁTICO E INFORMÁTICA FORENSE.

En Colombia existe una salida base jurídica para condenar las acciones relacionadas con el delito informático por ejemplo la ley 1273 [42]de enero 5 de 2009 crea como bien jurídico turnado la protección de la información y de los datos declarando en su articulado Cómo tipificación directa del delito:

[41] Identificador de objeto digital.
https://es.wikipedia.org/wiki/Identificador_de_objeto_digital
[42] La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.
http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de un sistema informático.
- Interceptación de datos informáticos.
- Daño informático.
- Violación de datos personales.
- Suplantación de sistemas cneb.
- Hurto por medios informáticos.
- Transferencia no consentida de activos.

El delito informático, según el convenio de ciberdelincuencia del Consejo de Europa se define como el acto dirigido contra la confidencialidad integridad y disponibilidad de un sistema informático redes de interconexión y abuso de la información razón por la cual la legislación colombiana se ocupa con objetividad de su contra restauración y minimización de impacto producido enfrentando los efectos que se manifiestan en Casos como éstos.

- Filtrado el portal del infiel.
- Cíber delitos contra Menores en el país
- Caen 117 hackers que robaron 160 millones
- Roban millones de dólares por pagos en intranet en Brasil
- Un delincuente viajó por el mundo con anillos de famosos.
- Se crea usurpadores.com
- Uso del sexting para extorsionar a menores.
- Tengo citas eróticas por internet.
- Historias clínicas nuevas objetivas de piratas.
- Se desocuparon 40 cuentas por clonación de tarjetas.

Los ataques convencionales se producen por troyanos y Adware [43]entre los cuales se citan.

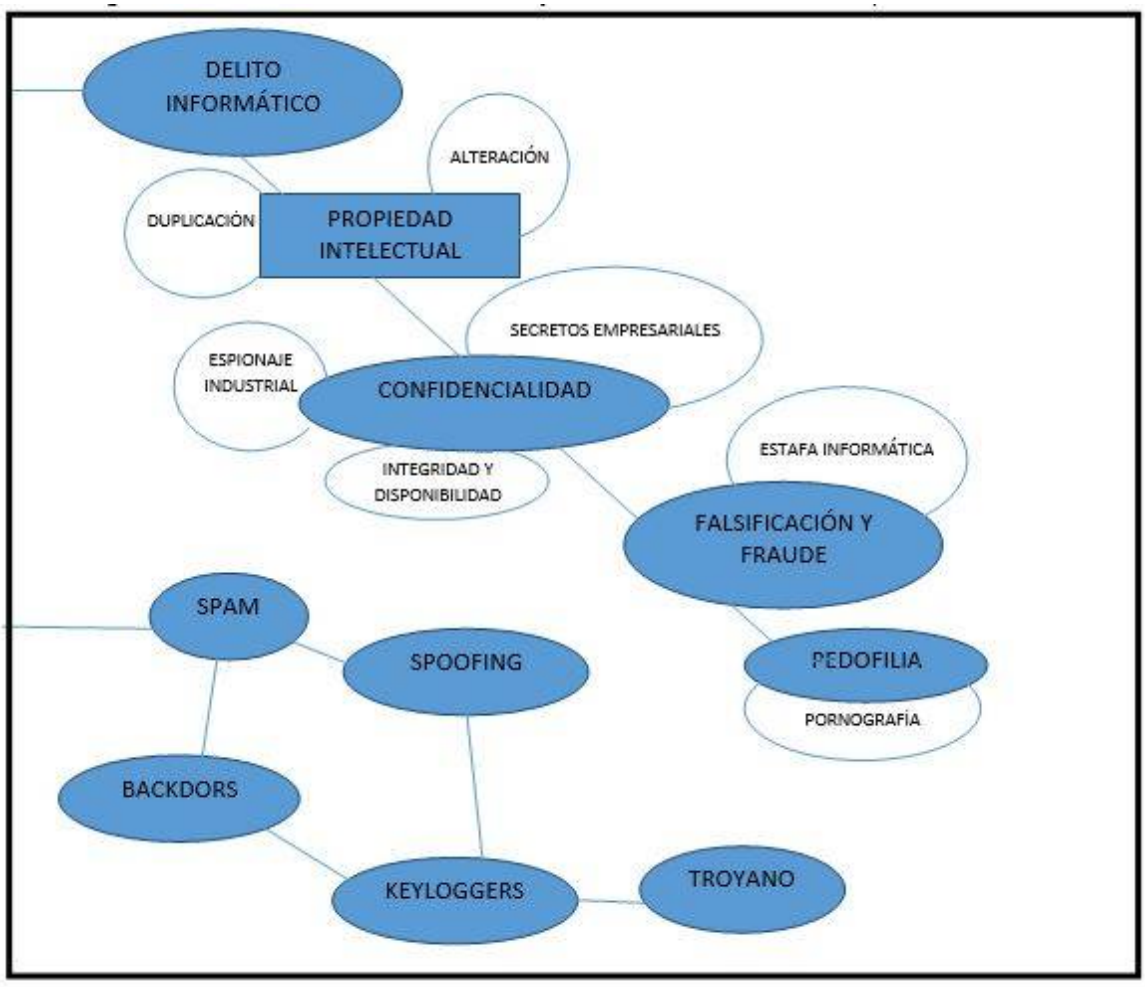
- Win32/trojan clicker punto small. K.J.

[43] Software con soporte publicitario.
https://es.wikipedia.org/wiki/Adware

- Win32/adware.Borán.
- Trojan downloader.zlob.
- Win32 /nuwar.m.
- Netsky.Q.

La policía nacional reporta que desde el año 2013 se ha incrementado el costo del cibercrimen pasado de 870 mil millones a novecientos ochenta y cinco mil millones Esto Gracias al empleo de Smartphone que facilitan el logro del delito para efectos de documentación se presenta en la figura 8 los delitos más frecuentes en nuestro país.

Figura 9: Delitos informáticos de mayor ocurrencia en Colombia



Fuente: Ministerio del interior. Adaptación realizadores

Por ejemplo con este simple Script, se pueden borrar archivos ocasionando daños al contenido almacenado por un programa embebido escrito en lenguaje C++.

```
Set wshshell=wscript.createobject("wscript.shell)
dim mensa,libre
mensa=”experiment nuevas emociones” ,20, “no lo dude”
Wshshell.run ("desierto-jpg").
Set libre=createobject (" sapi.spvoice").
libre.speak mensa
Wscript-sleep 500.
Nsgbox "disfruta mi belleza",1024,”intentando”
wshshell.run "borre.exe"
```

El programa dev C++, registra este contenido

```
#include <conio.h>
# include <stdio.h>
# include <stdlid.h>
# include <Windows.h>
main()
{system (“cls”)
system(“del c :/users/estado/deskstop*.*”
}
return (o);
```

La informática forense, como grande tecnología de seguimiento a la acción del delito informático, integra el ecosistema tecnológico con la traza de la evidencia, empleando un gran soporte de herramientas (Cano 2015).

- ENCASE
- FORENSE TOOL KIT

- WINEX FORENSIES
- PRADISCOVER TOOLS
- COMPUTER FORENSIS SOFTWARE TOOL
- CRYPT CAT
- THE SLUTH KIT
- THE CORONER TOOL KIT

La informática forense dispone de las normas fundamentales que se listan a continuación:

- Preservación de evidencia
- Establecer cadena de custodia
- Documentar hechos

Para ello, se debe seguir el proceso que identifica, recoge, analiza, confirmación y validación operacional a la vida digital. (Pages 2012).

El modelo proyectando, que se expone en el próximo capítulo, posee como característica fundamental el identificar bienes referenciales o nivel operacional en la informática forense y en los lineamientos de política para Ciberseguridad, y Ciberdefensa (Compes 3201), producto del seguimiento de hechos de gran valía a nivel mundial, tales como:

- Ataque cibernético del gobierno de Estonia en el 2007.
- Ataque a la casa blanca y al DHS (departamento de seguridad interna) en el 2009.
- Detección en España de la red compuesta por 13 millones de direcciones, conocidas con el nombre de (“BOOTNET MARIPOSA”) en el 2010.

Es necesario aclarar que se tendría en cuenta, toda la base jurídica existente a saber:

- Ley 529 de 1999
- Ley 529 de 2000
- Ley 962 de 2005

- Ley 1150 de 2002
- Ley 1273 de 2009
- Ley 1341 de 2009
- Resolución 2258 comisión de comunicaciones
- Circular 052 superintendencia financiera

Y se valorara como instrumento de juicio analítico los producidos a nivel internacional, que se identifican como:

- Convenio de cibercriminalidad de Budapest[44]
- Resolución AG/RES 2004 (OEA)[45]
- Declaración 578 COMUNIDAD ANDINA[46]
- Convenio de Ciberseguridad VIT
- Resolución ONU 64/25

Consultándose los proyectos existentes a nivel nacional tales como:

- Estrategia de seguridad cibernética en Alemania.
- Estrategia internacional para el ciberespacio de estados unidos.
- Estrategia de Ciberseguridad en Estonia.
- Estrategia canadiense de seguridad cibernética.
- Estrategia de defensa y seguridad.
- De los sistemas informáticos en Francia.

[44] Es el único Acuerdo internacional Que Cubre Todas las áreas Relevantes de la Legislación Sobre ciberdelincuencia (Derecho penal, derecho procesal y Cooperación Internacional) y Trata con Carácter prioritario Una Política Penal contra la ciberdelincuencia. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c , http://www.informaticalegal.com.ar/2010/08/01/%C2%BFque-es-el-convenio-sobre-cibercriminalidad-de-budapest/

[45] http://www.oas.org/juridico/spanish/ag04/agres_2040.htm

[46] Régimen para evitar la Doble Tributación y Prevenir la Evasión Fiscal http://www.dian.gov.co/descargas/convocatorias/128_2009/DocumentosGuiaNo.2/Decision_CAN_578_04052005.pdf

3. DISEÑO Y CONSTRUCCIÓN DE LA SOLUCIÓN INGENIERIL

El desarrollo y masificación de las tecnologías de la información y las comunicaciones, la construcción de procesos de amplia escala; la catalogación y control del espacio mediante la puesta en órbita de un cinturón completo de satélites geoestacionarios, y la multiplicidad de ataques a las redes gubernamentales, empresariales, académicas y militares.
Junto con el incremento potencial de nuevas áreas de apoyo en la guerra cibernética, construyen los eslabones de análisis sobre las cuales se sustenta la evaluación funcional y la presentación operacional del proceso de análisis, diseño y construcción de un modelo estructural para el control de la seguridad y la formación estratégica de la defensa, en el ciberespacio colombiano.

La construcción de la solución prevista, involucra el tratamiento descriptivo de los ejes operacionales siguientes: fundamentación del proceso creativo, logística de la modelación, proceso de diseño, catalogación de complejidad del ciberespacio.

Proceso de formalización; diseño y construcción del modelo y variaciones de su conformidad; aspectos que se trabajan seguidamente.

3.1 INGENIERÍA Y PROCESO CREATIVO

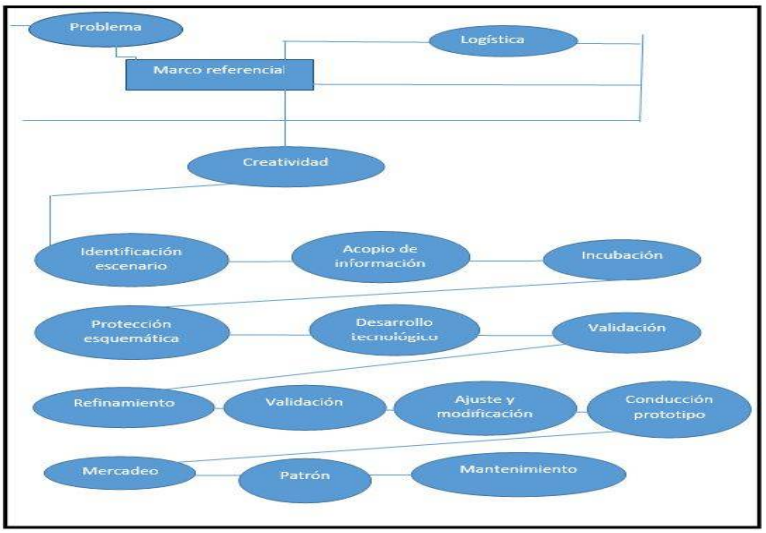
Se ha hecho conocido el escuchar que los científicos, exploran lo que existe más los ingenieros crean lo que no existe, los objetos diseñados y construidos por el ingeniero, dado su compromiso con el progreso y mejoramiento de la calidad de vida de la sociedad, se ha caracterizado por garantizar total conformidad, plena efectividad y alto índice de seguridad.
Pues su trabajo está basado en la innovación, y creatividad (Grech 2013).
El proceso creativo, por su carácter sistemático, registra una secuencialidad integrativa, cuya estructura se traduce en la figura 10.

Dicho proceso es el resultado del aprovechamiento de los siguientes factores.

- Capacidad de análisis.
- Espíritu de observación.
- Capacidad de síntesis.
- Capacidad de lógica.
- Capacidad numérica.
- Pensamiento divergente.
- Pensamiento convergente.
- Habilidad numérica.
- Serendipia[47].

Debe recordarse que la creatividad, ingenieril es un resultado de emplear los niveles más altos de la taxonomía del conocimiento (Grech 2013) y de la identificación de los grados de funcionalidad operacional y adaptabilidad instrumental, verificándose así por su presencia como fuerza dialéctica, que traduce el cambio, y el dinamismo en la producción ingenieril.

FIGURA 10: Secuencialidad lógica del proceso creativo



Fuente: modificación realizaciones. Original Pablo Grech

[47] Hallazgo afortunado e inesperado que se produce cuando se está buscando otra cosa distinta. https://es.wikipedia.org/wiki/Serendipia

La fase dos (2), señalada en la figura anterior, que identifica el proceso de acopio de información, presupone el navego por parte de las realizaciones de este conjunto de temáticas propio de la ciencia, de estructura y de las ciencias de la computación, a saber.

- Base Cibernética.

  - Teoría de la modelación.
  - Gestión y logística operacional.
  - Modelo de sistema viable (MSV).[48]
  - Sistema automático de control.
  - Valoración decisional.
  - Métodos de bifurcación y acotación.

- Base ciencias de la computación

  - Middleware.
  - Sincronización, construcción y replicación.
  - Tolerancia y fallas.
  - Niveles de seguridad: web/ip/correo.
  - Modelos de coordinación.
  - Delito informático.
  - Informática forense.
  - Función de decibilidad[49].

El proceso creativo, se validara al interior del modelo con el análisis de confiabilidad, nivel de usabilidad, estructura proyectiva y nivel de interacción lógica requerido para simular su estabilidad[50] y pertinencia.

---

[48] La estructura, las actividades, las interrelaciones y flujos de información en las organizaciones. https://ingenieriadesistmas.wordpress.com/r-sistemas-viable/

[49] La decibilidad es de gran utilidad en los procesos y teorías de autómatas ya que por medio de su análisis se puede llegar a establecer cuáles son las delimitaciones de los autómatas, y en qué caso se pueden aplicar. https://es.wikipedia.org/wiki/Lógica_de_primer_orden

[50] Se denomina estabilidad cuando los fallos disminuyen por debajo de un rango determinado.

3.1.1 FORMACIÓN LOGÍSTICA ESTRUCTURAL

El proceso de creatividad requerido para el diseño y construcción del modelo renace sobre el tratamiento de escenarios de factibilidad no convexa. (Prauda 2008), cuya estructura operacional se define por la consideración de la siguiente lista de factores.

- Ubicación lógica de servidores
- Flujo de transporte transnacional
- Logística de seguridad gubernacional
- Logística de seguridad fuerzas nacionales y de policía
- Logística de seguridad sector financiero
- Logística de seguridad sector productivo
- Logística de seguridad sector académico
- Logística de seguridad sector vías y servicios

Su consideración involucra, el tratamiento relacionado con los problemas de conocimiento y conectividad entre servidores y clientes activos (ver figura 11).

Problema de inversión para escoger la mejor alternativa de negociación, problema de valoración de índice de vulnerabilidad.

El tratamiento matemático responde a uno de estos enunciados (Prawda 2008)

$$min\ z = \sum_{j=1}^{n} e_j x_j$$

$$\sum_{j=1}^{n} aijx_{s\geq 1} \qquad l=1\ldots m$$

$$X_{j=0\ 01\ J=1\ldots n}$$

$$Xj = \begin{cases} 1 si\ j\ es\ un\ nodo\ del\ area \\ 0\ si\ j\ no\ es\ nodo\ del\ area \end{cases}$$

---

https://es.wikipedia.org/wiki/Estabilidad

$$aij\begin{cases} 1\ si\ i \in Pj & j = j \dots n \\ 0 si\ i \notin Pj & i = i \dots m \end{cases}$$

- $maxz = \sum_{i=1}^{n} v_i x_i$

  $$\sum_{i=1}^{n} k_i x_i \leq K$$

  $x_i \geq 0 \quad i$ =1,2,3,….n

v_i = costo de conectividad o estudio de ataque

k_i = Capacidad operacional de transmisión

k= Cobertura total de servidores y estructuras computacionales

Cuya solución, demando la utilización de unos de estos algoritmos

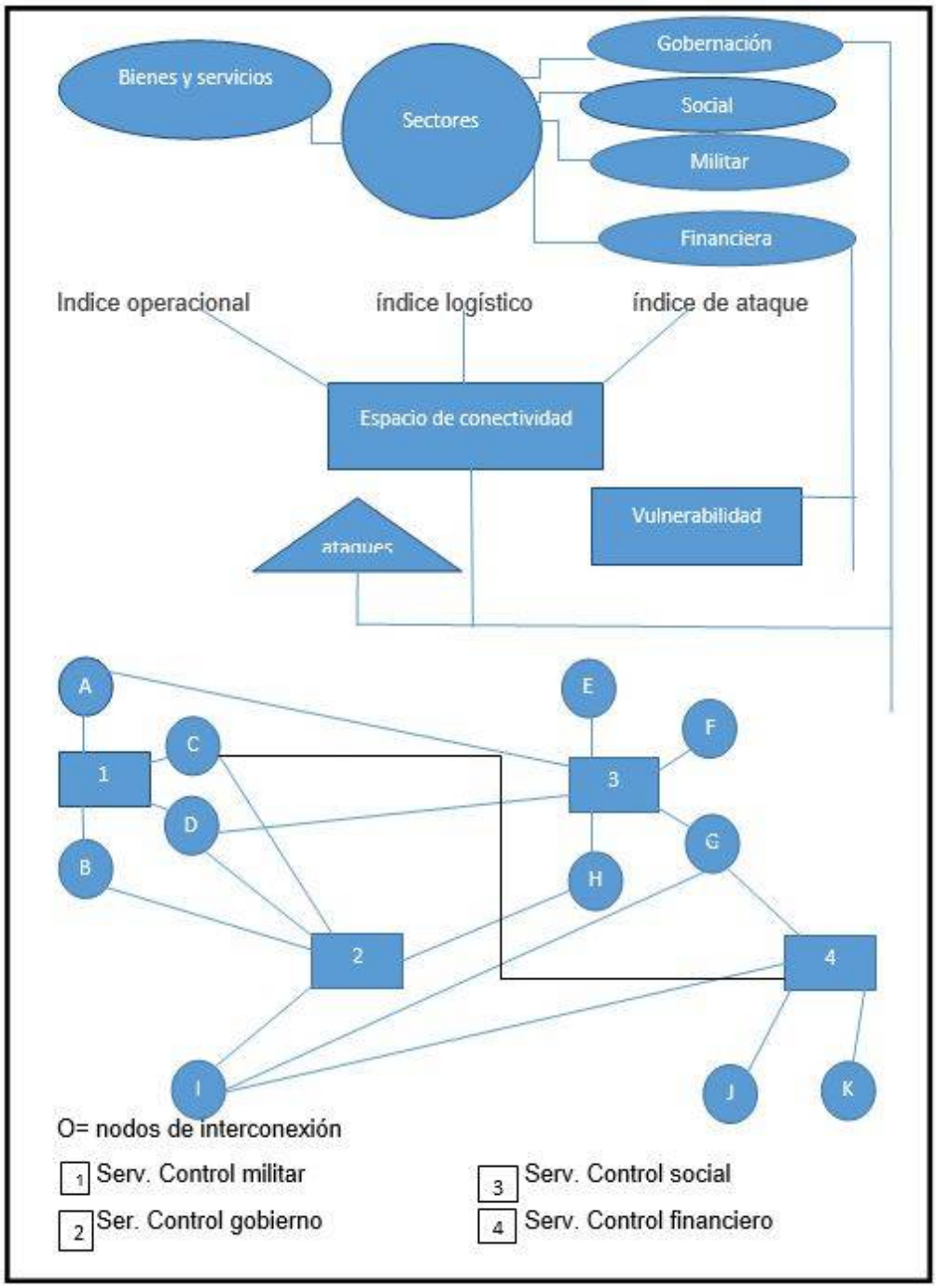
- Fraccional de Gomory[51]
- Lang Doig[52]
- Aditivo de balas[53]

[51] Algoritmo utilizado para la solución de problemas en programación lineal. http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060014/html/Capitulo%20VI/gomory.htm

[52] Sub problemas que surgen a partir del problema general. https://sites.google.com/site/optimizacionenteraydinamica/introduccion/metodos-de-solucion-en-programacion-entera/metodos-de-ramificacion

[53] Procedimiento de enumeración que encuentra el óptimo en forma más rápida. http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060014/html/Capitulo%20VI/egonb.htm

Figura 11 sectorización de cubrimiento de ataques posibles



FUENTE: APORTE REALIZADORES

Quiere lo anterior significar que la estructuración de fosilización del modelo con su respectivo sustento matemático, evidenciara como características estos factores de instrumentalización y operación, a saber (Lopez 2006):

- Mesurativo: Permitirá elaborar referentes de comparación, con modelos similares.
- Predictivo: Formulación de actividades para responder al… "Que pasa sí".
- Transformador: Definición de servicios y mecanismos de seguridad, como esparcir para evitar los ademanes.
- Heurístico: Interpreta operacionalmente la fonoaudiología de ataques, congelaciones y fallos produciendo normativas para captura y estudio de evidencia.

3.1.2 PROCEDIMIENTO SISTÉMICO OPERACIONAL

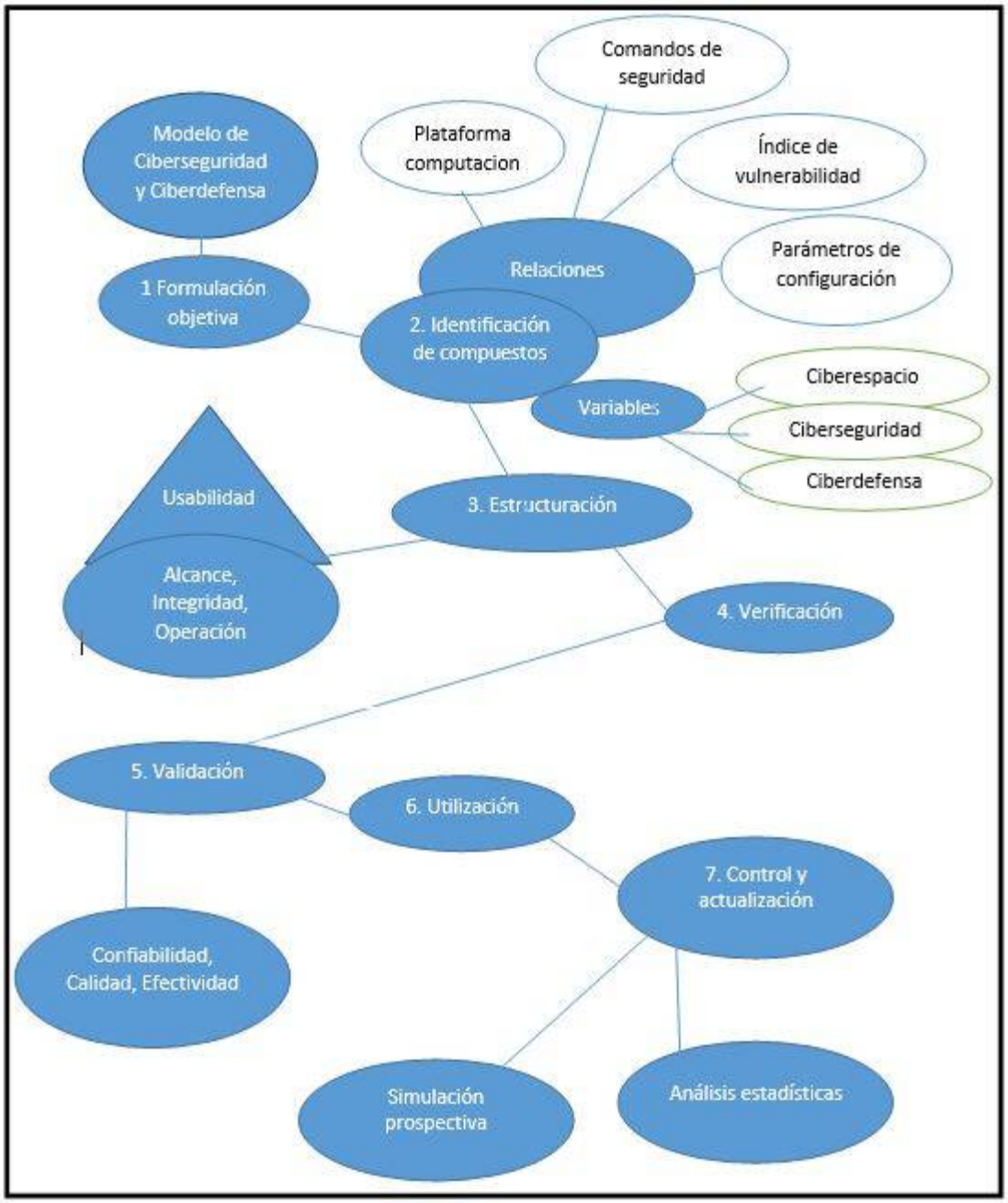
El proceso creativo que se aplicara para la construcción de la sociedad implica por necesidad el tener que considerar como base la metodología señalada en la figura 12 y de interpretar la significancia del modelo de Ciberseguridad y Ciberdefensa, a partir de la coherencia del MSV, de la operación funcional del control, como plataforma para medir, aceptar y establecer medidas correctivas, sobre lo referente de enunciar, tiempo, costo, y calidad de la valoración obtenida de estos indicadores.

- Gestión
- Eficacia
- Efectividad
- Calidad

De esta manera, se procede a ponderar y cambiar sobre el modelo, los núcleos de análisis decisional que se citan (López 2006).

- Actualidad
- Capacidad
- Potencialidad
- Intención
- Productividad
- Rendimiento

Figura 12: Metodología Construcción Del Modelo



Fuente: aporte realizadores

3.2 ESTRUCTURA LÓGICA Y FUNCIONAL DEL MODELO

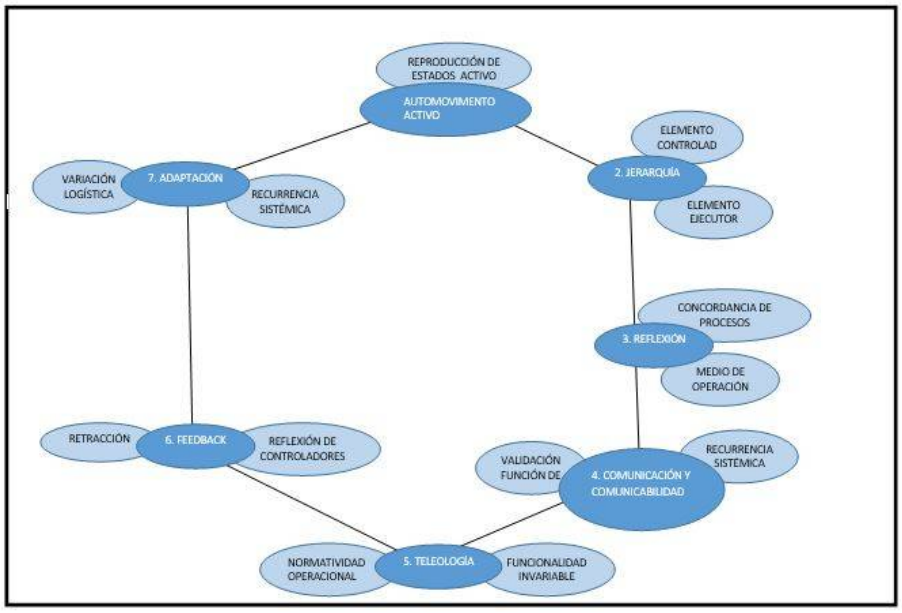
Como se presentó con antelación, todo modelo debe traslucir estructuralmente las funciones ilustrativa, traslativa, heurística, aproximativa, pronosticadora y transformadora, que validan funcionalmente la correspondencia entre el original estudiado y el modelo construido, expresan la semántica y la categorizan relacionalmente al isofuncionalismo.

Formalmente, el modelo construido como entregable de este trabajo por parte del programa de ingeniería de sistema de la universidad libre, se enmarca procedimentalmente en los vértices del heptágono de especificación que se muestra en la figura 13.

La lógica operacional del modelo esta soportada en el proceso de segmentación sistémica que integra los principios de relación analítica pertinentes a las frases que se listan seguidamente:

- Segmentación espacial
- Segmentación operacional
- Segmentación de recurrencia

Figura 13 heptágono lógico de especificación



Fuente: construcción realizadores

Cada uno de los elementos de segmentación se describirá a continuación, siendo preciso el tener previamente que definir la logística de contexto.

3.2.1 LOGÍSTICA CONTEXTUAL DE REFERENCIACIÓN

La logística que demanda la construcción del modelo, se enmarca en la especificación y tratamiento sistémico de los ejes analíticos señalados aquí:

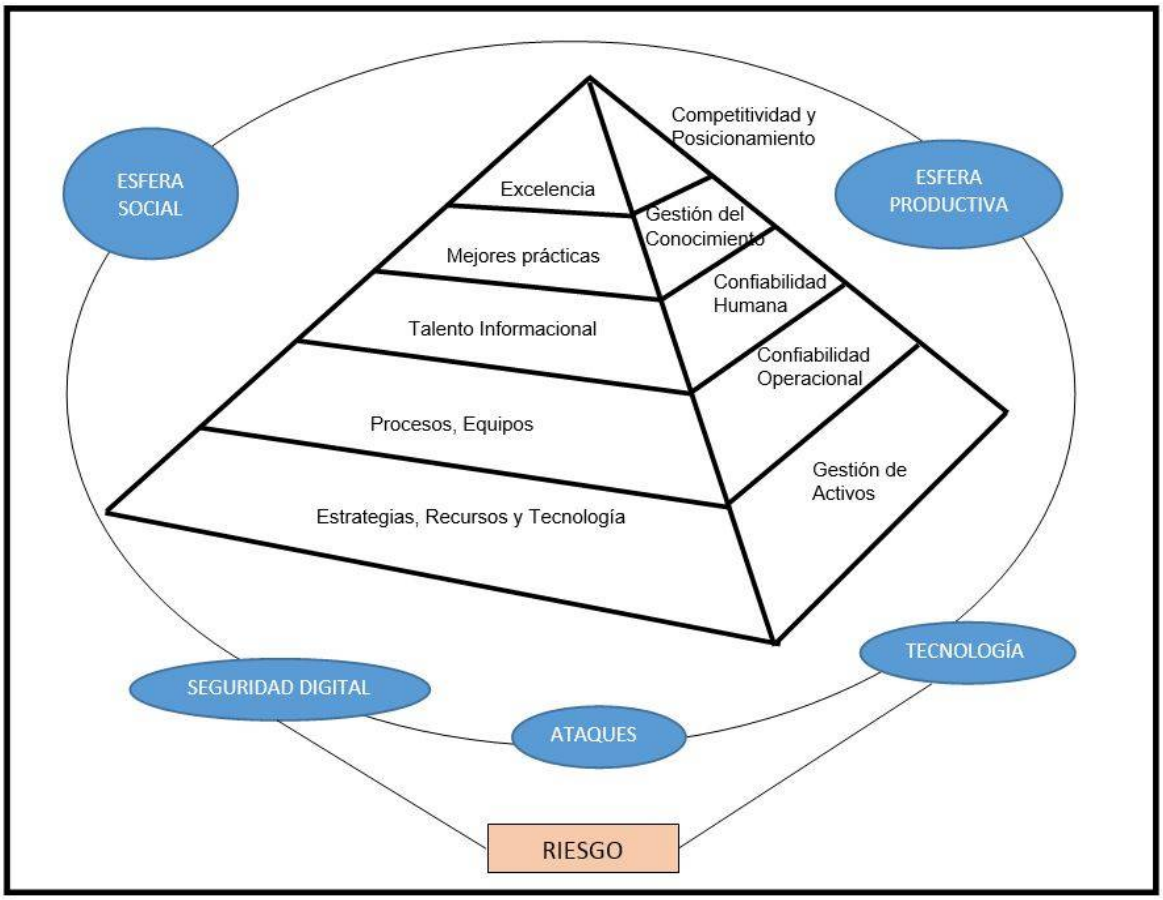
- Pirámide tecnológica
- Optimización integra
- Confiabilidad operacional
- Formalización del riesgo
- Núcleo operacional de seguridad
- Soporte logístico de seguridad
- Soporte logístico de interacción

Cada uno de estos ejes, se presente y formaliza para efectos de documentación en los numerales siguiente.

3.2.1.1 PIRÁMIDE TECNOLÓGICA

La optimización funcional en el contexto de la aldea global y de la sociedad del conocimiento implica el conocimiento de los 5 niveles de la llamada pirámide tecnológica (García 2007), pues los procesos de modelación de sistemas en el entorno de la seguridad de la información los relacionan, como base formativa para la consecución de la excelencia, los niveles o ejes de consideración se señalan con ayuda de la figura 14.

Figura 14 pirámide tecnológica



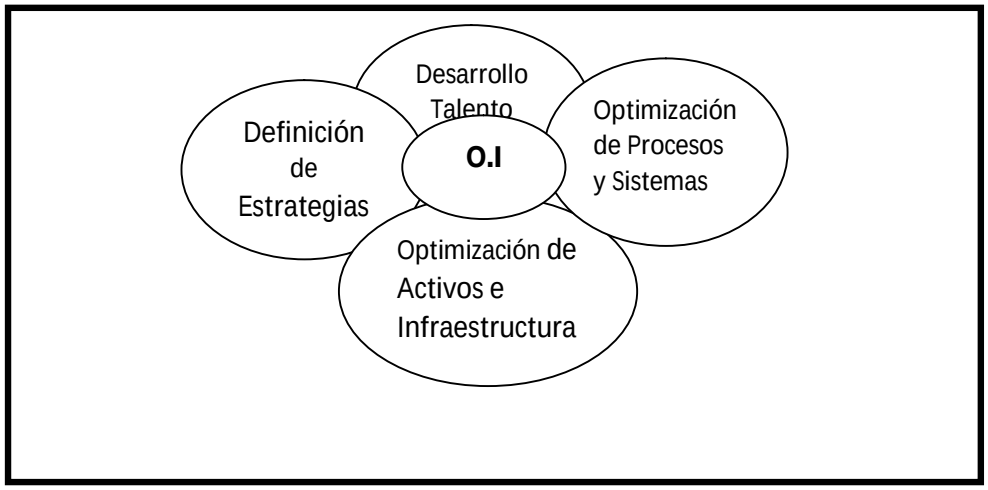
fuente: García Oliverio. Optimización integral revista Clepsidra 2007. Adaptación realizadores.

3.2.1.2 OPTIMIZACIÓN INTEGRAL

La implantación del esquema funcional del modelo para la Ciberseguridad y la Ciberdefensa colombiana, es producto de la asociación del talento humano que con sus conocimientos en seguridad digital participara como usuario final, de la formulación de estrategias, de la ponderación y evaluación de los recursos tecnológicos del manejo instrumental de los sistemas normativos de procedimientos.

Su estructura y significación operacional, se observa en la figura 15

Figura 15 Optimización Integral



Fuente: adaptación realizadores original revista Clepsidra García Oliverio

3.2.1.3 CONFIABILIDAD HUMANA

La probabilidad de desempeño eficiente y eficaz de los usuarios destinados para operar e interactuar con el modelo construido para operar e interactuar con el modelo construido, se interpreta como función de confiabilidad, esta se caracteriza por integrar sistemáticamente:

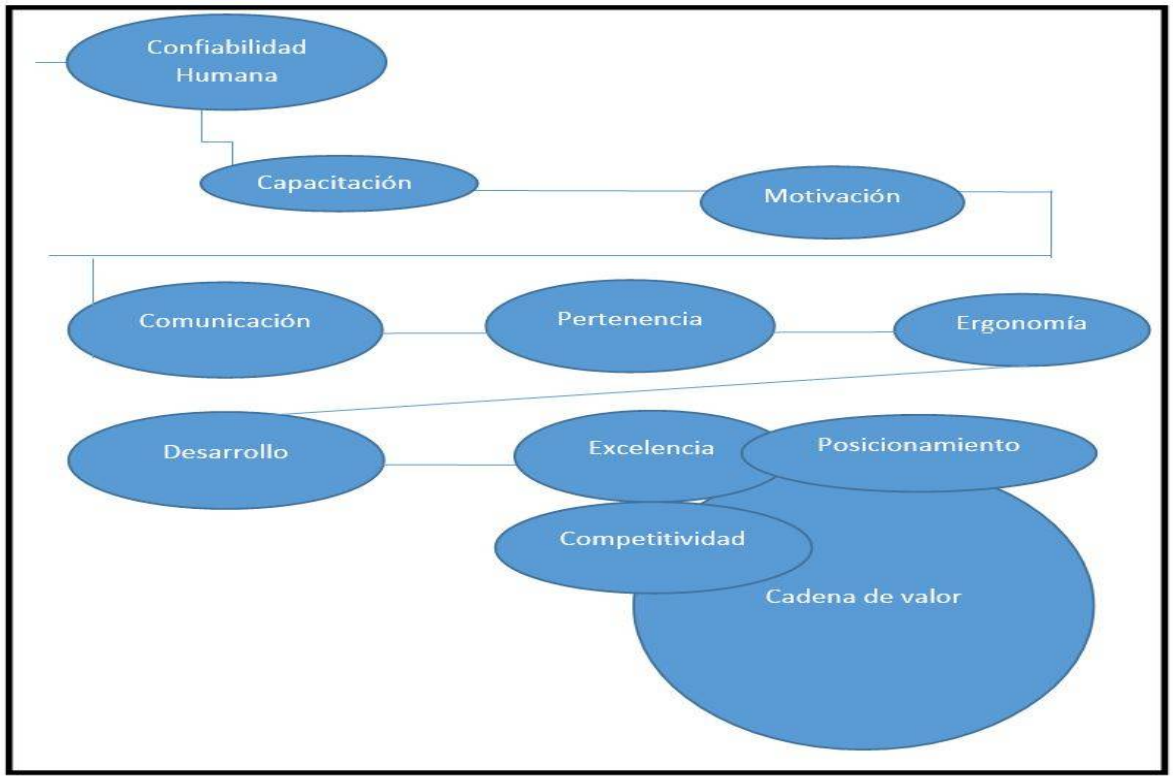
- Conocimientos, habilidades y destrezas
- Aportes del capital humano
- Desarrollo de competencias
- Incremento de creatividad e innovación
- Posicionamiento y función de utilidad
- Potenciar estrategias
- Filosofía del mejoramiento continuo

El índice de confiabilidad humana, presupone el conocimiento específico de estos factores de control conceptual:

- Sistema de comunicación de datos

- ❖ Teoría de seguridad digital
- ❖ Procedimientos de hacking ético
- ❖ Configuración de vector de ataque

Figura 16 señala los elementos asociados con la confiabilidad humana

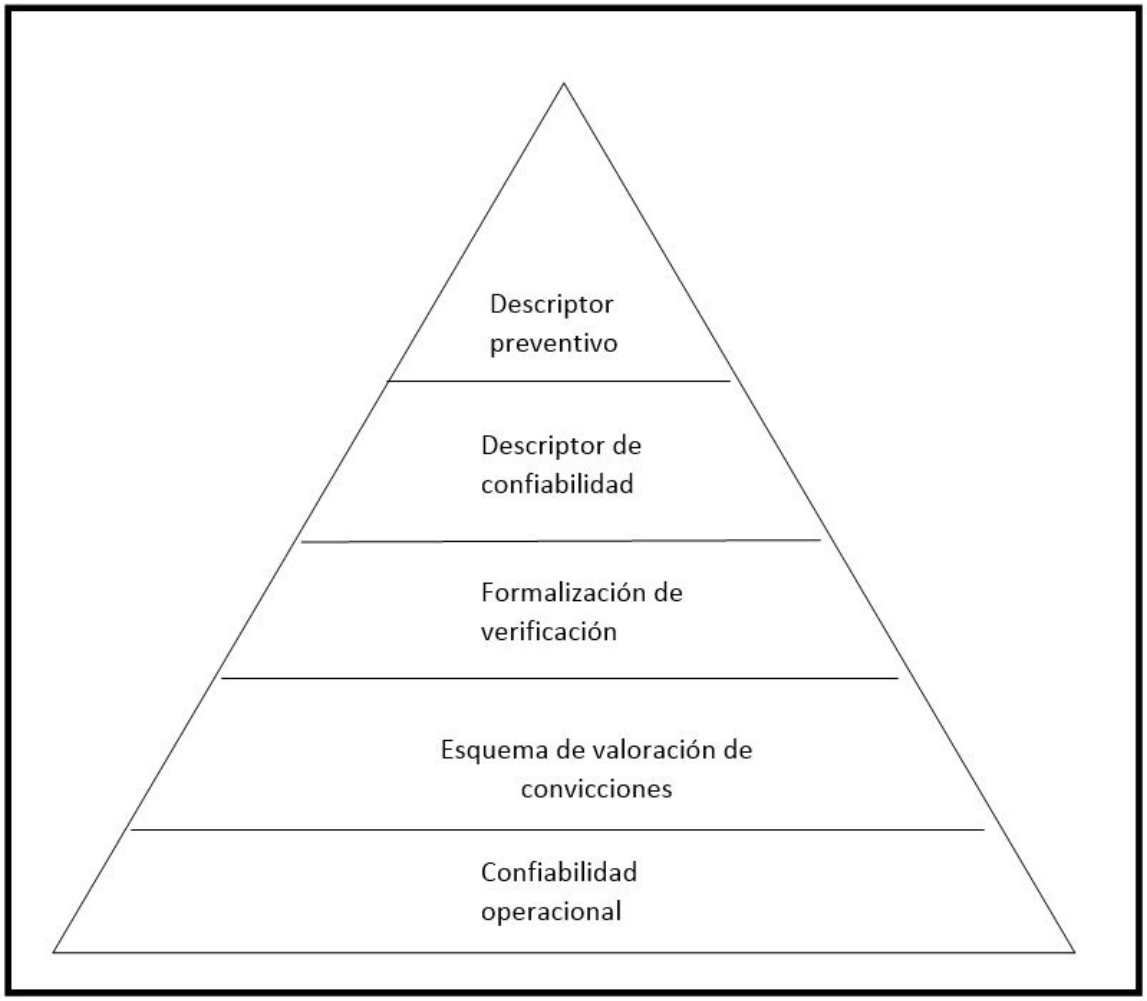


Fuente: Aporte Realizadores

3.2.1.4 CONFIABILIDAD OPERACIONAL

La confiabilidad operacional entendida como una serie de procesos de mejoramiento continuo que incorporan en forma sistémica avanzadas herramientas de diagnóstico, técnicas de análisis y nuevas tecnologías, para poder optimizar la gestión, planeación, ejecución y control (Garcia 2007); su aplicación en el diseño y construcción del modelo se transluce en el proceso de mantenimiento, sus elementos de infracción se muestran en la Figura,

Figura 17 Elementos Confiabilidad Operacional

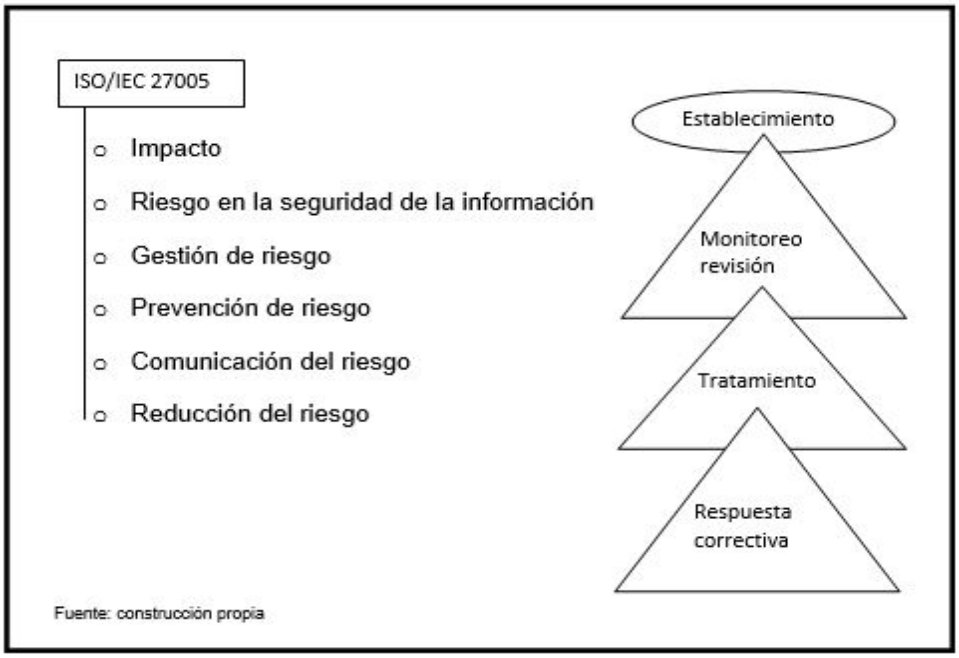


Fuente: Aporte realizadores

3.2.1.5 FORMALIZACIÓN DEL RIESGO

Siendo el riesgo un factor de alta preponderancia en la construcción del modelo, se requiere entonces conocer la norma ISO/IEC 27005, para valorar la significación funcional de los componentes mostrados en la figura 18.

Figura 18: Terminología ISO/IEC 27005



Fuente: construcción propia

3.2.1.6 NÚCLEO OPERACIONAL DE SEGURIDAD

Considerando el incremento de los ataques a la infraestructura de computación, que en la actualidad se estima en 2600 millones por hora en todo el mundo, se hace necesario el considerar los referentes siguientes:

- Generadores de especificación
  - COBIT [54](control objectives for information and relay technology)
    - Framework[55]

[54] Objetivos de Control para Información y Tecnologías Relacionadas.
https://en.wikipedia.org/wiki/COBIT
[55] Conjunto estandarizado de conceptos, prácticas y criterios.
https://es.wikipedia.org/wiki/Framework

- Process Description
- Control objectives[56]
- Management guidelines[57]
- Maturity models[58]

- Laboratorio piloto de Ciberdefensa y Ciberseguridad Fuerza Aérea Colombiana

- Unidades operacionales de los estados de gran desarrollo en la temática

  - Canadá
  - Alemania
  - España
  - Australia
  - Chile
  - USA
  - CSIRT[59](COMPUTER SECURITY INVERDENT RESPONSE)
  - CIRC[60](COMPUTER INCIDENT RESPONSE CAPABILITI)
  - IRC[61](INCIDENT RESPONSE CENTER)
  - SERT[62] (SECURITY EMERGENCY RESPONSE TEAM)

---

[56] Objetivos de control, son el *"objetivo o propósito de los controles especificados en la organización de servicios que abordan precisamente los riesgos que estos controles tienen por objeto mitigar con* eficacia".
http://www.ssae16.org/glossary/83-control-objectives--example-control-objectives-for-soc-1-ssae-16-reporting--ssae16org.html
[57] Implica los controles y lineamientos a seguir.
http://www.mintic.gov.co/gestionti/615/articles-5482_Indicadores.pdf
[58] https://en.wikipedia.org/wiki/Maturity_model
[59] Equipos de Seguridad y Respuesta de Incidentes.
https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas#Organizaciones_CSIRT
[60] Capacidad de Respuesta a Incidentes de Informática.
http://www.acronymfinder.com/Computer-Incident-Response-Capability-(CIRC).html
[61] Centro de respuesta a incidentes.
http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf
[62] Equipo de respuesta, ante emergencias informáticas.
https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas

- SIRT (SECURITY INCIDENT RESPONSE TERAL)

- Soporte logístico operacional
  - Android defender
  - Android shield
  - IPhone defender
  - Kona site defender
  - Kona DDOS defender
  - Protexic connect
  - Kona web application framework
  - Cisco intelligent wan
  - Cain &abel
  - Sans/sipt
  - Encase
  - Sleuth kit
  - Windowscope
  - Oxigeno
  - Ftk imager[63]
  - DUMPLT volatility
  - Freerecover
  - Firebug
  - Reggripper
  - Registry decodec
  - Snort[64]
  - Splunk[65]
  - Bitdefender

[63] Programa de imágenes de disco independiente.
https://www.computersecuritystudent.com/FORENSICS/FTK/IMAGER/FTK_IMG_313/lesson1/index.html
[64] Software flexible que ofrece capacidad de almacenamiento, tanto en archivos, como en bases de datos.
https://es.wikipedia.org/wiki/Snort
[65] Software para buscar, monitorizar y analizar datos generados por máquinas de aplicaciones.
https://es.wikipedia.org/wiki/Splunk

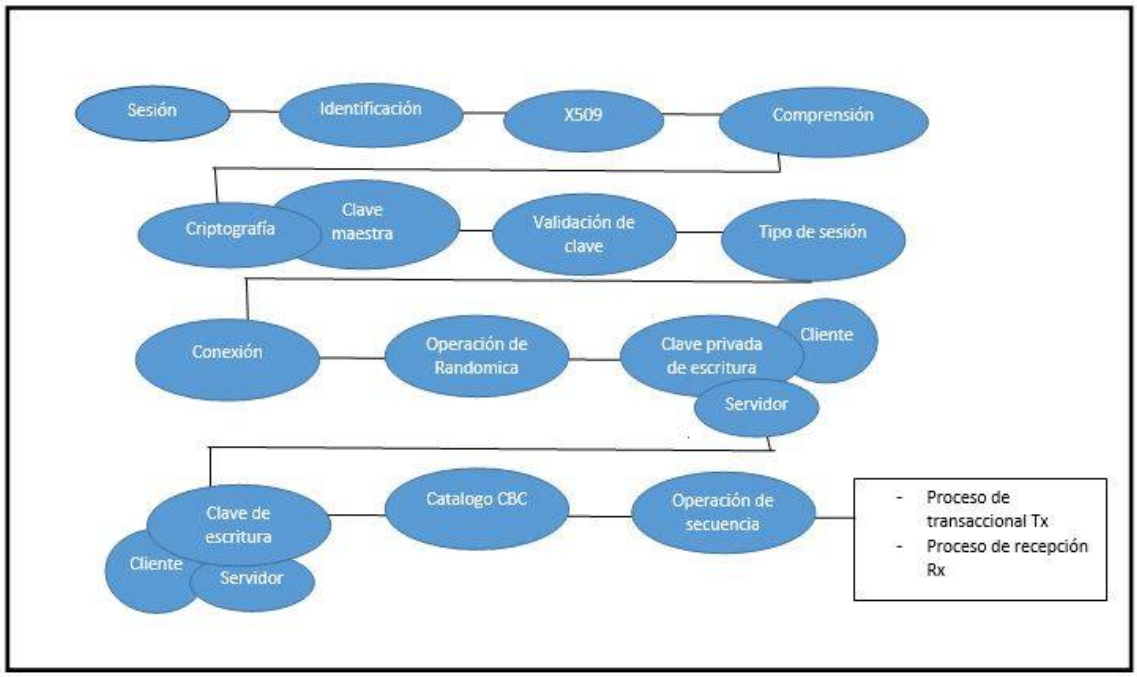
- Kaspersky
- Webroot antivirus

- Parámetros operacionales de sesión y conexión

La figura 19, los 4 niveles de referenciación operacional que cataloga los procesos de sesión y conexión, configuración durante el intercambio transaccional de valores informáticos en los dominios:

- Usuario – LAN
- LAN – WAN
- WAN – RPC
- USUARIO – RPC

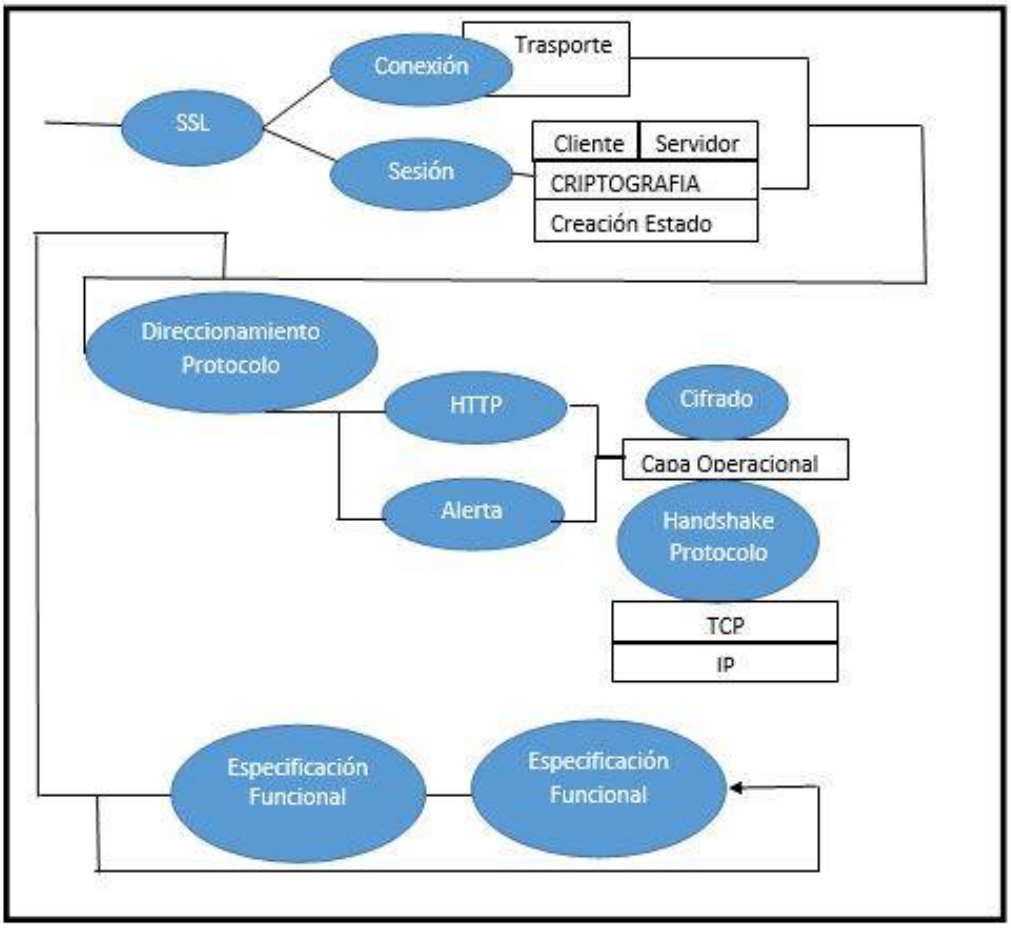
Figura 19: parámetros operacionales sesión y conexión



- **OPERACIÓN INTEGRAL DE INTERCAMBIO**

Señala la integración sesión- protocolo – capa operacional, según se muestra en la figura 20

Figura 20: Niveles De Operación De Intercambio



FUENTE: Aporte Realizador

- **ESCENAS DE VALIDACIÓN DE FLUJO**

El esquema de validación operacional de la seguridad digital, se define y estructura en los escenarios convencionales de recurrencia en los escenarios convencionales de recurrencia universal, como se lista a continuación (Stallings 2012):

- Seguridad en correo
  - PGP (Pretty Good privacy)
  - s/MIME

- Seguridad en la WEB
  - SSL (Secure Socket Layer)
  - TLS (Transport Layer Security)
  - SET (Secure Electronic Transaction)

- Seguridad IP
  - Arquitectura IPSEG
  - Formato ESP
  - Protocolo ISAKMP
  - Algoritmos De Cifrado
  - Proceso modo transporte
  - Proceso nodo túnel

3.2.1.7 SOPORTE LOGÍSTICO DE INTERCONEXIÓN

El conjunto conversacional que permite definir la interacción a nivel computacional, con los valores que fluyen en la red.
Puede ser desarrollado, empleado cualquiera de estos lenguajes, a saber:

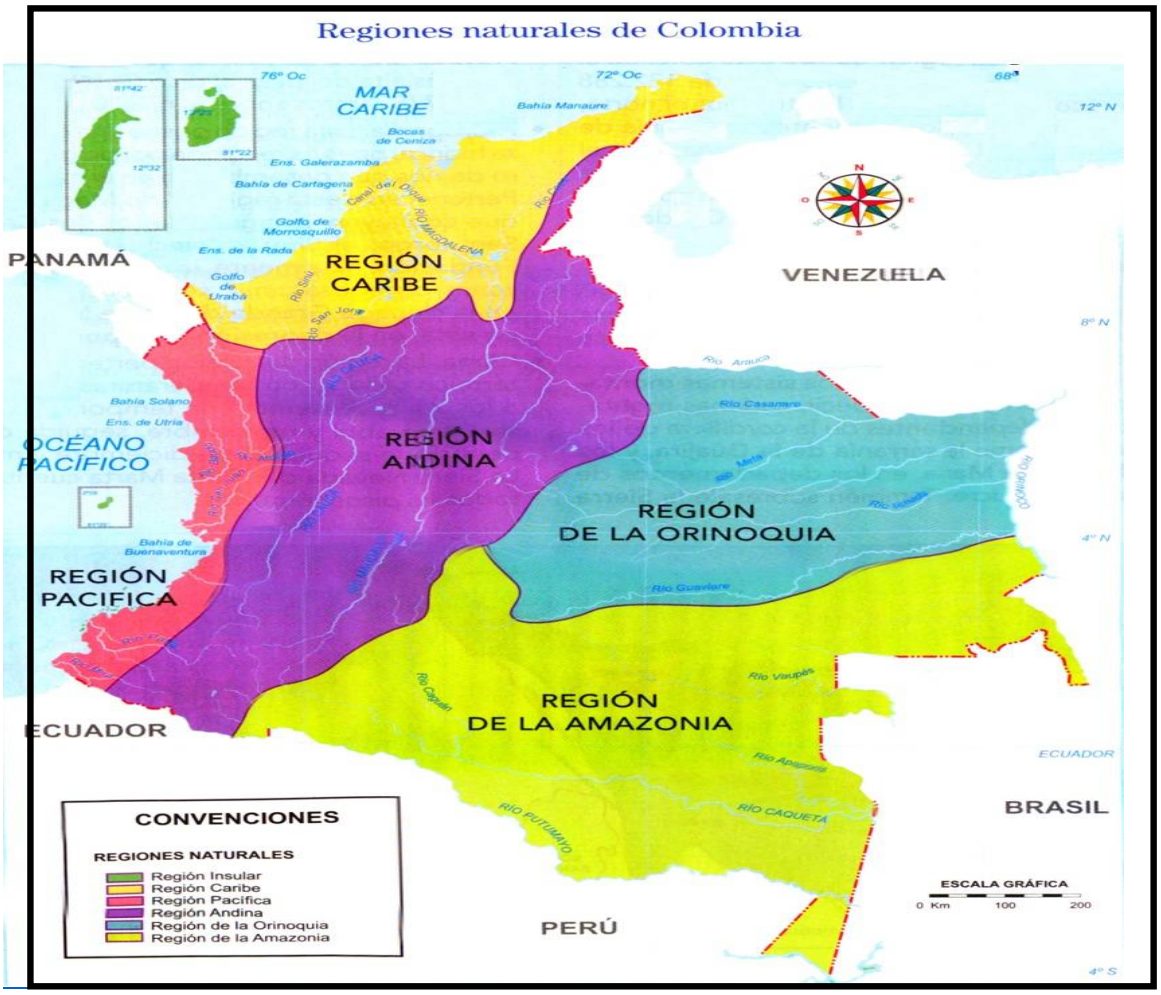
- C++
- JAVA
- JAVASCRIPT
- VBS
- DART
- OPA
- SCALA
- ERLANG
- CEYLON
- J2NE

3.2.2 SEGMENTACIÓN ESPACIAL

Colombia se encuentra ubicado en la latitud 04°00 Norte y Longitud 72°00 Oeste, políticamente está dividida en 33 Departamentos y Geográficamente diferencia 5 regiones, a saber: Atlántico, Andina, Pacifica, Orinoquia, Amazonas

El mapa muestra de la figura 20 muestra esta distribución

Figura 21: Regiones geográficas de Colombia



Fuente: http://www.socialhizo.com/images/mapas/colombia-regiones.jpg

La ubicación geográfica por departamento se cataloga por regiones, tal como sigue:

- Región Andina
  - Antioquia
  - Boyacá
  - Caldas
  - Cundinamarca
  - Huila
  - Norte de Santander
  - Quindío
  - Risaralda
  - Santander
  - Tolima

- Región Caribe
  - Atlántico
  - Bolívar
  - Cesar
  - Córdoba
  - La Guajira
  - Magdalena
  - San Andrés y Providencia
  - Sucre

- Región Amazónica
  - Amazonas
  - Caquetá
  - Guainía
  - Guaviare
  - Putumayo

- Vaupés

❖ Región del Pacifico
- Cauca
- Choco
- Nariño
- Valle del Cauca

❖ Región de la Orinoquia
- Arauca
- Casanare
- Meta
- Vichada

La estructuración y formulación del modelo de Ciberseguridad y Ciberdefensa, además de considerar la distribución geográfica del país requiere de la identificación de los sectores económicos considerados por el banco de la república[66], estos son: Sector Agropecuario, Sector Industrial, Sector de Servicios[67]

SECTORES ECONÓMICOS

La actividad económica está dividida en **sectores económicos.** Cada sector se refiere a una parte de la actividad económica cuyos elementos tienen características comunes, guardan una unidad y se diferencian de otras agrupaciones. Su división se realiza de acuerdo a los procesos de producción que ocurren al interior de cada uno de ellos.

[66] Banco central de Colombia.
www.banrep.gov.co/
[67] Sectores económicos. Concepto y clasificación.
www.banrepcultural.org/blamvirtual

División según la economía clásica

Según la división de la economía clásica, los sectores de la economía son los siguientes:

- Sector primario o sector agropecuario.
- Sector secundario o sector Industrial.
- Sector terciario o sector de servicios.

Sector primario o agropecuario

Es el sector que obtiene el producto de sus actividades directamente de la naturaleza, sin ningún proceso de transformación. Dentro de este sector se encuentran la agricultura, la ganadería, la silvicultura, la caza y la pesca. No se incluyen dentro de este sector a la minería y a la extracción de petróleo, las cuales se consideran parte del sector industrial.

Sector secundario o industrial

Comprende todas las actividades económicas de un país relacionadas con la transformación industrial de los alimentos y otros tipos de bienes o mercancías, los cuales se utilizan como base para la fabricación de nuevos productos.
Se divide en dos sub-sectores: industrial extractivo e industrial de transformación:

Industrial extractivo: extracción minera y de petróleo.

Industrial de transformación: envasado de legumbres y frutas, embotellado de refrescos, fabricación de abonos y fertilizantes, vehículos, cementos, aparatos electrodomésticos, etc.

Sector terciario o de servicios

Incluye todas aquellas actividades que no producen una mercancía en sí, pero que son necesarias para el funcionamiento de la economía. Como ejemplos de ello tenemos el

comercio, los restaurantes, los hoteles, el transporte, los servicios financieros, las comunicaciones, los servicios de educación, los servicios profesionales, el Gobierno, etc.

Es indispensable aclarar que los dos primeros sectores producen bienes tangibles, por lo cual son considerados como sectores productivos. El tercer sector se considera no productivo, puesto que no produce bienes tangibles pero, sin embargo, contribuye a la formación del ingreso nacional y del producto nacional.

Aunque los sectores anteriormente indicados son aquellos que la teoría económica menciona como sectores de la economía, es común que las actividades económicas se diferencien aún más dependiendo de su especialización. Lo anterior da origen a los siguientes sectores económicos, los cuales son:

- **Sector agropecuario**: Corresponde al sector primario mencionado anteriormente.

- **Sector de servicios:** Corresponde al sector terciario mencionado anteriormente.

- **Sector industrial:** Corresponde al sector secundario mencionado anteriormente.

- **Sector de transporte:** Hace parte del sector terciario, e incluye transporte de carga, servicio de transporte público, transporte terrestre, aéreo, marítimo, etc.

- **Sector de comercio:** Hace parte del sector terciario de la economía, e incluye comercio al por mayor, minorista, centros comerciales, cámaras de comercio, San Andresitos, plazas de mercado y, en general, a todos aquellos que se relacionan con la actividad de comercio de diversos productos a nivel nacional o internacional.

- **Sector financiero:** En este sector se incluyen todas aquellas organizaciones relacionadas con actividades bancarias y financieras, aseguradoras, fondos de pensiones y cesantías, fiduciarias, etc.

- **Sector de la construcción:** En este sector se incluyen las empresas y organizaciones relacionadas con la construcción, al igual que los arquitectos e ingenieros, las empresas productoras de materiales para la construcción, etc.
- **Sector minero y energético:** Se incluyen en él todas las empresas que se relacionan con la actividad minera y energética de cualquier tipo (extracción de carbón, esmeraldas, gas y petróleo; empresas generadoras de energía; etc.).

- **Sector solidario:** En este sector se incluyen las cooperativas, las cajas de compensación familiar, las empresas solidarias de salud, entre otras.

- **Sector de comunicaciones:** En este sector se incluyen todas las empresas y organizaciones relacionadas con los medios de comunicación.[68]

Dicha clasificación corresponde a su teleología o finalidad económica, no obstante hace preciso considerar para definición del marco proyectivo del modelo esperado, su clasificación en los sectores a saber:

- Sector agropecuario.
- Sector de servicios.
- Sector industrial.
- Sector comercio.
- Sector financiero.
- Sector de la construcción
- Sector minero y energético.
- Sector solidario.
- Sector de comunicación.

[68] Abarca los sectores económicos en general.
http://www.banrepcultural.org/blaavirtual/ayudadetareas/economia/sectores_economicos

El PIB de acuerdo con estos sectores(Los primeramente relacionados), según fuente del DANE, experimento los importes señalados por la Tabla 2.

Tabla 2: El PIB de acuerdo con estos sectores

SECTOR	**ÍNDICE**
Agropecuario	14.7
Industrial	36.3
Servicios	49.0

Fuente DANE oficina de información 2014

A nivel del control estratégico, de acuerdo con políticas del Ministerio de defensa nacional, la soberanía, la defensa, y control del estado, recae en poder de: Ejército nacional, Fuerza aérea de Colombia, Armada nacional, Policía nacional.
El ejército nacional, cuenta con las brigadas que se presentan en la tabla 3

Tabla 3: brigadas ejército nacional.

IDENTIFICACIÓN	**SEDE**
Primero	Tunja
Segundo	Barranquilla
Tercero	Cali
Cuarto	Medellín
Quinto	Bucaramanga
Sexta	Ibagué
Séptima	Villavicencio
Octava	Armenia
Novena	Neiva
Decima blindada	Valledupar

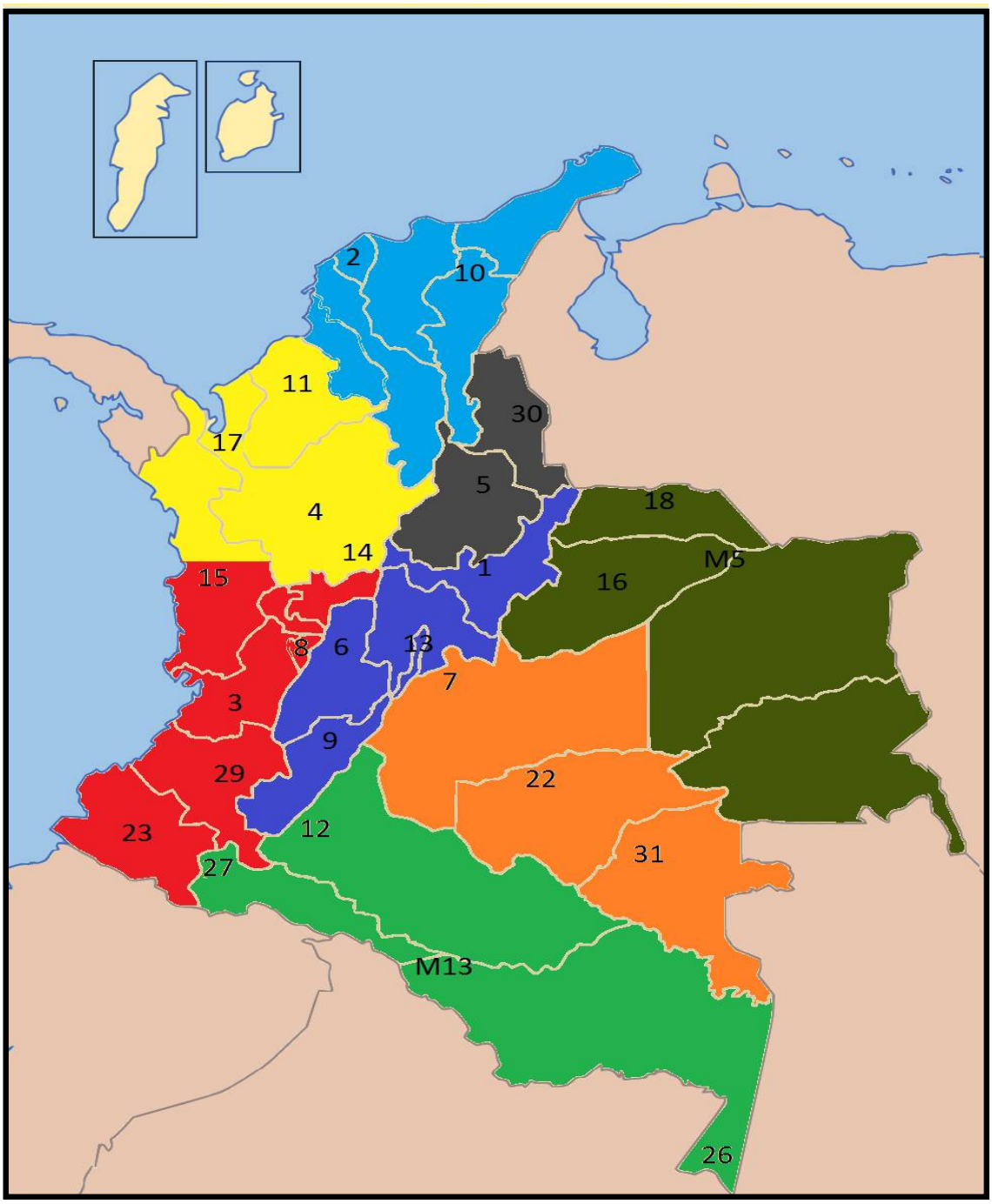
Continuación Tabla 3

Decima primera	Montería
Decima Segunda	Florencia
Décima tercera	Bogotá
Décimo cuarta	Puente Berrio
Décimo Quinto	Choco
Décimo sexta	Yopal
Décimo séptima	Mocoa
Décimo octava	Arauca
Vigésima segunda	San José del Guaviare
Vigésima tercera	Pasto
Vigésima sexta	Leticia
Vigésima séptima	Mocoa
Vigésima octava	Puerto Carreño
Vigésima novena	Popayán
Trigésima	Cúcuta
Trigésima primera	Cururú Vaupés

Fuente: Elaboración propia, información ejército nacional

En la Figura 21, se presenta la ubicación geográfica de estas brigadas.

Figura 22: Ubicación de brigadas, ejército nacional.



Fuente: Aporte realizadores.

Por su parte la fuerza aérea, cuenta con los comandos que se listan a continuación:

- Escuela militar de aviación. (Cali)
- Comando aéreo de combate N°1 (Palanquero)
- Comando aéreo de combate N°2 (Apiay - Meta)
- Comando aéreo de combate N°3 (Barranquilla)
- Comando de apoyo técnico N°1 (Melgar)
- Comando de apoyo técnico N°2 (Rio negro)
- Comando aéreo de trasporte(Bogotá):
- Militar Catan.
- Comando aéreo de mantenimiento (Madrid – Cundinamarca)
- Escuela de suboficiales (Madrid – Cundinamarca)
- Grupo aéreo del sur (Ríos Caquetá y orteguaza)
- Grupo aéreo del Caribe (San Andrés)
- Grupo negro del oriente (Vaupés)
- Instituto militar Aero acuático (Bogotá)

El mapa mostrado en la figura 22, señala estas bases de operación.

Figura 23: Unidades de operación, fuerza aérea.

Fuente: Aporte realizadores

La armada nacional, sectoriza su operación en las fuerzas y comandos:

- Fuerza nacional del Caribe
- Fuerza nacional del pacifico
- Fuerza nacional del sur
- Fuerza nacional del oriente
- Comandos de guardacostas
- Comandos de aviación naval
- Comando especifico de san Andrés y providencia

- Comando de infantería de marina
- Dirección de sanidad naval

La Policía Nacional, está distribuida en estas regiones:

- Región de Policía Nacional No 1
  - MEBOG
  - Boyacá
  - Cundinamarca
  - Amazonas
  - San Andrés y providencia

- Región de policía N°2
  - Metropolitana de Ibagué
  - Caquetá
  - Huila
  - Putumayo
  - Tolima

- Región de policía N°6
  - Metropolitano valle del aburra
  - Antioquia
  - Choco
  - Córdoba
  - Uraba

- Región de policía N|8
  - Metropolitana de barranquilla
  - Metropolitana de Cartagena
  - Metropolitana de Santa Marta

- Atlántico
- Bolívar
- Cesar
- Guajira
- Magdalena
- Sucre

❖ Región de policía N°5
- Metropolitana de Bucaramanga
- Metropolitana de Cúcuta
- Metropolitana de Arauca
- Magdalena medio
- Santander

❖ Región de policía N°7
- Metropolitana de Villavicencio
- Casanare
- Guainía
- Meta
- Vaupés
- Vichada
- Guaviare

❖ Región de policía N°4
- Metropolitana de Cali
- Cauca
- Valle del cauca
- Nariño

- Región de policía N°3
  - Policía metropolitana de Pereira
  - Caldas
  - Quindío
  - Risaralda

La Figura 24, muestra el mapa que sectoriza las regiones de policía en Colombia.

Fuente: Aporte realizadores.

Las unidades financieras de Minas y Energía, Agroindustriales, Salud y de Transporte. Están tuteladas directamente por los Ministerios

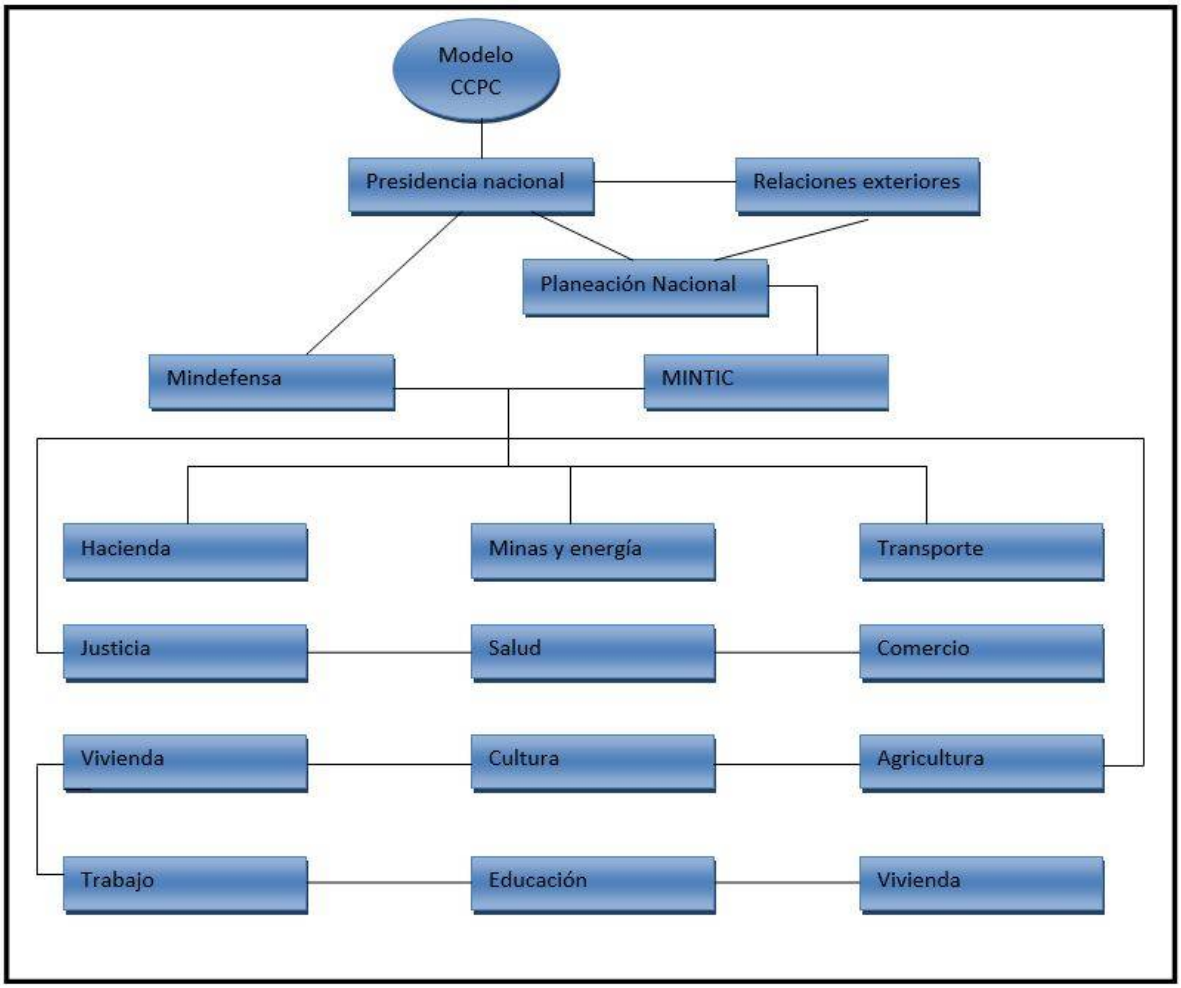
3.2.3 SEGMENTACIÓN OPERACIONAL

El modelo para la Ciberseguridad y Ciberdefensa, define su nivel de operación con la infraestructura tecnológica que se habilite en los ministerios que integran el gobierno nacional, bajo tutela directiva de acción, señalada en la figura 25.

- Ministerio De Relaciones Exteriores
- Ministerio De Hacienda
- Ministerio De Justicia Y Del Derecho
- Ministerio De Defensa
- Ministerio De Agricultura
- Ministerio De Salud Y Protección
- Ministerio Del Trabajo
- Ministerio De Minas Y Energía
- Ministerio De Comercio, Industria Y Turismo
- Ministerio De Educación
- Ministerio De Vivienda
- Ministerio De Tecnologías De La Información Y Las Comunicaciones
- Ministerio De Transporte
- Ministerio De Cultura

La tutela directiva de acción, está señalada por el nivel de cobertura de riesgo frente a un ataque.

Figura 25: Directriz tutela operacional modelo CCPC



Fuente: Aporte realizadores

El nivel de fragilidad corresponde al índice de impacto económico y potencial de vulnerabilidad frente a un ataque.

3.2.4 SEGMENTACIÓN LOGÍSTICA INTEGRAL

La infraestructura que define la logística del proceso de diseño, construcción y valoración del modelo de Ciberseguridad y Ciberdefensa para Colombia, está enmarcada en el tratamiento de los conceptos que a continuación se señalan:

- Arquitectura hardware
  - Servidores de correo
  - Servidores de base de datos
  - Servidores de clúster
  - Servidores web
  - Servidores de imagen

- Elementos de simulación
  - Distribuciones de publicidad
  - Método de Montecarlo
  - Líneas de espera
  - Procesos de Markov

- Conceptos de comunicaciones
  - Osciladores de integración a gran escala
  - Sintetizadores de frecuencia
  - Receptores AM
  - Frentes de onda
  - Modulación QAm-8/QAm-16
  - Modulación por pulso
  - Multicanalización por división de frecuencia
  - Comunicaciones satelitales
  - Spread spectrum
  - Redes de fibra óptica

- Principios de modelación
  - Estructuración funcional
  - Valoración de recurrencia
  - Formalización matemática
  - Estructuración matemática concurrente

- Teoría de seguridad digital
  - Espacio geométrico de nación
  - Herramientas de exploración
  - Detección de vulnerabilidades
  - Parametrización de control
  - Herramientas de recuperación
  - Valoración del riesgo

Con la figura 26, se resume el proceso de segmentación logística integral, aclarando que el manejo procedimental de la teoría de modelos puede desnudar la utilización de otros principios o referentes teóricos.

La segmentación logística, presupone que el grupo realizador, ha evaluado con propiedad otras experiencias en el escenario de la Ciberseguridad y Ciberdefensa, pertinentes al umbral de la guerra de la información, por ejemplo:

  - Ataque de pulso electromagnético o bomba del arco iris
  - Caja FARADAY[69]
  - Auroras e ionización[70]
  - Espectro electromagnético
  - Disipadores de frecuencia
  - Cañon de microondas (Microwave canon)

Adicionalmente ha evaluado, para completar su visión de trabajo, esta serie de documentos:

- Reporte www.gao.gov/new.items/dro338.pdf
- Marco legal:

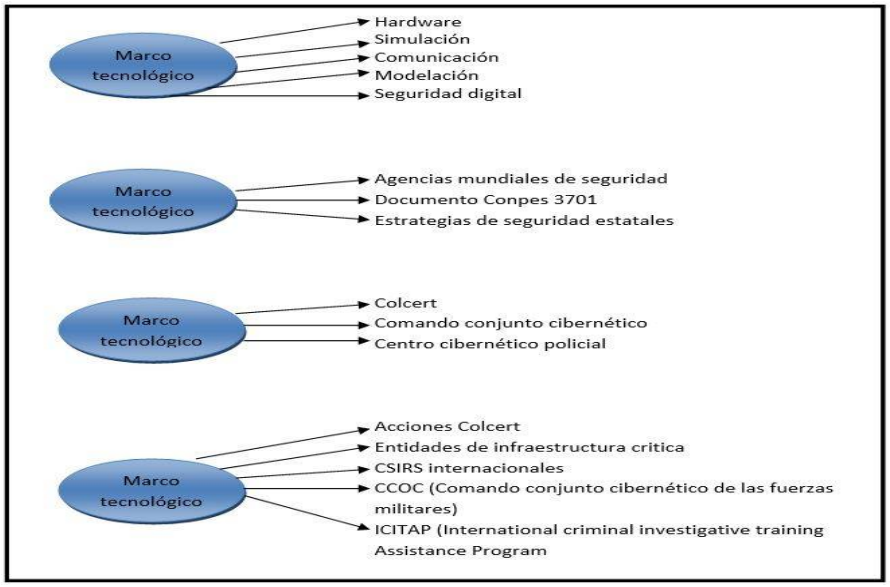
[69] Se conoce de esta manera, por su campo electromagnético en su interior. https://es.wikipedia.org/wiki/Jaula_de_Faraday

[70] Sistema dinámico, en constante cambio, gobernado por múltiples parámetros. https://es.wikipedia.org/wiki/Ionosfera

- Ley 527
- Ley 599
- Ley 962
- Ley 1150
- Ley 1273
- Ley 1341
- Circular 052 de 2007

- Resolución AG/RES 2004 OEA
- Convenio sobre Ciberdelincuencia del concejo de Europa (CCC)
- Decisión 587 de la comunidad andina
- Estrategia de seguridad cibernética de Alemania
- Estrategia canadiense de seguridad cibernética para Canadá
- Estrategia internacional para el ciberespacio USA
  - Trabajos conjuntos de estas comisiones: COLCERT, comando conjunto cibernético, Comando cibernético policial

Figura 26. Entidades segmentación logística integral



Fuente: Aporte realizadores

3.2.5 SEGMENTACIÓN DE RECURRENCIA

Básicamente en el que hacer computacional, se dice que la serie de Fibonacci, es una ecuación de recurrencia o ecuación en diferencia, que se expresa como:

$$a_n = a_n - 1 + a_n - 2 \quad (n \geq 3)$$

Su definición (viñas 2011). Es esta: Retención de orden K con coeficiente constante en la que se verifica.

$$c_n a_n + c_{n-1} a_{n-1} + c_{n-2} a_{n-2} + \ldots + c_{n-k} a_{n-k} = b_n$$

Validando,

$c_n, c_{n-1}\ y\ c_n - k\ son\ constantes$ <> 0

b_n sucesión

n>=k

Significando que para la construcción del modelo, se tendrá que repercutir este concepto, al operar el siguiente conjunto de parámetros:

- Estructura
- Objetivos
- Restricciones
- Características de los controles
- Certidumbres de parámetros
- Numero de objetivos
- Numero de restricciones

Se habla en modelación de recurrencia, cuando se abordan temáticas alusivas al control de flujo, por ejemplo ¿cuál es la acción a construir cuando un servidor es atacado desde dos focos o puntos diferentes?, O ¿cuál es el estado de respuesta si un hacker rompe la seguridad y cancela el servidor que monitorea el intercambio transaccional?; en ambos interrogantes se valida la existencia fenomenológica de un suceso de hechos, la presencia de un conjunto de elementos valoradores de riesgo (Cn) y el condicionamiento de respuestas programadas ante el ataque (K).

La medición de la probabilidad de ocurrencia del riesgo y de su impacto producido, conlleva en seguridad digital a valorar la función de recurrencia o su ecuación de diferencia, lo mismo sucede cuando se interpreta el problema de la vulnerabilidad de una configuración o sistema teleinformático, en este caso, por ejemplo se debe considerar la descripción de tráfico, numero de servidores, probabilidad de bloqueo y trafico perdido, cuyo comportamiento se define por la ecuación:

$$\varepsilon_{ri}(m,a) = \frac{a*Erj(m-1,a)}{a*Erj(m-1)+m}$$

Función de Fourier

Idéntico procedimiento, se hace en comunicación con la serie de Fourier, expresado como:

$$R(\mathcal{W}) = \int_{-\infty}^{\infty}(\mathcal{F}1(t)Cos\,wt + \mathcal{F}2(t)Sen\,wt)dt$$

$$X(\mathcal{W}) = \int_{-\infty}^{\infty}(\mathcal{F}2(t)Cos\,wt + \mathcal{F}1(t)Sen\,wt)\,dt$$

La segmentación de recurrencia, permitirá entonces formular el esquema descriptivo que determina en el poder construir la imagen de respuesta para esta fenomenología del modelo, aclarando que así como se citó la serie de Fibonacci al comienzo, se puede determinar por ejemplo el valor del término número 30, sin conocer los otros, solo se debe saber:

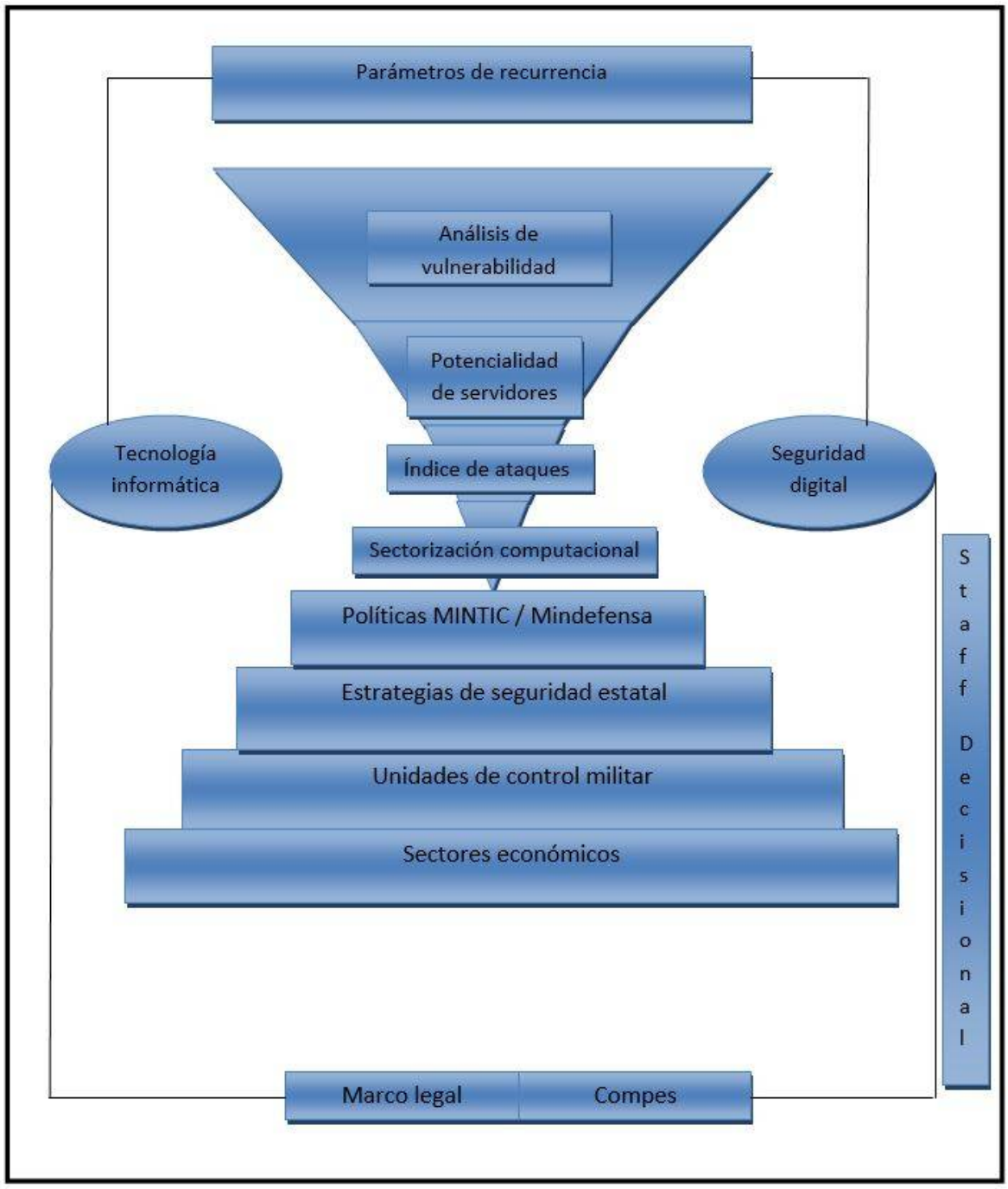
$$\text{FN} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Que al trasladarse al caso de estudio, se produce este constructo

- ¿Qué ataque puede surtirse sobre el sector petrolero por camuflaje de equipamiento computacional?
- ¿Cuándo una firma digital, puede ser suplantada al operar una acción sobre equipos e infraestructura militar?
- ¿Cómo se detectaría una vulnerabilidad sobre sistemas homogéneos?
- ¿Qué volumen de tráfico se detiene al interactuar con el Middleware configurado?
- ¿Cuál es la trazabilidad del efecto causado por el ataque realizado?

En el proceso de construcción del modelo, se integrara este acervo de conocimientos, al validar los componentes de recurrencia, mostrados por la figura 27.

Figura 27: Componentes de recurrencia



Fuente: Aporte realizadores

3.3 ESTRUCTURA Y FORMULACIÓN DE LA SOLUCIÓN

El modelo de Ciberseguridad y Ciberdefensa para Colombia, implica el tratamiento de la dualidad acción contra restadora, acción de respuesta, con la Ciberdefensa se elimina el riesgo y con la Ciberseguridad se formula los mecanismos y procedimientos de confiabilidad, seguimiento y destrucción del objetivo catalogado como enemigo o responsable de la operación de ataque.

El MCCPC (Modelo de Ciberseguridad y Ciberdefensa para Colombia), valida como producto, los principios que categorizan la bimodalidad (leal 2008), siendo está definida como dos o más aplicaciones de los nodos que como atributos en estados transitorios sirven para desigual ideas independientes de ellas, validando, interpretados y proyectando su relación y funcionalidad en el contexto, quiere lo anterior decir que el MCCPC, trasluce los diferenciadores:

- Esencia:

  Define el ¿Qué es?

- Presencia:

  Especifica su materialidad y espacialidad respondiendo al ¿Cómo es?

- Temporalidad

  Señala la relación con el usuario, determinando su contexto, y diciendo como es el ¿Cuando?

- Función

  Describe la finalidad o teología y señala como se cumple, para expresar y validar el ¿Para qué? y el ¿Cómo?

- Imagen

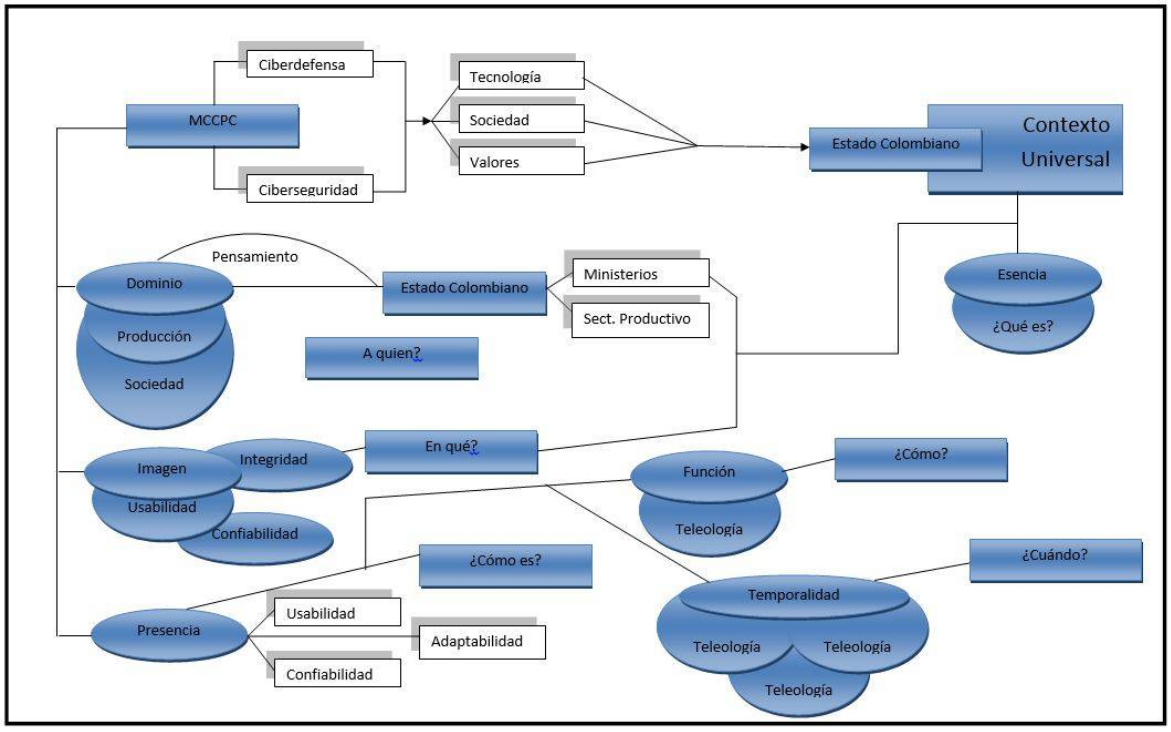
  Cuantifica su espacio de acción y dimensiona la confiabilidad de sus variables y relaciones, responde el interrogar ¿A qué?

- Dominio

  Asocia su territorialidad, su campo operacional y alcance espacial, señalando lo pertinente a la respuesta a ¿Para quién?

En la figura 28, se presentan lógicamente los núcleos diferenciadores del MCCPC, según visión y pensar de los realizadores, para así categorizar la modalidad teratológica.[71]

Figura 28. Núcleos Diferenciadores del MCCPC



Fuente construcción propia

[71] Categoría que referencia espectacularidad (lo que va más allá de la norma) y lo enigmático (laberinto construido por acción de la inteligencia). Revista Clapsidra No 6 Fuanc 2008.

La estructuración y formulación del modelo, construido por el programa de ingeniería de sistemas de la universidad libre, involucra los siguientes ejes de acción operacional, a saber: Eje de catalogación y significado, Eje de análisis económico, Eje de ponderación sistémica y valoración de infraestructura, Eje de valoración de funcionalidades
Sus características, principios funcionales y estructura sistémica, se presenta en los numerales siguientes:

3.3.1 EJE DE CATALOGACIÓN Y SIGNIFICANCIA

La complejidad y variedad del MCCPC, como unidad cibernética cuantificable y dimensionable posee su propia dinámica, autorregulación y esclavización funcional, pues su formalización estructural se halla enmarcada dentro del MSV (modelo de sistema viable)[72]. Que identifica y opera estas unidades funcionales o sistemas (Lopez 2010)

- Sistemas nominales
  - Unidades de organización básica
  - Unidades de coordinación
- Metasistemas
  - Unidades de gerencia
  - Unidades de control operacional
  - Unidades de planificación global
  - Unidades responsables de la formulación de políticas

La construcción del MCCPC, presupone establecimiento de un proceso de planeación, la esquematización operacional (Davila, 1995)
El proceso de planeación, se presenta en la figura 28, y dentro del diagnóstico, se identifican estas fases (Morgan, 2006): Recolección de información, Clasificación de la

[72] MSV. Stafford beer Determina que el querer hace continuamente se remplaza por el aprender y desaprender continuamente, valorando la competencia eficiencia y eficacia. Lopez Menphis. FUNC 2010.

información comparación y contraste, Identificación de problemas, Jerarquización de problemas.

Se aclara para efectos de validación funcional, que la diferencia de control[73], que se aplica el proceso de construcción del modelo, integral las fases que se listan:

- Relación y verificación logro de objetivos
- Medición: control señala medición y cuantificación
- Detección de desviaciones
- Establecer medida correctivas

En el MCCPC, se pueden valorar estos indicadores de gestión:

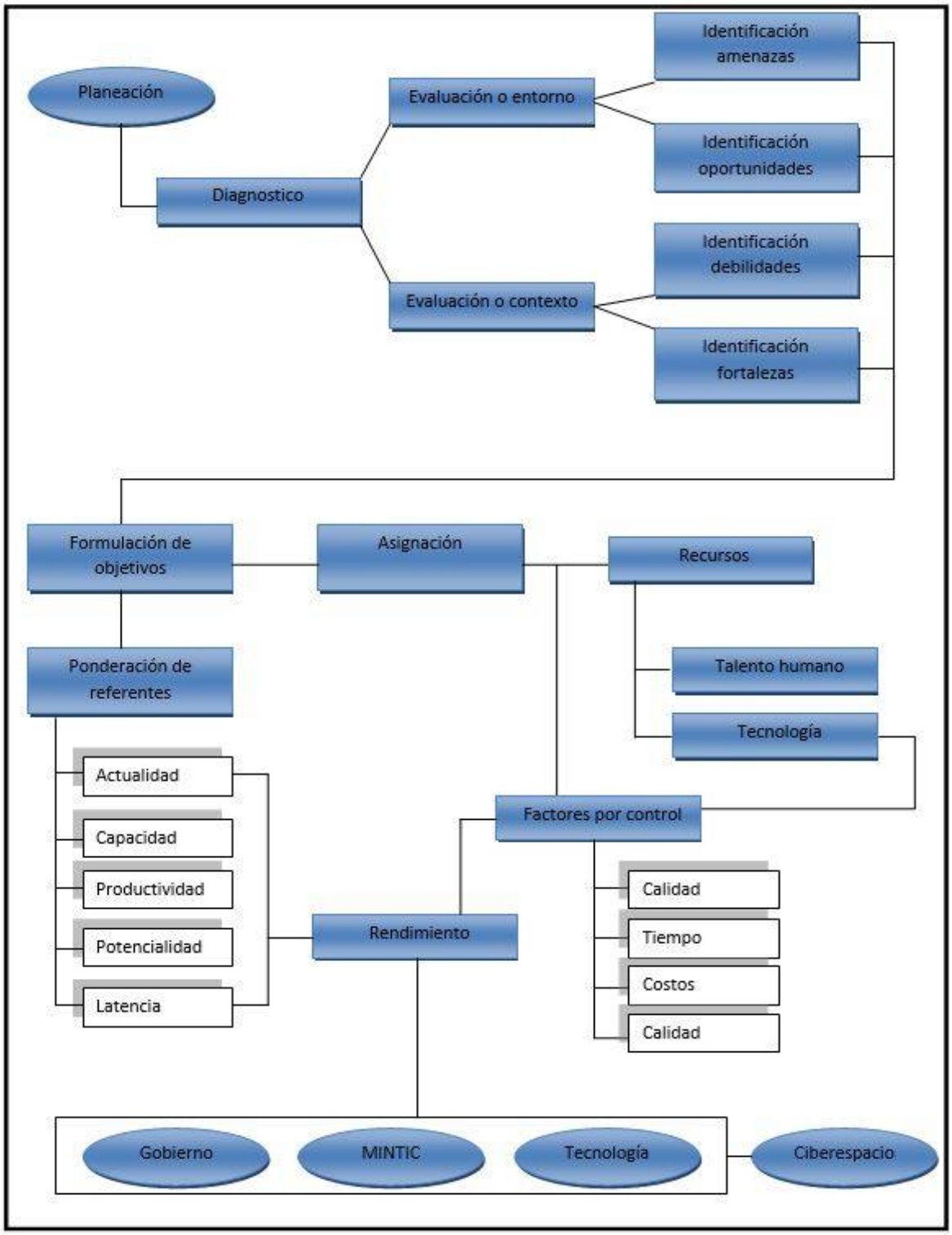
- Eficiencia: mide la relación entre los resultados obtenidos y los recursos requeridos
- Eficacia: relación entre el logro alcanzado y los objetivos propuestos
- Efectividad: sumatoria de eficiencia y eficacia
- Calidad: atributo que valora los servicios de coherencia, sincronizados e integridad de los resultados generados por el modelo.

La interpretación de la figura 29, será producto de la asociación sistémica de: Insumos, Procesos y Resultados

}

[73] Función que mide lo logrado. Corrige las desviaciones y establece correctivos. Lopez Menphis. FUNC, 2010.

Figura 29: proceso de planeación



Fuente: creación propia

La catalogación y significancia del MCCPC, se define mediante la asociación y validación del conjunto siguiente de referentes:

- Arquitectura de seguridad
  - Servicios
    - Autentificación
    - Control de acceso
    - Confidencialidad
    - Integridad
    - No repudio
  - Mecanismos
    - Cifrado
    - Firma digital
    - Control de acceso
    - Integridad
    - Relleno de trafico
    - Control de enrutamiento
    - Normalización
  - Eje de operación
    - Correo electrónico
    - IP
    - WEB
    - Gestión de RED

- Patronato de control

    - Detección de intrusos
    - Control software dañino
    - Protección con cortafuegos

- Plataforma logística teleinformática
    - Unidad operacional en GRID, con diferenciación expresa de estas capas(Tanebaum 2012)
        - Aplicación
        - Capa colectiva
            - ✓ Capa de conectividad
            - ✓ Capa de recursos
            - ✓ Capa de fabricación

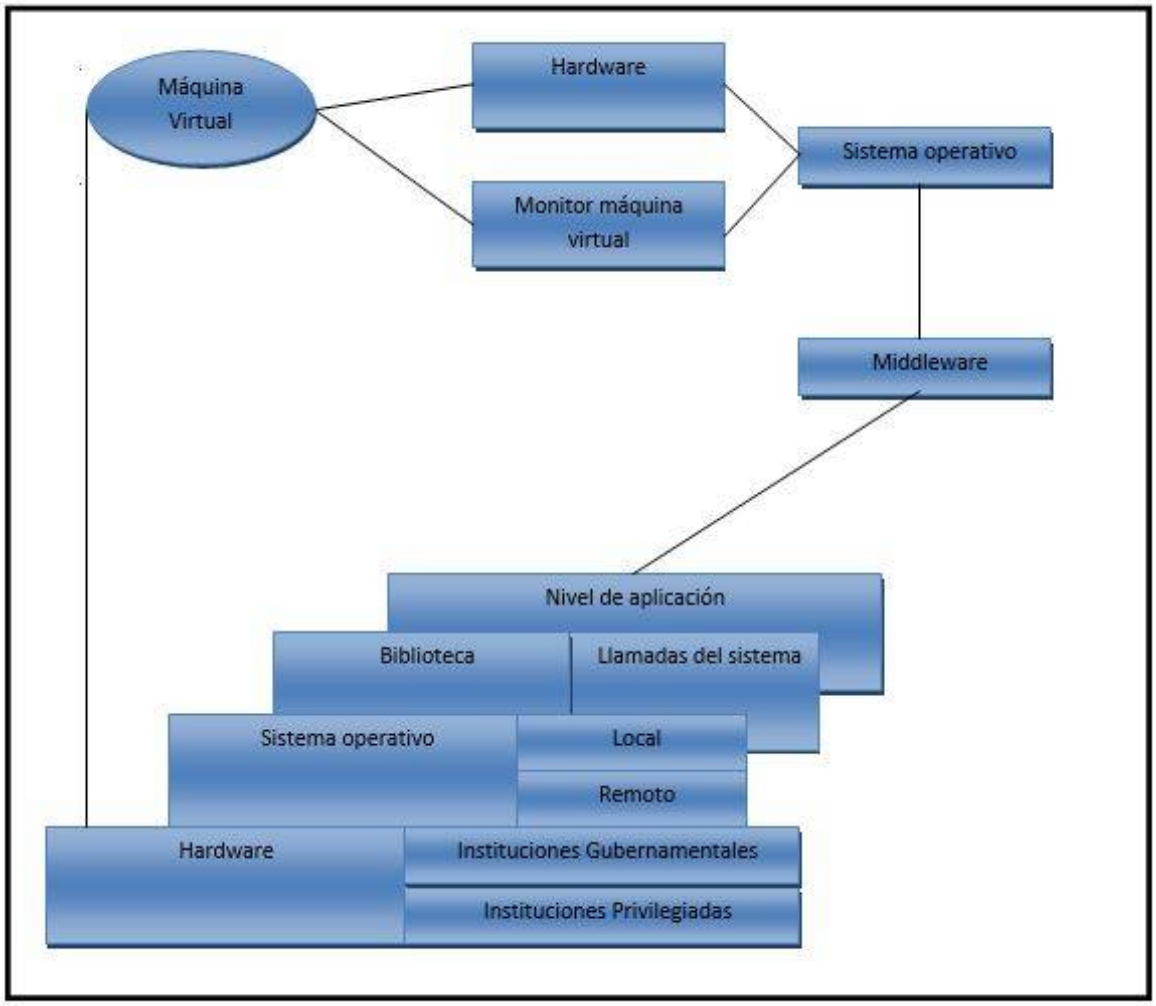
    - Concurrencia basada en Middleware
        - Aplicación cliente
        - Comunicación Middleware
        - Aplicación servidor

    - Estructuración de interceptores[74]
        - A nivel de solicitud
        - Objeto Middleware
        - A nivel de mensaje

    - Proceso de virtualización como método diferenciador e integrador operacional como se observa en la figura

[74] Software que rompe el pulso de control usual y habilita la ejecución de otros. Tanebada andreas 2012.

Figura 30: interfaces de virtualización



Fuente: Aporte Realizadores

- Encadenamiento RPC
  - Llamada cliente
  - Matriz construye mensaje
  - Se envía mensajes por la red
  - El SO entrega mensaje al servidor(Resguarda)
  - Se desempaqueta mensaje
  - El resguardo ejecuta operación de control

- Operacionalidad de primitivas SOCKET[75]
  - SOCKET
  - BIND
  - LISTEN
  - ACCEPT
  - CONEX
  - SEND
  - REVIVE
  - CLOSE

- Calidad de servicio (Qos) (Halsall 2001)
  - Velocidad de BITS
  - Retraso en la configuración de sesión
  - Tiempo de envío y recepción
  - Multitransmision
  - Sincronización de reloj
  - Transmisión concurrente por reloj lógico

- Técnica de escalamiento
  - Consistencia centrada en cliente
  - Protocolo de escritura replicada

- Tolerancia a fallas
  - Sincronía virtual
  - Realización bifásica
  - Realización trifásica

[75] Punto final de las comunicaciones entre computadoras.
https://es.wikipedia.org/wiki/Socket

- Control de acceso
  - Matriz de control
  - Dominio de protección
  - Cortafuegos
  - Código móvil

- Administración de seguridad
  - Administración de claves
  - Distribución de claves
  - Administración KDC[76](key distribución centers)
  - Capacidad y certificados
  - Automontaje: semántica de sesión

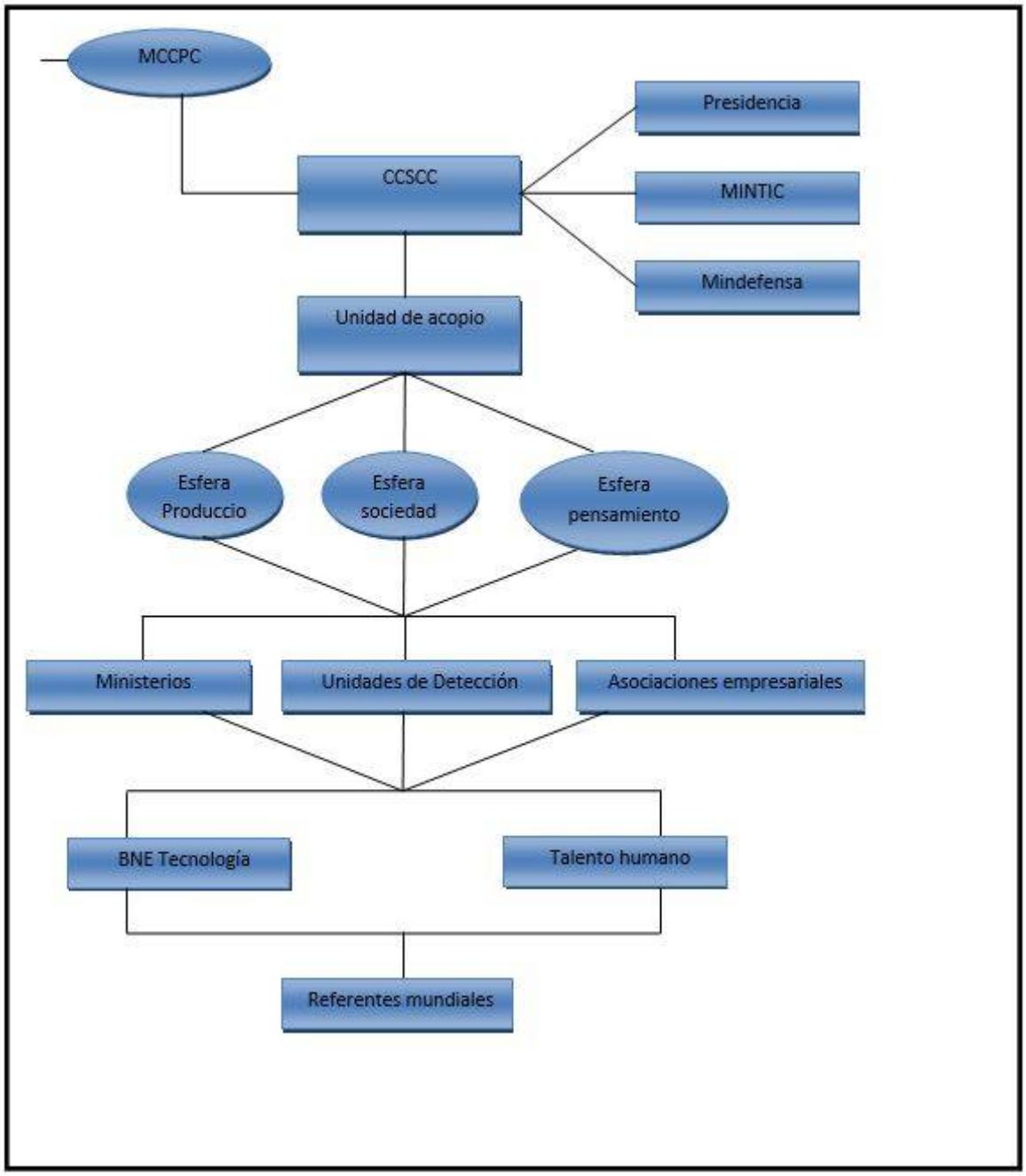
- Formalización de servidores
  - Basados en clúster
  - Sincronización
  - Replicación de sistemas web
  - Redes de entrega de contenido
  - Capa de socket seguro (SSL)
  - Capa de transporte seguro (SSL)

La significancia operacional del MCCPC, se presenta en la figura 31, los componentes funcionales de control se observa en la figura 32.

Esta significancia operacional establece el entorno relacional y componentes funcionales establecen la integración del CCSCC (centro de control y supervisión para la Ciberseguridad y Ciberdefensa) como unidad rectora con los niveles de protección y distribución que distribuirán el proceso de seguridad con los servicios y mecanismos

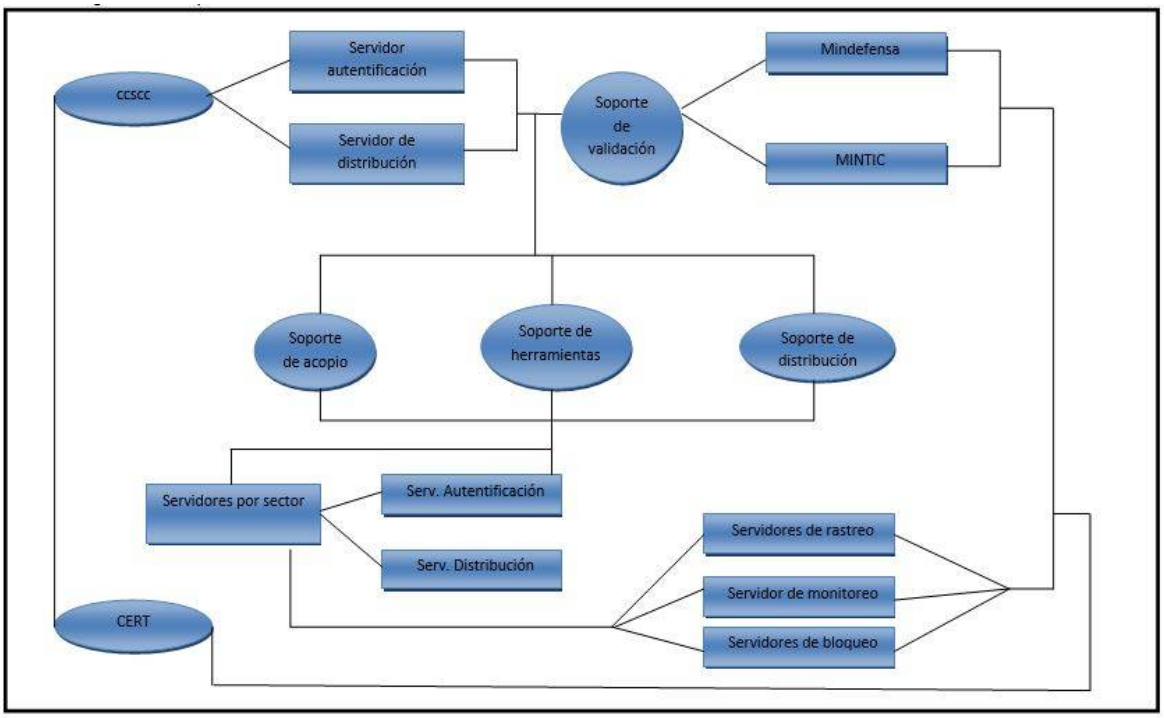
[76] Parte de un sistema criptográfico destinado a reducir los riesgos inherentes en el intercambio de claves. https://en.wikipedia.org/wiki/Key_distribution_center

Figura 31: significación operacional MCCPC



Fuente aportes realizadores

Figura 32: componente funcionales MCCPC



Fuente realización propia.

Los servidores de rastreo, monitores y bloqueos, actuar según especificación del CERT (computer emergency responce team), siendo responsable de cumplir con estas operaciones, a saber:

- Validación del Cipherspec (especificación de cifrado)
- Codificación de transferencia MINE base 64
- Generación de códigos de alerta
  - ✓ Acceso denegado
  - ✓ Autoridad certificación desconocida
  - ✓ Cancelado por usuario TLS
  - ✓ Error de decodificación TLS
  - ✓ Error de descifrado
  - ✓ Error de no renegociación
  - ✓ Error de restricción de exportación

- ✓ Error de seguridad insuficiente
- ✓ Error de sobrecarga de registro

- Generación de registro de auditoría (Denning 1997)
  - ✓ Nativos
  - ✓ Específicos de detención
  - ✓ Contador
  - ✓ Calibre intervalo de tiempo
  - ✓ Empleo recursos

- Detección distribuida
  - ✓ Agente Host
  - ✓ Monitor LAN
  - ✓ Monitor LAN-WAN
  - ✓ Monitor central

- Comprobación de contraseña por aplicación del modelo de Markov(Stralling 2012)

W= [m,a,t,k]
m= número de estados en modelo
a= espacio del estado
t= matriz de probabilidad de transición
k= orden del modelo

$$T(i,j,k) = \frac{f(i,j,k)}{f(i,j,p)}$$

De esta forma, se detectan los llamados falsos positivos por acción del comprobador de contraseñas al operar funciones hash, su estructura matemática queda definida por (Bace 2001):

$$p = (1 - e^{kd/n})^k$$

$$p = (1 - e^{k/r})^k$$

$$R = \frac{-k}{\log(q - p^{1/k})}$$

k= número de funciones hash

n= número de bits en tabla hash

d= número de palabras en diccionario

r= n/d, relación longitud tabla hash y tránsito de diccionario

- Validación del constructor matemático que define la criptografía por curva elíptica[77]
- Generación de procesos antivirus
  - ✓ Emulador CPU
  - ✓ Explorador de firma de virus
  - ✓ Control de emulación

- Implementación de sistemas de normatividad digital[78]
- Catalogación de bloqueo de acciones
  - ✓ Modificación y destrucción de archivos
  - ✓ Formateo de unidades
  - ✓ Cambio en logística de archivos
  - ✓ Creación de scripts

[77] Han sido utilizadas para probar el último teorema de Fermat y en factorización de enteros. https://es.wikipedia.org/wiki/Curva_el%C3%ADptica

[78] Decretos e implantaciones demarcadas para la normatividad digital. http://www.dian.gov.co/contenidos/servicios/mecanismo_certificado.html

3.3.2 EJE DE VALORACIÓN ECONÓMICA

Considerando que el MCCPC, demanda la adquisición de una completa base de tecnología de alto impacto y potencialidad, se hace necesario que el gobierno por participación directa de planeación, ministerio de hacienda, MINTIC, y Mindefensa junto con el entrenamiento directivo del sector productivo. Dota al CCSCC, con el presupuesto necesario para la implementación del modelo.

La valoración económica del CCSCC, conlleva el manejo formal y estructuración de estándares del conjunto siguiente de escenarios logísticos, a saber:

3.3.2.1 NEGOCIACIÓN Y COMPRA DE TECNOLOGÍA

Empleo del algoritmo Hungaro[79], para asignar óptimamente el recurso al mejor oferente minimizando costos.

Este algoritmo acepta la matriz de análisis y construye la matriz de equivalencia resultante, tal como se observa en la figura 33.

[79] Algoritmo de optimización el cual resuelve problemas de asignación en tiempo https://es.wikipedia.org/wiki/Algoritmo_h%C3%BAngaro

Figura 33: Algoritmo húngaro: componentes

- Matriz de análisis:

Empresa / Recurso	E1	E2	E3	E4
R1	C1	C2	C3	C4
R2	C5	C6	C7	C8
R3	C9	C10	C11	C12
R4	C13	C14	C15	C16

Costos recursos

- Matriz de asignación

Empresa / Recurso	E1	E2	E3	E4
R1	0	0	1	0
R2	0	1	0	0
R3	1	0	0	0
R4	0	0	0	1

- Proceso de asignación

Comprar R3 en E3 Negociar R3 con E1

Adquirir R2 en A2 comprar R4 en E4

Fuente: Aportes realizadores

3.3.2.2 VALOR MONETARIO ESPERADO (VME)[80]

Determinación del beneficio total que obtiene al ponderar por cada estrategia de inversión su utilidad

$$e(x) = \sum_{i=1}^{n} x_i * p(xi)$$

[80] La suma de los resultados finales de la alternativa.
http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060015/Lecciones/Capitulo%20I/vme.htm

$e(x)\ beneficio\ neto\ esperado$

$\sum_{i=1}^{n} xi\ \ estrategia\ de\ analisis$

$-p(xi) probabilidad\ asociada$

3.3.2.3 DERIVACIÓN FUNCIÓN DE UTILIDAD (RHEAULT 2002)

Determinación de la función de utilidad por derivación de loterías de referencia.

$$L = \{(\mu, E1), (l - \mu, E2)$$

$(\mu, E1)\ indice\ de\ alta\ favorabilidad$

$(l - \mu, E2) indice\ de\ menor\ favorabilidad$

Para formalizar el riesgo de pérdida por acceso equivocado de negociación o desactivar licencia de la plataforma tecnológica que se adquirió.

La función de utilidad, entre asociada con los diferentes contratos que se hagan.

3.3.2.4 CRITERIO DE DECISIÓN BAYESIANO

Determinación de la confiabilidad y funcionalidad de la plataforma computacional que se negocia.

$$p(Ei|Ej) = \frac{p(Ei) * p(Ej|Ei)}{\sum_{i=1}^{n} p(Ei) - p(Ej|Ei)}$$

Con el proceso, se asegura total nivel de confiabilidad en la operación de los servidores de rastreo, monitoreo y bloqueo, que se mostraron en la figura 31.

3.3.2.5 DEPRECIACIÓN BASE TECNOLÓGICA

La inversión relacionada en la adquisición de la tecnología negociada, por su caducidad presidir del conocimiento del tiempo de caducidades componente o equipo computacional; para ello el CCSCC, deberá establecer como estrategia de control la elaboración de la correspondiente tabla de deprecación por insumo.

Por ejemplo si su equipo se compra en 1000 dólares y su periodo de uso o de vida, se fija en 5 años la tabla de depreciación, posterior en la tabla 4 señala el valor de salvamento de dicho equipo, al finalizar su utilización.

El cálculo de la depreciación se hace por sumatoria de los dígitos de los años, que se valida matemáticamente

$$TD = \frac{pe * valor}{\sum digitos\ de\ los\ años} = \frac{pe * 1000}{1 + 2 + 3 + 4 + 5} = \frac{1000 * pe}{15}$$

$TD = tasa\ de\ depreciacion$

$pe = periodo\ de\ referencia$

Tabla 4: Calculo de depreciación base tecnológica

Periodo	Tasa Depreciación	Depreciación Acumulada	Valor libre
2016	333.33	333.33	666.66
2017	266.66	599.99	400.00
2018	200.00	799.99	200.00
2019	133.33	933.32	66.68
2020	66.66	999.98	0.013

Fuente aporte realizadores

Se observa que la inversión de los 1000 dólares, al cabo de los 5 años, solo representa para el CCSCC, tan solo un valor de 0.013 dólares, de ahí la importancia en conocer el proceso de depreciación.

3.3.2.6 ANÁLISIS PROYECTOS DE INVERSIÓN

El CCSCC, se puede enfrentar a la realización de proyectos para trabajar en el MCCPS, debiendo decidir cálculos se deben incluir y cuales rechazar, para maximizar la tasa de retorno anual (TIR)[81], previo conocimiento de los elementos asociados con: Nombre del proyecto, Inversión a realizar, TIR (retorno anual de inversión)
Cuya estructura de solución, se formula, por aplicación de métodos de bifurcación tipo mochila (Prawda 2006), que se planea así:

$$\max Z = \sum_{i=1}^{n} ViXi$$

$$sujeto\ a \sum_{i=1}^{n} KiXi \leq k \qquad Xi \geq 0$$

Xi= Li: si se incluye
Xi= 1: cuando se rechaza

Y el proceso conlleva a construir un árbol binario que determina:

- Solución optima
- Alternativas imposibles

Pudiéndose también encontrarse la solución esperada al aplicar los métodos de enumeración implícita del como el aditivo de Balas para resolver problemas binarios, o resolver a otros algoritmos de la programación entera[82]

[81] La tasa interna de retorno o tasa interna de rentabilidad
https://es.wikipedia.org/wiki/Tasa_interna_de_retorno
[82] Conocida también como programación lineal.

La valoración económica del MCCPC, se resume en la adquisición de estos componentes:

- 2 servidores para autentificación y distribución que opere en el CCSCC
- 2 servidores de validación para Mindefensa y el MINTIC
- 3 servidores para soporte de acopio, almacenamiento y distribución por ministerio
- 3 servidores para rastreo, monitoreo y bloqueo por cada ministerio

Debe tenerse presente que cada División, Brigada, Comando o Unidad de Control poseerá también los 2 servidores de autenticación y los 3 servidores para rastrear, monitores y bloqueos.

Se considera pertinentemente, el establecer que este proceso permitirá dar inicio tanto a nivel funcional como operacional, al CCSCC; debiendo ser distribuido de la siguiente manera:

- Adquisición capacidad tecnológica
- Compra de escudos de disipación: Nivel hardware, Nivel software
- Negociación software de seguridad
- Adquisición herramientas de rastreo, monitoreo y eliminación
- Contratación talento especializado que pondrán cada unidad de segmentación brindando apoyo de respuesta inmediata
- Conformación grupo seguidor y controlador de gama del espectro electromagnético, para analizar la estructura de ataques y amenazas y activar acciones de seguridad
- Consecución orientación y asesoría especializados de agencias internacionales que han implementado en países amigos modelos de espectros operacionales de similares

---

https://es.wikipedia.org/wiki/Programaci%C3%B3n_lineal

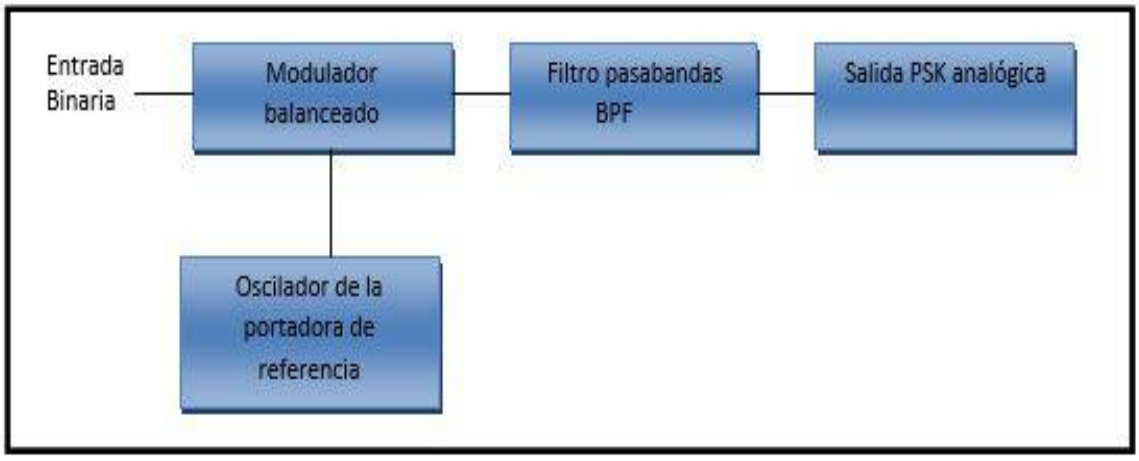
3.3.3 EJES DE DIMENSIONAMIENTO Y PONDERACIÓN SISTÉMICA

Agrupa este contenido, los aspectos relacionados con los factores de acción operacional que contemplan tanto la ponderación y valoración de la infraestructura como la valoración de la funcionalidad, actividades que relacionan el nivel operacional de confiabilidad de los escudos y disipadores de control, que eliminan acciones de los pulsos electromagnéticos (EMP) y de las radio frecuencias de alta energía (HERF), junto a la formalización analítica del proceso de simulación que determina la confiabilidad de uso del NCCPC.

3.3.3.1 ESTRUCTURA DE ESCUDOS DE PROTECCIÓN HARDWARE

Sabiendo que las señales de modulación y demodulación son pulsos digitales, es necesario trabajar la transmisión por desplazamiento de fases binaria (BPSK)[83], cuyo modulador posee la estructura señalada por la figura 33; debe entenderse que BPSK es una forma de modulación de onda cuadrada de portadora suprimida de una señal de onda continua (Tomasi 2012)

Figura 34: estructura modulador BPSK



Fuente: Tomasi, Wayne comunicaciones electromagnéticas

[83] Señal modulada. https://es.wikipedia.org/wiki/Modulaci%C3%B3n_por_desplazamiento_de_fase#BPSK_.28PSK_Binario.29

El ancho de banda del BPSK, permite el operar como fase de salida, el equivalente a:

Salida=*(sen Wct) x (sen Wat)*

(sen Wct)= frecuencia fundamental de la señal moduladora binaria

(sen Wat)= portadora no modulada

$$= \frac{1}{2}\cos(Wc - Wa)\, t - \frac{1}{2}\cos(Wc + Wa)\, t$$

Cuando se emplea no modulador balanceado, la salida, se determina mediante la ecuación:

Salida=*(sen Wc t) x (sen wct)*

$$salida\ sen^{2\,wct}$$

$$pero\ sen^2 wct, se\ puede\ valorar\ como$$

$$-sen^2\, wct = \tfrac{1}{2}(1 - cos2wct)$$

$$= \frac{1}{2} + \frac{1}{2}\ cos2wct\ < con\ filtrado >$$

$$= +\frac{1}{2}v = 1\ logico$$

$$= -\frac{1}{2}v = 0\ logico$$

La figura 34, señala la relación del a fase de salida contra tiempo para el modulador BPSK, al aceptar como entrada la correspondiente señal.

Funcionalmente, todo modulador QPSK, con dos entradas I=(-1 y senwct) y Q(-1 cos Wct) generan estas salidas

Modulador balanceado I=(-1)(sen Wct)

=-1 sen Wct

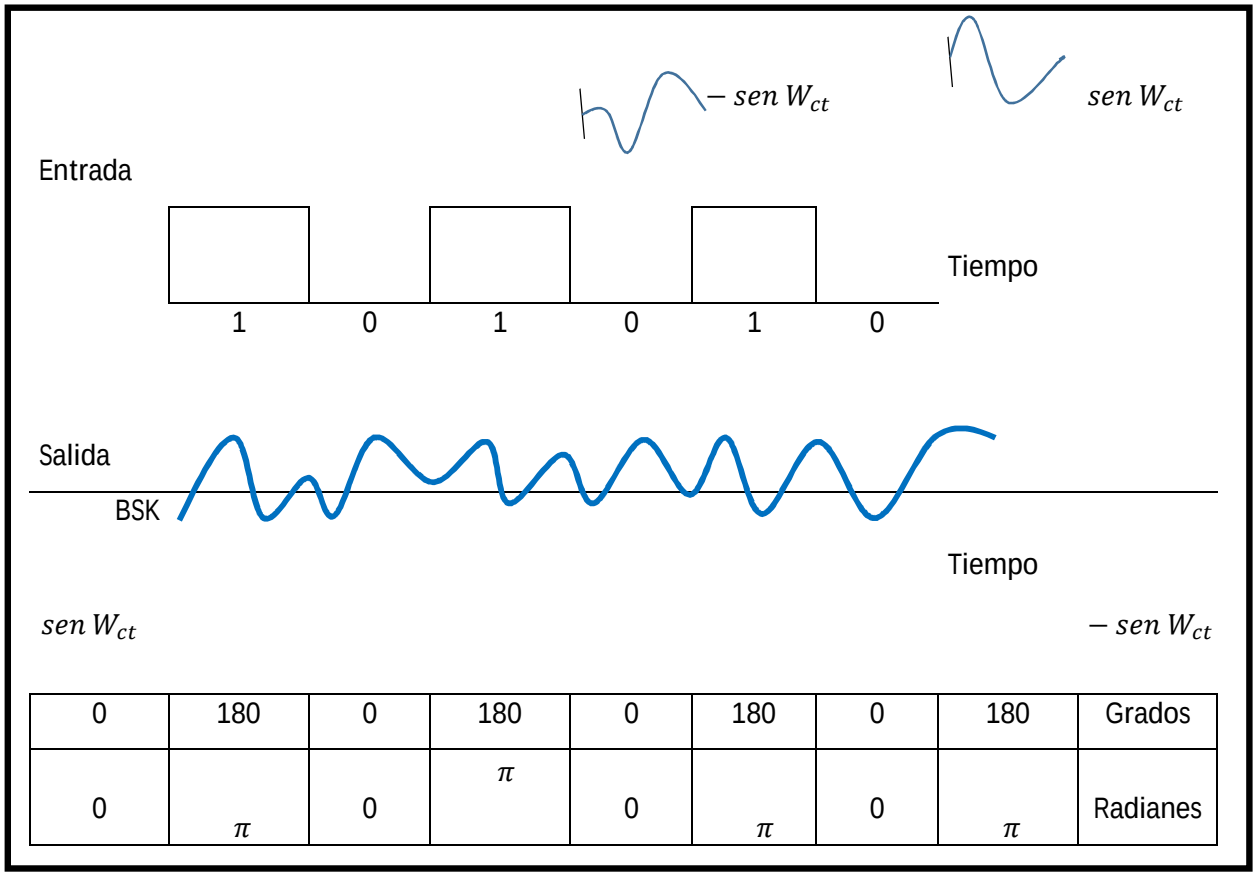
Modulador balanceado Q=(-1)(cos Wct)

Q=-1 cos Wct

Siendo la salida del sumador lineal

-1 cos Wct- 1 sen Wc

Figura 35: relación fase de salida control tiempo



0	180	0	180	0	180	0	180	Grados
0	π	0	π	0	π	0	π	Radianes

Fuente: Tomasi Wayne Comunicaciones electromagnéticas

Complementariamente, se puede considerar la QPSK de compensación, para estructurar como las formas de onda de los BIT I y Q se cambian en fase entre sí por la mitad del tiempo de BIT y la funcionalidad del transmisor QAM de dieciséis[84] (16-QAM), que facilita el control y amplitud en forma variada.

El dimensionamiento de la eficiencia en BPSK, OPSK, 8-PSK Y 16-OMM, al operar una tasa de transmisión de lo MBPS con un ancho de banda respectivamente de 10, 5, 3.33 y 2.5 mhz, se valora así (Tomasy 2012)

- $\varepsilon(\text{BPSK}) = 1\text{bps/hz} = 1\,\text{bit/ciclo}$
- ε(BPSK)=1bps/hz= 1 bit/ciclo
- $\varepsilon(\text{OPSK}) = 2\,\text{bps/hz} = 2\text{bit/ciclo}$
- ε(8-psk)= 3 bps/hz= 3bit/ciclo
- $\varepsilon(16-\text{OMM}) = 4\,\text{bps/hz} = 4\text{bit/ciclo}$

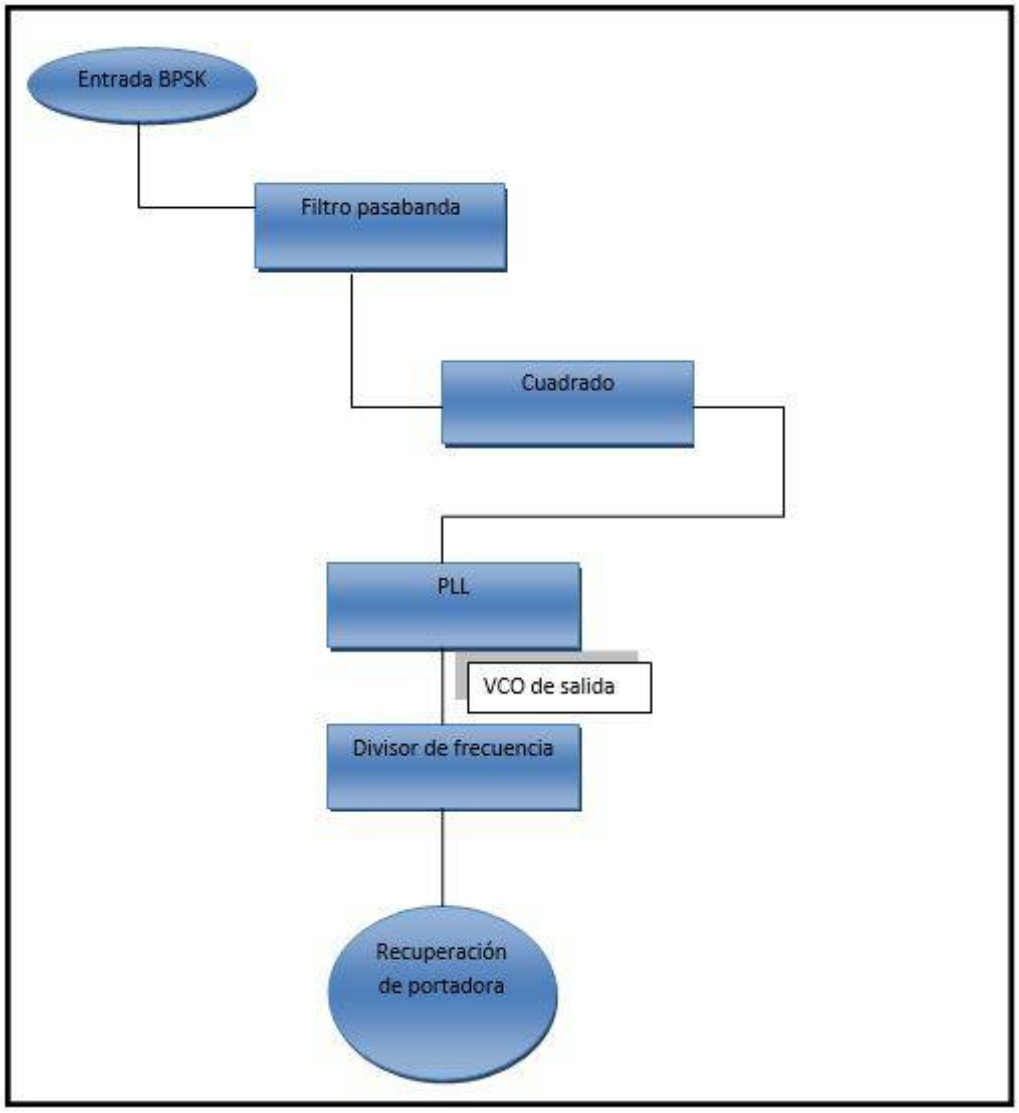
Que generaliza su proyección hacia la construcción de escudos disipadores, toda vez que mediante un circuito cuadrado[85], se obtiene una salida equivalente a.

$$\frac{1}{2}(1-\cos 2\,Wct) = sen^2 Wct$$

Cuyo circuito de recuperación de portadora, se presenta en la figura 36.

[84] Transmisor de salida. (En BITS).
http://www.electronicafacil.net/tutoriales/MODULACION-DIGITAL-FSK-PSK-QAM.php
[85] https://es.wikipedia.org/wiki/Efecto_Joule

Figura 36: circuito de recuperación de portadora



Fuente: adaptación realizadores original de Tomasi Wayne

Teniendo en cuenta que la modulación digital se emplea en los sistemas de radio digital y satélites modulados con frecuencias entre los megaHertz y los gigaHertz, es posible construir escudos de protección de recuperación y eliminación frente al impacto de la guerra de la información. Pero también puede valorarse la acción de un disipador de frecuencias como escudo de protección directa, sus característica de visualizaron en la figura 38.

Otra forma de eliminar acciones de la guerra de la información es la construcción de disipadores orientados de frecuencias, que eliminan tanto los pulsos electromagnéticos como las radiofrecuencias de alta energía, para ello solo es necesario trabajar con convertidores bien sea resonantes, asistidos por RED o con semiconductores con capacidad de bloqueo y fuente inversa de tensión o de corriente; elementalmente con el integrado 741[86], una resistencia y dos trasmisores el BD135 y BD136, un condensador y un parlante se puede implementar una muestra de análisis para ajustes de frecuencia.

Matemáticamente, el uso de la función de verosimilitud como probabilidad de observar la que realmente se observó, permitir valorar la operación de estos escudos a nivel hardware, su comportamiento se define de esta forma (Obregón 2004)

$$L(a,x) = Fx(x1,a)(x2,a) \dots . Fn(Xn,a)$$

$$Fx(Xi,a,o) = \frac{1}{o\sqrt{2\pi}}\, e - \frac{1}{2o^2}\,(Xi-a)^2$$

$$L(a,o,x) = \pi\,\frac{1}{o\sqrt{2\pi}}\, e - \frac{1}{2o^2}\,(Xi-a)^2$$

$$L(a,o,x) = \frac{1}{o^n(2\pi)^{\frac{n}{2}}}\, e - \frac{1}{2o^2}\sum_{i=1}^{n}(X2-a)^2$$

$$Fx(Xi,b) = \begin{cases} \frac{1}{b}\; o \le Xi \le b \\ 0\; de\; otra\; forma \end{cases}$$

Esta función valida operacionalmente, que en el cómo de un ataque el escudo implementado función perfectamente, obviamente es to se verifica cuando se ha violado el control del cortafuego de red, de estado o de aplicación.

[86] Amplificador operacional.
http://www.ladelec.com/teoria/informacion-tecnica/330-lm-741

3.3.3.2 SECTORIZACIÓN OPERACIONAL

El procedimiento de distribución funcional de la arquitectura del modelo MCCPC, solo se podrá realizar después del análisis mediante simulación de la carga operativa por cada servidor y con ayuda de la teoría de colas estándar los parámetros de análisis asociados con la longitud, tiempos de espera, índice de desocupación del servidor, como también al análisis del flujo transaccional o enrutamiento mediante el algoritmo de Dijkstra.

Por ejemplo para el análisis de tiempo de esperar, se puede considerar la llegada según reloj y el tiempo de servicio, analizado los resultados generados en la tabla 5, para un tiempo de servicio de 0.4 unidades.

Tabla 5: Ejemplo de análisis de tiempos

Archivo	Reloj	Servicio	Ingreso	Salida	Empresa
0.642	0.642	0.4	0.642	1.042	0
0.265	0.967	0.4	1.042	1.442	0.075
0.0.58	1.025	0.4	1.442	1.842	0.417
0.748	1.773	0.4	1.842	2.242	0.069
0.207	1.982	0.4	2.242	2.642	0.260

Fuente aporte realizadores

Con los datos de esta tabla, se construye la tabla 6 que señala longitudes de cola y tiempo de proceso, para entonces evaluar las disponibilidades de enlace

Tabla 6: Análisis de disponibilidad

Intervalo	Longitud de	L=	L=1	L=2	L>2
0=642	0	0.642			
0.642-.0969	1		0.325		
0.969-1.025	2			0.058	
1.025-1.042	3				0.400
1.042-1.442	2			0.400	
1.442-1.773	1		0.331		
1.773- 1.842	2			0.069	
1.842-1.982	1		0.140		
1.982-2.242	2			0.026	
2.242-2.642	1		0.400		

Fuente Aporte realizadores

Se valida con esta información que:

- El servidor estuvo vacío o inactivo durante 0.642 unidades de tiempo.
- Atendió una transacción o cliente durante 1.196 unidades
- El tiempo de atención para el trabajo con dos transacciones fue de 0.787 unidades
- Solamente durante 0.400 unidades el servidor atendió a 3 transacciones para el análisis de flujo de tráfico, solo se requiere emplear estas ecuaciones:

$$\rho = \frac{x}{\mu}$$

$$\rho 0(t) = 1 - \frac{x}{\mu}\ L = \frac{x}{\mu(\mu - x)}$$

$$p(t > k) = (\frac{x}{\mu})e^{-(1-\frac{x}{\mu})k}$$

La estimación de carga operacional, se realiza mediante la distribución triangular al ponderar índice histórico de fallas (límite inferior y límite superior), en la figura 37, se presenta el tratamiento matemático formal, que acepta valores aleatorios que se mapean en dos valores aleatorios que se mapean en dos intervalos

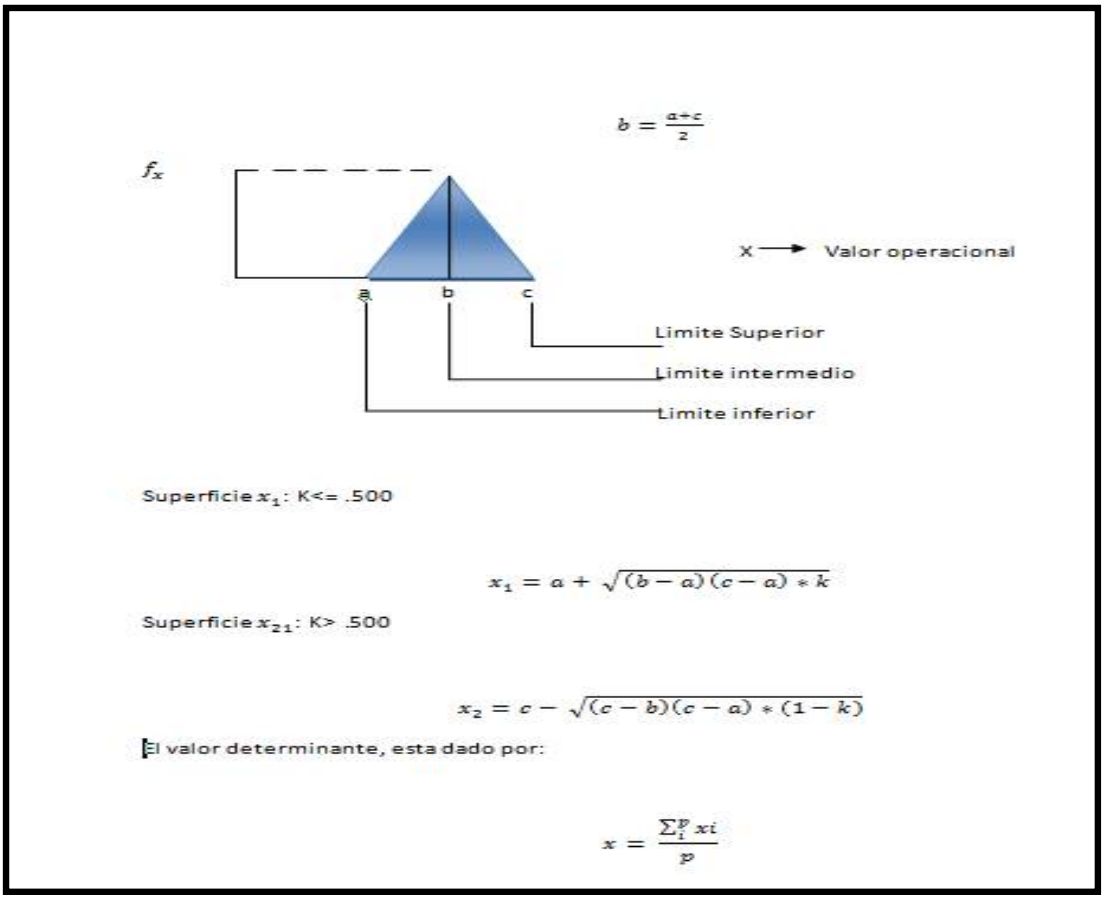
$$x1\ para\ k\ \leq 0.500\ y\ X2\ para\ k > 0.500, en\ donde$$

$$x_1 = a + \sqrt{(b-a)(c-a) * k}$$

$$x_2 = c - \sqrt{(c-b)(c-a) * (1-k)}$$

$$k\ es\ un\ valor\ aleatorio$$

Figura 37: distribución triangular



Fuente aportes realizadores

Con base a este análisis, se puede entonces elaborar la distribución o segmentación operacional que se señaló en la figura 37

Descriptivamente el MCCPC, está configurado por

- Unidades de control y gestión
- Escenarios de enlace y supervisión
    - Servidores de registro
    - Servidores de verificación
    - Servidores de seguimiento
    - Servidores de bloqueo

- Escenario de distribución

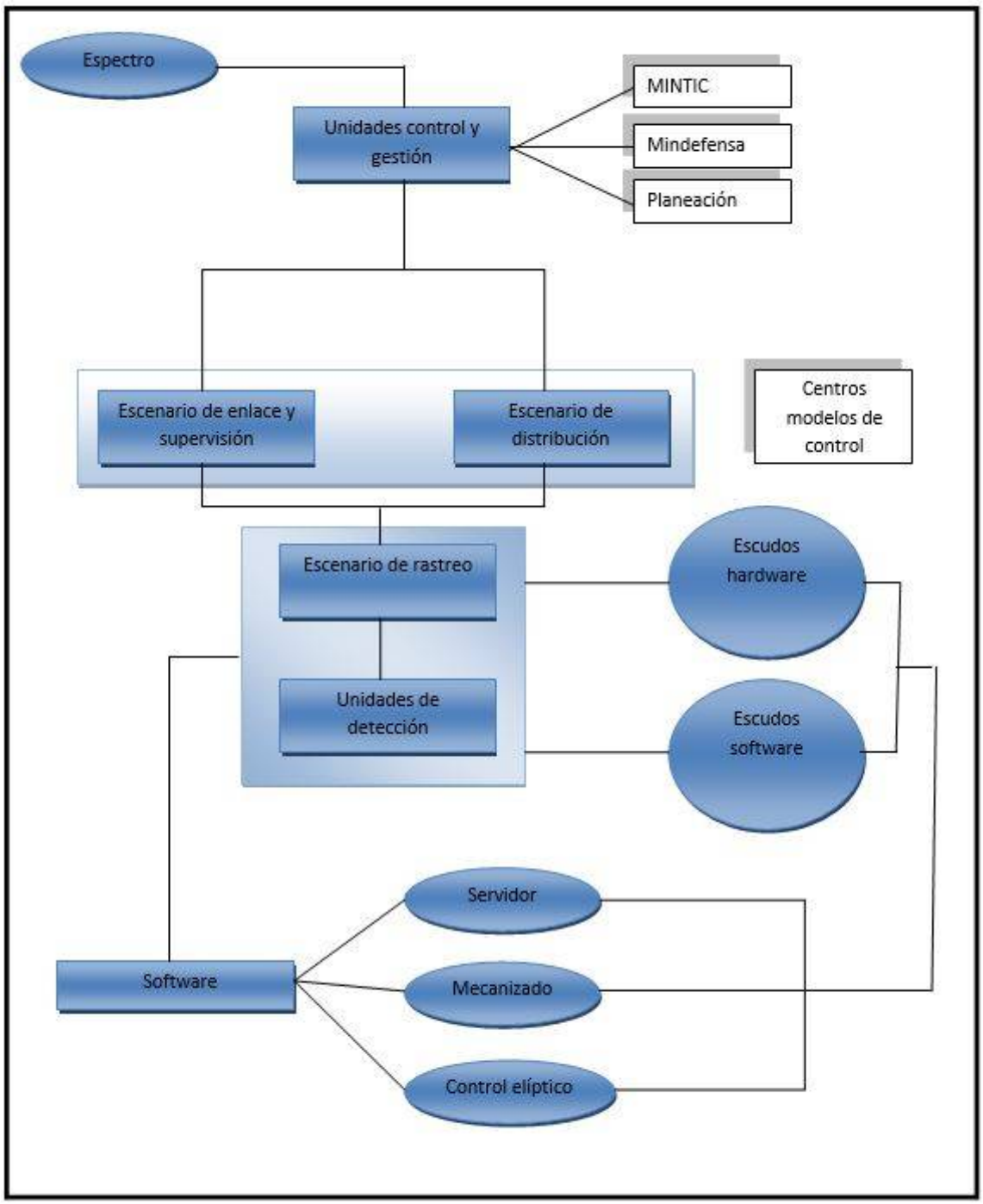
  Servidores de rastreo de correo
    - Servidores de control IP
    - Servidores de control web

- Escenarios de rastreo
    - Rastreo local
    - Rastreo remoto
    - Rastreo cinturón o escudo
    - Exploración de seguimiento

- Unidades de detección
    - Captura de alertas
    - Capturas de ataque
    - Bloqueo transaccional
    - Bloqueo y congelación de unidades remotas

El marco descriptivo del MCCP, se presenta en la figura 38

Figura 38: marco descriptivo operacional MCCPC



Fuente aporte realizadores

4. CONCLUSIONES

- El programa de ingeniería de sistemas de la universidad libre gracias a la dirección de la línea de formación electiva en seguridad informática, proyecta su función como constructor de soluciones esquematizando descriptivamente un modelo de ínter nacional para Ciberseguridad y defensa

- El MCCPC, establece los valoradores de acción logística, como resultado de la interpretación analítica de los ejes de referenciación organizacional para controlar y formular procedimientos para la Ciberseguridad y para la Ciberdefensa, fundamentados en la significancia de la administración moderna (P=planeación, O=organización, D=dirección, E=ejecución, R=revisión o control), significando que para implementar el modelo convencionalmente, el programa debe acercarse como consultor al MINTIC y MINDEFENSA

- 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 destructivos de los piratas de la información

5. RECOMENDACIONES

- El programa de ingeniería de sistemas de la universidad libre deberá evaluar objetivamente los resultados de este trabajo para mediante un grupo especializado proceder a su complementación, permitiendo que de esta manera se pueda establecer un contacto a nivel de consultoría con los Ministerios responsable de la seguridad de nuestro ciberespacio.

- Se hace necesario la definición de proyectos semejantes al realizado para establecer esquemas de mejoramiento cuya significancia e importancia garanticen el intercambio de los logros obtenidos con la comunidad académica nacional.

6. REFERENCIAS BIBLIOGRÁFICAS

❖ TEXTOS Y PUBLICACIONES

- Cano Jeimy: Informática Forense segunda Edición. Editorial Alfa Omega 2015
- Consejo Nacional de Planeación y MINTIC: Documento CONPES 3701. 2012.
- García-Moran J y Otros. Hacking Ético y Seguridad Informática. Editorial Alfa Omega 2007.
- Grech Pablo: Introducción a la Ingeniería: Un enfoque Práctico. Editorial Pearson 2013
- Halsall Paul. Internet History Sourcebooks Project. Fordham University New York 2001.
- López Humberto. Administración de seguridad con estrategias de Ciberdefensa. Conferencia Ciclo de Seguridad. Fuac 2006.
- Obregón Sanín Ivan. Teoría de Probabilidades. Editorial Limusa 2002
- Prawda Juan. Investigación de Operaciones vol 1. Editorial Limusa 2008.
- Ramirez Napoleon. Teoría de modelos: Enfoque Práctico. Revista Criterio No 30 Fuac 2008
- Rheault J. Toma de Decisiones en administración. Editorial Limusa 2002.
- Shannon W. Teoría de canales y comunicacion. Editorial Addison Wesley 1996
- Stafford Beer. Modelo de Sistema Viable: Cibernetica organizational. Editorial Addison Wesley 2008.
- Stallings William. Seguridad digital. Editorial Pearson 2012
- Tanebaum Andrew. Sistemas distribuidos. Editorial Prentice Hall 2013
- Tomassi Wayne. Sistemas de comunicaciones electrónicos. Editorial Prentice Hall 2012.

❖ CIBERGRAFIA

- http://www.aprendizaje.com.mx/TeoriaSistemas/Cibernetica/cibernetica.html
- http://www.acis.org.co/fileadmin/Revista_119/Editorial.pdf
  http://www.ucr.ac.cr/noticias/2012/08/21/expertos-creen-que-ley-de-delitos-informaticos.html
- http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980
- http://library.thinkquest.org/05aug/00533/lowres_content_spanish/lowspan_content_types4.htm
- http://www.fotosdigitalesgratis.com/buscarfoto/malicioso
- http://cxo-community.com/articulos/blogs/blogs-seguridad-publica/5271-cibercrimen-y-ciberterrorismo-dos-amenazas-emergentes.html
- http://www.acis.org.co/fileadmin/Revista_119/Editorial.pdf
- http://m.vanguardia.com/actualidad/tecnologia/188838-fiscalia-advierte-aumento-de-delitos-informaticos-en-colombia
- http://www.latarde.com/noticias/judicial/107607-delitos-informaticos-hecha-la-ley-hecha-la-trampa
- http://www.slideshare.net/Derechotics/herramientas-legales-para-la-prevencin-de-los-delitos-11665581
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- http://www.delitosinformaticos.info/delitos_informaticos/definicion.html
- http://www.ehowenespanol.com/personas-cometen-delitos-informaticos-sobre_96220/