Modelo de sistema integrado de información para la automatización del ciclo de inteligencia en cumplimiento de la ley 1621 de 2013

Eduardo de la Torre Díaz

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2019

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO"

MODELO DE SISTEMA INTEGRADO DE INFORMACIÓN PARA LA AUTOMATIZACIÓN DEL CICLO DE INTELIGENCIA EN CUMPLIMIENTO DE LA LEY 1621 DE 2013

MAYOR EDUARDO DE LA TORRE DÍAZ

Director

MSC. HÉCTOR FERNANDO VARGAS MONTOYA

MAESTRIA EN CIBERSEGURIDADY CIBERDEFENSA
TRABAJO DE GRADO PARA OPTAR TITULO DE MAGISTER

BOGOTÁ
2019

Dedicatoria.

El fruto del esfuerzo de esta investigación no hubiese sido posible sin el apoyo de todas las personas que a lo largo de este trasegar hicieron posible la culminación de este proyecto; unas pocas líneas y unas cuantas palabras no son insuficientes para agradecer todo lo que día a día hacen por mi; a mi Gaby princesa quien es mi motor de vida y quien me motiva a dar lo mejor de mi en cada proyecto que emprendo; hija mía tu eres mi horizonte, mi norte, mi luz, y mas que eso eres la bendición que Dios me dio; a mi amada madre a quien admiro y respeto con todo mi corazón, por ser para mi un ejemplo de fortaleza, esfuerzo y dedicación, gracias por tu comprensión, apoyo y sobre todo gracias infinitas por la paciencia que me ha tenido, unas líneas no son suficientes para agradecerte las incontables veces que me brindas tu sabio consejo en las decisiones que he tomado a lo largo de mi vida.

A mis hermanos por llenarme de alegría día tras día, por todos los consejos brindados, por su compañía y porque a pesar de las circunstancias siempre están ahí para mí cuando más los necesito.

Y sobre todo a ti Pao, amor mío por tus consejos, apoyo incondicional, por motivarme a ir cada día más alto, por tus noches en vela ayudándome a cumplir este sueño, sin ti esto no sería posible, mi compañera de viaje de aventura de estudio de trabajo de diversión y de vida.

Agradecimientos

En primer lugar, deseo expresar mi más sentido agradecimiento al director de esta tesis, MSc. Héctor Fernando Vargas Montoya, por la dedicación, apoyo y paciencia brindada durante este proceso y por el cual puede concluir este trabajo, por el respeto a mis sugerencias e ideas, por la dirección y por sus invaluables aportes desde el inicio y el rigor que ha facilitado a las mismas, gracias por la confianza que deposito en mi desde el primer día que iniciamos con este objetivo.

Asimismo, agradezco a mis compañeros de la maestría por su apoyo personal y humano y sobre todo por su acompañamiento a lo largo de mis estudios.

Pero un trabajo de investigación es también fruto del reconocimiento y del apoyo vital que nos ofrecen las personas que nos estiman, sin el cual no tendríamos la fuerza y energía que nos anima a crecer como personas y como profesionales.

Gracias a mi familia, a mi madre quien es mi fuente de inspiración y a mis hermanos, con quienes comparto las grandes decisiones de mi vida y quienes están hay siempre para darme su apoyo y consejo oportuno.

Gracias a mis compañeros de trabajo en mi glorioso Ejercito Nacional, que siempre me han prestado un gran apoyo moral y humano, necesarios en los momentos difíciles de este trabajo y esta profesión.

Pero, sobre todo, gracias a mis hermosas mujeres Pao y Gaby, por su paciencia, comprensión y solidaridad con este proyecto, por el tiempo que me han concedido, un tiempo robado a la historia familiar. Sin su apoyo este trabajo nunca se habría escrito y, por eso, este trabajo es también el suyo.

A todos, muchas gracias.

Resumen

En este estudio se determina un prototipo de cómo se puede llegar a implementar un sistema integrado de información, contemplando todos los aspectos que se deben tener en cuenta tanto a nivel de hardware, software y recurso humano, lo anterior haciendo énfasis en lo que concierne al engranaje del proceso de información desde el punto de vista de inteligencia militar, en lo cual reviste gran importancia "la seguridad de la información", que aun siendo transversal a todos los procesos, se debe hacer hincapié en los nodos físicos y lógicos más sensibles para mitigar fuga o incidente que afecte los tres pilares de la seguridad (integridad, confidencialidad y disponibilidad) y en especial, no se vea vulnerada la información militar que pueda estar en un sistema de información.

Del estudio realizado se observa como al no tener un sistema de integración de información adecuado se pierden oportunidades importantes para realizar apreciaciones adecuadas, así como realizar proyecciones o anticiparnos a las actividades que realiza el adversario. El tema es aún más relevante cuando se habla de información concerniente a activos estratégicos de la nación, toda vez que una fuga de información da ventajas al adversario en la toma de decisiones.

En este trabajo final se hace un acercamiento al estado del arte y marco teórico, seguidamente se tienen 3 capítulos, el primero es la identificación del problema, oportunidades, objetivos y determinación de los requerimientos de información, el segundo son los requerimientos tecnológicos para el diseño del sistema y el tercero despliega una propuesta de cómo se puede implementar el modelo de seguridad y cómo se podría hacer su verificación (plan de auditoria). Finalmente se entregan las conclusiones y el trabajo futuro.

Palabras claves: Información, Integración, Integridad, confidencialidad, disponibilidad, sinergia entre fuentes de información, inteligencia militar, ataque, ciberseguridad, ciberdefensa.

Abstract

During the development of intelligence operations, it is necessary to collect large volumes of information; what hinders the work carried out by the analysis sections where, on many occasions, intelligence information is left out, relevant information, because it can not be processed due to the large volume of it.

The objective of this study is to design an integrated intelligence information system, which allows the management of military intelligence information of the Army, by integrating existing technologies that allow the information to be available in a secure, complete, reliable and timely complying with the law; To this end, the research question is as follows: How to design an integrated information system that integrates existing capacities and complies with the provisions of the intelligence law? In this context, the design of the system is developed to the extent that the information collection sensors are more technician and collect more valuable information in less time.

The research question is answered through the development of tasks that allow the structuring of an efficient, dynamic and safe system that allows an optimal management of the information; based on the three pillars of security, such as integrity, confidentiality and availability; Bearing in mind this, it is necessary for military intelligence to centralize their information for a more efficient and effective management.

Key Words: system, integrated, Information, intelligence, management, confidentiality, availability, integrity, analysis, sensors.

Tabla de contenido

Introducción

Los atentados del 11 de Septiembre de 2001 se constituyeron en el momento de cambio para los servicios de inteligencia en el mundo; esto debido a que se pudo establecer que la información sobre los atentados ya estaba advertida; pero se encontraba diseminada en diferentes informes de fuentes diversas, lo que no permitió su integración y proceso de una manera adecuada, consistente y rápida; razón por la cual no se tomaron medidas efectivas para evitar la tragedia; lo que planteo un cambio estructural en la manera como se recolecta y se procesa la información hoy en día.

Lo anterior debido a que Al Qaeda desarrollaba sus actividades en Internet y este grupo supo interpretar muy bien las posibilidades y necesidades: una organización en red y "en la red"; y desde este punto de vista comenzaron a ganar la batalla, dado que las organizaciones encargadas de ofrecer seguridad no estaban organizadas en red, no disponían de sistemas de trabajo colaborativos, no se propiciaba una gestión del conocimiento colectivo entre servicios de inteligencia y fuerzas de seguridad (Blanco, 2011).

En la era de la información el flujo de datos que reciben los cuerpos de inteligencia sobrepasa la capacidad de procesamiento de los mismos; para lo cual es necesario adoptar soluciones concretas capaces de controlar y convertir en conocimiento útil los grandes volúmenes de información que se deben procesar; de manera que permitan la gestión del conocimiento, para permitir que los servicios de inteligencia se transformen en organizaciones confiables, eficientes y eficaces, dicho en otras palabras "una fuerza basada en el conocimiento, rápidamente desplegable y globalmente enfocada" (Masback, 2002).

Si logramos comprender el hecho que la información obtenida por diversas fuentes es el elemento con el que se trabaja, descubrimos que estamos ante lo que se denomina en la actualidad un proceso de gestión del conocimiento; tarea complicada de desarrollar si tenemos en cuenta que los servicios de inteligencia se mueven en los paralelos de la información secreta y reservada, dificultando la necesaria integración de conocimientos y habilidades necesarios en los procesos de adquisición, selección, tratamiento, difusión y uso de la información.

La era digital convive con múltiples desafíos tales como lograr identificar fuentes de información fiables, procesos autónomos que de manera eficiente entreguen resultados, información local o en tránsito que debe ser protegida, datos en tiempo real que permita la toma de decisiones, entre otros. Esto genera una serie de retos desde las ciencias computacionales y la ciberseguridad, en consideración que la información militar y estratégica es clave para la seguridad nacional, por lo que su protección es un elemento clave, así como la relevancia e importancia de los datos y reportes arrojados luego de su procesamiento.

Dado lo anterior, es necesario diseñar un sistema integrado de información de Inteligencia, que permita la gestión de la información de Inteligencia militar del Ejército, mediante la integración de tecnologías existentes que permitan disponer de la información de manera segura, completa, confiable y oportuna cumpliendo con la ley 1621 de 2013.

Este documento se organiza iniciando con la descripción de los objetivos planteados en el proyecto, un marco teórico, seguidamente se desarrollas 3 capítulos, el primero sobre las necesidades y alcance del sistema integrado, el segundo sobre los requerimientos en el protocolo de seguridad y el tercero implementación y evaluación del sistema, finalmente se entregan las conclusiones y recomendaciones.

Descripción del problema

Las tecnologías de información y comunicaciones – TIC hace posible la recolección y procesamiento de grandes volúmenes de información en corto tiempo, las fuentes de información cada vez se expanden más y puede tornarse difícil la concentración y procesamiento de éste volumen en los procesos de inteligencia, por lo que es necesario establecer una organización o modelo que permita concentrar esfuerzos cuando la misma información debe tener un alto nivel de seguridad y protección, dado que dicha información es recolectada, almacenada, producida y difundida a nivel nacional; en consecuencia, se crea la necesidad de establecer mecanismos para la gestión de conocimiento sobre la misma información, que le permita de forma estratégica, disminuir la incertidumbre para la toma de decisiones y la respuesta eficiente, eficaz y efectiva a los requerimientos actuales de información.

Existe una necesidad por parte del sistema de inteligencia militar del Ejército Nacional de Colombia de proteger la información local y/o en tránsito contra posibles riesgos de ciberseguridad, específicamente en la sistematización de los procesos del ciclo de inteligencia, el cual tiene como fin controlar, verificar, evaluar y difundir en todos los niveles de la estrategia nacional de manera confiable, clara y oportuna por lo cual, las diferentes funciones de conducción de la guerra deben una difusión oportuna y transversal de información por intermedio de un sistema integrado de información, el cual lograría integrar todos los datos obtenidos por intermedio de las fuentes que lo alimentan y búsqueda información, además de realizar evaluaciones pertinentes y acertadas en cuanto a la calidad y veracidad, esto permite realizar consultas de datos de manera transversal en todo el sistema de inteligencia militar del Ejército Nacional; la mala o deficiente comunicación entre las funciones de conducción de la guerra o el ingreso de información errada, remanente o baja en integridad, los intereses estratégicos de las FFMM, la falta de entendimiento del nivel de conducción y dirección de sistemas de seguridad y gestión de datos, además de la falta de una directriz fija y constante institucional que se ajuste a los nuevos escenarios, crea fisuras y retardos en la toma de decisiones.

Del mismo modo, se observan distorsiones doctrinales, elevados índices de incomprensión de las técnicas, tácticas y procedimientos en el nuevo concepto único que oriente el desempeño de la fuerza y la desactualizada doctrina no incluyente de los nuevos procesos. Sin embargo, el

comando de educación y doctrina junto con sus escuelas de educación militar consideran que los métodos, desarrollados por el plan DAMASCO[1], son acordes a la idiosincrasia del entorno.

Los niveles de motivación para revisar y crear una nueva doctrina que actualice y transforme el concepto operacional en un solo enfoque, impactan de manera favorable en la comunicación y convocatoria de todas las funciones de la guerra. La deficiencia a la hora de la difusión de los planes y directrices de Damasco afecta el entendimiento de los instructores a la hora de hacer la ejecución de la instrucción y por supuesto, a la interacción de nuevos sistemas electrónicos de alta tecnología militar; retrasando un poco la actualización tecnológica y doctrina del ejército del futuro.

Entonces ¿Hasta qué punto sus métodos para crear doctrina y estandarización responden a la naturaleza de la institución y el nivel educativo militar de los niveles operacionales y estratégicos de la institución? Su manera de actuar puede ser la que está ocasionando la desmotivación, entendida su manera de actuar tanto como la difusión de la nueva doctrina, como sus gestiones y canalización de las problemáticas con el cliente final, la nación y los nuevos escenarios de guerra, como lo son las fronteras nacionales.

Formulación:

En el contexto de la búsqueda de información existe una falencia entorno al manejo de grandes volúmenes de información generados por todas las fuentes y medios de búsqueda, estos tienden a desbordar la capacidad de análisis y gestión de la información, lo cual hace que sea menos eficaz y eficiente el uso de esta, así mismo, la protección de la información es fundamental toda vez que se requiere un modelo de seguridad que permita la integridad, disponibilidad y confidencialidad de esta.

---

[1] El plan DAMASCO es la "la doctrina que amalgama los principios fundamentales de las Fuerzas Militares que guiarán sus acciones en apoyo de los objetivos nacionales". Tomado de https://cedoe.mil.co/index.php?idcategoria=141

Objetivo general

Diseñar un sistema integrado de información de Inteligencia, que permita la gestión de la información de Inteligencia militar del Ejército, mediante la integración de las tecnologías existentes que permitan disponer de la información de manera segura, completa, confiable y oportuna cumpliendo con la ley 1621 de 2013.

Objetivos específicos

1. Identificar del problema, oportunidades, objetivos y determinación de los requerimientos de información.
2. Establecer los requerimientos tecnológicos para el desarrollo del sistema.
3. Definir el protocolo de implementación, seguimiento y evaluación del sistema.

Metodología

Enfoque. Cualitativo, La metodología cualitativa es aquella que permite examinar los datos de manera numérica, especialmente en el campo de la estadística. El desarrollo del proyecto de Grado "Modelo de sistema integrado de información para la automatización del ciclo de inteligencia" tiene un enfoque cualitativo debido a que emplea un análisis causa-efecto y va a tener un proceso probatorio el cual nos servirá para demostrar la problemática que conlleva el no actualizar los equipos que se tienen. El proyecto va a garantizar mayor precisión y mayores resultados en general.

Diseño. transversales correlacionales, se encargan de describir relaciones entre dos o más variables en un momento determinado, En el caso de nuestro proyecto utilizaremos la modalidad no experimental puesto que resaltaremos la funcionalidad de un modelo de sistema integrado de información para la automatización del ciclo de inteligencia con respecto a la información.

Marco teórico y estado del arte

La información es el recurso más importante que tienen los estados y las personas para el proceso de toma de decisiones efectiva aplicadas a la protección contra amenazas internas o externas; mediante el proceso y análisis de datos se produce la inteligencia necesaria para la defensa.

La definición de inteligencia universalmente puede tomarse desde varios puntos de vista, a pesar de que se han ensayado numerosas definiciones (Warner, 2002), la inteligencia compete a varias líneas de trabajo que deben estar enfocadas en la acción, medios y recursos que logren establecer una posición inicial y final con respecto a los acontecimientos que puedan suceder en el campo militar (Navarro, 2015); se destaca la delimitación de inteligencia como conocimiento del enemigo presidido por el secreto, para cuya creación se nutre de las informaciones obtenidas por agentes de información, por medios técnicos o de fuentes y recursos de información abiertos (Thomas, 1992); datos que sumados analizados y correlacionados con hechos permiten acceder a una apreciación más adecuada de una situación determinada o amenaza.

De acuerdo con lo anterior un servicio de inteligencia efectivo debe fundamentar su razón de ser en un eficaz sistema de información, aplicando los procedimientos e instrumentos para la gestión de datos con el fin de suministrar al Estado conocimiento para la comprensión de su ambiente operacional y estratégico de manera que le permita ajustar su estrategia, adoptar medidas para la defensa nacional; con esto cumple su objetivo que es generar información evaluada para los organismos de decisión política que contribuya a despejar el escenario de incertidumbre interno y externo donde actúe el estado (Fraguas, 1991).

La diversidad y el carácter no convencional de las nuevas amenazas del siglo XXI a la seguridad nacional como lo son el ciberterrorismo, terrorismo, redes transnacionales del crimen organizado, entre otros. Particularmente el ciberterrorismo ha tomado en los últimos años un vuelco importante en los diferentes ámbitos, toda vez que el uso de las TIC viene constituyendo herramientas cada vez letales a la hora de robar información o dejar por fuera un servicio informático o de telecomunicaciones (Nieto, 2018), los grupos u organizaciones que delinquen de

manera asimétrica e irregular, utilizan los medios tecnológicos para su accionar, frente al tradicional enfrentamiento de ejércitos nacionales con grandes efectivos humanos y materiales que se despliegan sobre el territorio, refuerzan aún más la necesidad de disponer de información y conocimiento de muy diversa procedencia y naturaleza por parte de las fuerzas armadas y los cuerpos de seguridad del estado; donde la información toma un carácter estratégico de primera magnitud, bien como medio activo de defensa: conocer para prevenir, o reactivo: conocer para atacar (Kahn, 2001).

En Colombia la función de inteligencia y contrainteligencia es aquella que desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas (Senado, 2013); para lo cual la misma ley exige a los organismos de Inteligencia (entre los cuales está la inteligencia militar), la implementación de los centros de protección de datos y archivos.

Según la asociación bancaria y de entidades financieras de Colombia en el año 2016 (Asobancaria, 2016) "m*ás de 169 millones de registros personales fueron expuestos en 2015 como producto de las 781 infracciones publicitadas por los sectores financieros, de negocios, educación, gobierno y salud"* lo que plantea la necesidad más clara y fuerte del gobierno Colombiano de posicionar diferentes mecanismos para la ciberdefensa y la ciberseguridad, que ayuda a todos los gremios a fortalecer su propia estrategia.

Antecedentes

Mediante resolución No. 612 del 19 de febrero de 1985, expedida por el Ministerio de Defensa Nacional, se creó la Dirección de Inteligencia del Ejército, Comando Operativo de Inteligencia y Contrainteligencia y Batallón Escuela de Inteligencia y Contrainteligencia BG. CHARRY SOLANO, desde esa fecha y hasta el momento la inteligencia ha generado 5 cambios a lo largo de este tiempo, pasando de comando operativo a Brigada, de Brigada a Central de Inteligencia y en la actualidad a comandos de Apoyo de combate, situación que ha generado que

la información de inteligencia se vaya trasladando de un lugar a otro, al punto que dentro una misma especialidad hay infraestructuras informáticas diferentes en una misma organización.

Los hechos anteriores generaron que en la actualidad, el flujo de información de inteligencia este disperso y la integración de la información no pueda hacerse en tiempo real, perdiendo la posibilidad de explotar el principio de oportunidad; hecho que ha llevado a la especialidad a explorar diferentes herramientas para la integración de información, encontrando en el mercado programas que permiten hacer procesos de integración semiautomáticos pero no se adaptan a las necesidades del sistema de Inteligencia.

Como elemento de referencia, en Colombia varias organizaciones y agencias han desarrollado sistemas más automáticos y de integración de información, tal es el caso de la agencias como la Unidad de Información y análisis financiero – UIAF han desarrollado sistemas de gestión de la información que les ha permitido por medio de algoritmos enlazar las diferentes bases de datos con que cuenta el sector financiero y así poder generar líneas de acción para el cumplimiento de la misión de mencionada entidad, así mismo está el sistema integrado de información SISPRO del Ministerio de Salud que pretende consolidar toda la información necesaria para la toma de decisiones.

Con la promulgación de la ley 1621 de 2013 "*Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de Inteligencia y Contrainteligencia cumplir con su misión constitucional y legal*", le exige a los organismos de Inteligencia (entre los cuales está la inteligencia militar), la implementación de los centros de protección de datos y archivos, con el fin de garantizar los procesos de recolección, almacenamiento y difusión de información, así como la actualización, corrección y retiro de datos y archivos de inteligencia, actividad que es imposible cumplir a cabalidad, sin el empleo de tecnología orientada a la automatización del ciclo.

Adicionalmente se cuenta con lo recomendado en el Consejo Nacional de Política Económica y Social, CONPES 3854 del 11 de abril de 2016 el cual tiene como objetivo general fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital,

en un marco de cooperación, colaboración y asistencia; política en el cual se ordena mejorar las capacidades de inteligencia a través de la gestión del riesgo digital dado el incremento del uso de la tecnología de información y comunicaciones TIC para desarrollar diferentes actividades tanto económicas como sociales.

Según la asociación Colombiana de Ingenieros de Sistemas (ACIS, 2017), existen una serie de obstáculos para lograr la seguridad de la información en el año 2017, entre los cuales se destaca que el 59.1% es por ausencia o falta de una cultura de seguridad o sensibilización frente a la protección de la información y un 42.6% es por falta de colaboración entre áreas dentro de una misma organización, lo que conlleva a pensar que hay una falencia importante relacionado con lo humano, que hace la integración de información se vuelva cada vez más difícil. Para las fuerzas militares no es ajeno que la información está segmentada en varios sistemas de información, lo que ha generado retardos en la toma de decisiones al no contar con información requerida en el momento oportuno.

Generalidades

Marco jurídico

El marco que encierra las actividades de ciberdefensa y ciberseguridad en nuestro país demuestran que cumplen las normas legales y reglamentarias dispuestas para el cumplimiento de los fines y límites a las actividades de inteligencia y contrainteligencia; sin embargo, cabe resaltar que respecto al capítulo "empleo de la producción de Inteligencia", nuevamente se incurre en el yerro jurídico de mezclar o confundir de cierta manera, a las actividades de inteligencia y C/I, con actividades de investigación judicial.

En el numeral 49, ítem No. 3 se les da valor judicial a los informes de inteligencia aportados a la Fiscalía General de la Nación. Aspecto que quebranta la esencia misma de la función de inteligencia, pues mientras las primeras, tienen una función meramente preventiva y anticipativa, las segundas tienen un contenido reactivo y punitivo, tal como lo anunció la Corte Constitucional

en sentencia C-540 de 2012, "*la investigación penal pretende recaudar pruebas y establecer los responsables de una conducta delictual que se desenvolverá en el marco de un proceso penal*", mientras que en relación con la actividad de inteligencia precisó que "las actividades de inteligencia se desenvuelven en el marco del procesamiento, análisis y circulación de información soportadas en un conjunto de datos y operaciones subjetivas que suelen tener un amplio margen de duda sobre mucha de la información, al trabajar sobre conjeturas o hipótesis de investigación que no resultan suficientemente probadas y comprometen derechos fundamentales como la intimidad y el habeas data".

Normas jurídicas empleadas para el desarrollo del proyecto

Ley 489 de 2005
Ley 1070 de 2006
Ley 1150 de 2007
Ley 1219 de 2008
Ley 1621 de 2013
Ley 1712 de 201
Ley 1476 de 2011
Decreto 1070 de 2015
CONPES 3701 de 2011
CONPES 3854 de 2016
NTCGP 1000:2009
Norma ISO 27001 Gestión de la seguridad de la información
Norma ISO 27002: El dominio político de seguridad
Decretos, Resoluciones y Directivas tanto del Ministerio de Defensa como del Ejercito Nacional.

Metodología en la ejecución del proyecto

Para obtener los resultados, se estableció un flujo de trabajo (figura 1) que permitió la estructuración y obtención de los resultados.

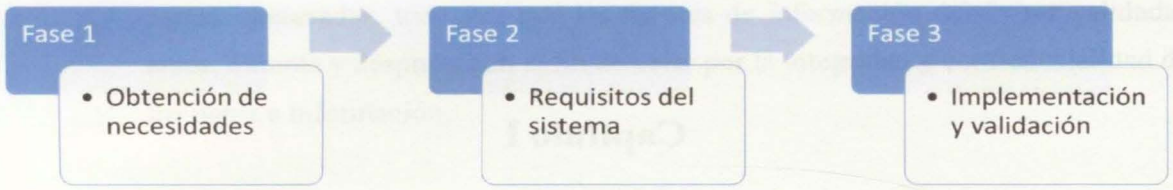


Figura 1: Fases para le ejecución de la metodología. Fuente: elaboración propia, agosto 2017

Para la fase 1, las diferentes necesidades del sistema integrado de información se recolectan a través del conocimiento mismo de los procesos de las fuerzas militares, así como la consulta a varias personas y mandos dentro de la organización, con ello, se consolida las necesidades más relevantes que le permitan al sistema establecer las mejoras en los procesos y en la seguridad.

Para la fase 2, los requerimientos del sistema parten de la necesidad misma en la implementación, y se hace una selección de posibles controles de seguridad con base en la norma internacional ISO/IEC 27001:2013 y para ello, se hace una selección de controles relevantes que ayudan a la reducción de riesgos del sistema integrado de información de inteligencia, así mismo, se establecen algunos protocolos de seguridad para el resguardo y entrega de información.

En la etapa final de implementación y validación de las medidas propuestas, se revisa la literatura sobre procesos y procedimientos de auditoria e implementación de soluciones de seguridad, y se genera una propuesta de cómo se debería implementar todo el proceso de validación del sistema.

En el siguiente capítulo se describen los resultados (propuestas a implementar) del flujo de trabajo.

Resultados

Para cada una de las fases de la metodología (figura 1), se tiene un capítulo en dónde se describe los resultados.

Capítulo I

Identificación de necesidades y alcance del sistema integrado de información de inteligencia

Alcance

Para controlar con un alto nivel de seguridad el volumen de información que es recolectada, almacenada, producida y difundida a nivel nacional; así mismo, como para generar la capacidad de gestión de conocimiento, que permita de forma estratégica, disminuir la incertidumbre para la toma de decisiones y la respuesta eficiente, eficaz y efectiva a los requerimientos actuales de información, es necesario que para el diseño del sistema se consideren los siguientes lineamientos:

- Proteger la información en un 95% del Subsistema de Inteligencia y Contrainteligencia ante eventos que vulneren la integridad, disponibilidad y confidencialidad en cumplimiento a los lineamientos de la ley 1621 del 2013.

- Centralizar en un 90% la información digital del subsistema de inteligencia con el fin de explotar la capacidad de análisis de grandes volúmenes de información, a través de herramientas tecnológicas de punta y procesos de investigación.

- ❖ Agilizar la generación de productos de inteligencia disminuyendo a un 50% el tiempo en el planeamiento del esfuerzo de búsqueda de información, análisis y difusión de datos e información de inteligencia.
- ❖ Establecer las necesidades de consulta, uso y transferencia de información por las partes interesadas, toda vez que las fuentes de información deben ser validadas antes, durante y después, con el fin de velar por la integridad y confidencialidad de los datos e información.
- ❖ Cada nueva fuente debe ser verificada y debe cumplir con el procedimiento para la entrega de la información, así mismo, las fuentes que ya no requieran acceso deben ser identificadas y retiradas.

Alcances conceptuales

El concepto de sistema integrado de información de inteligencia; hace referencia a un administrador de información que gestiona procesos de captura, acopio, estandarización, almacenamiento y reportes, los cuales presenta de una manera gráfica bien sea estadística o geográfica GIS.

Por lo anterior, es importante tener en cuenta que la información puede ser recolectada de múltiples fuentes, lo que hace necesario el proceso de filtrado que permita la identificación de la misma, su clasificación en relevante y no relevante que puede llegar en diversos idiomas, para lo cual es necesario:

- Desarrollar modelos de conocimiento y su aplicación a los datos recogidos.
- Tener la capacidad de relacionar los datos para la elaboración de información relevante.
- Identificar modelos y patrones, los cuales se pueden aplicar a nuevos datos.
- Agilizar la toma de decisiones, mediante análisis de tendencias, identificando amenazas y oportunidades.

- Disponer de sistemas de alerta y seguimiento, informar sobre cambios significativos o actualizaciones masivas en las fuentes de información.

Para el diseño de un modelo de sistema, debemos partir de la definición de modelo de información, la cual se define como una representación de conceptos y relaciones entre ellos; así como las restricciones, reglas y operaciones que les son aplicables en un dominio específico, a diferentes niveles de abstracción presenta tanto la relación entre categorías como entre ejemplares específicos de información. Son una herramienta para representar la estructura y el comportamiento de los flujos de información permitiendo que estos sean intercambiados y organizados en un contexto definido (Kalchev, 2019).

Definición de la necesidad

Deficiencia en el procesamiento del ciclo de inteligencia y análisis de grandes volúmenes de información retardando la respuesta y prevención ante amenazas internas y externas que atenten contra la Seguridad Nacional.

Oportunidades y alcance

- Capacidad de análisis de información con herramientas de tecnología de punta
- Mitigación de riesgo de fuga, alteración y/o perdida de información
- Oportunidad en el proceso de toma de decisiones
- Información centralizada para toma de decisiones
- Apoyo en la toma de decisiones en operaciones militares
- Capacidad para neutralizar amenazas internas y externas
- Capacidad de actualización, corrección y retiro de datos de inteligencia
- Mejora en la imagen institucional
- Aumento de la capacidad del subsistema de inteligencia

Por lo anterior es importante tener en cuenta que de acuerdo a lo establecido en el articulo 2 de la ley estatutaria 1621 de 2013; la inteligencia y contrainteligencia como función publica es "aquella que desarrollan los organismos especializados del Estado del orden nacional, utilizando medios humanos o técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional" (Senado, 2013).

Adicionalmente hay que entender que la inteligencia como proceso es el producto resultante de la recolección, procesamiento, integración, evaluación, análisis e interpretación de la información disponible con el fin de facilitar el entendimiento del ambiente operacional en cuanto al enemigo, terreno, condiciones del tiempo y consideraciones civiles, para visualizar las áreas de operaciones (AO) actuales y futuras (Ejercito Nacional de Colombia , 2017).

Por otro lado se encuentran las actividades de contrainteligencia las cuales están destinadas a la preservación de personal, instalaciones, infraestructura, equipos, material e información que están encaminadas a identificar, prevenir, detectar, interrumpir, explotar, contrarrestar, disuadir, desinformar y neutralizar las acciones de inteligencia internas y externas u otros tipos de amenazas (hibridas, no hibridas y antrópicas), las cuales pretendan invalidar, retrasar, impedir o bloquear el empleo de los medios, equipos, material e instalaciones dispuestos en el área de operaciones, obstaculizar el mando tipo misión, exponer vulnerabilidades internas y alterar u ocultar datos de interés de la amenaza que ocasionen la disminución de la eficiencia del actuar militar (Ejercito Nacional de Colombia , 2017).

Teniendo en cuenta la misión que se espera que cumplan los organismos de inteligencia y contrainteligencia podemos deducir que el insumo principal, es la información, con la cual estos desarrollan el planeamiento de operaciones y entregan productos de inteligencia al mando militar para la toma de decisiones es por esto por lo que para efectos de este proyecto debemos tener en cuenta una serie de requerimientos que permitirán la estructuración del sistema.

Requerimientos mínimos de las fuentes de información

Las diferentes fuentes de información que alimentan el sistema integrado debe satisfacer los siguientes requerimientos:

a. La fuente debe estar previamente identificada y registrada dentro de los activos de información del sistema.
b. La información suministrada debe tener al menos el origen de datos, fecha de entrega, fecha de referencia de la información, tamaño de los datos.
c. Las fuentes deben conectarse por un canal seguro (VPN) u otro mecanismo de conexión segura (criptográfico).
d. Una vez se usa la fuente de información o ésta ya no se requiere, se debe retirar el inventario.

Modelo de general de sistema de información

Un modelo de información es una técnica desarrollada para definir y numerar los requisitos mínimos de infraestructura y datos que se gestionaran durante el desarrollo del sistema, para lo cual hay diferentes métodos que permiten este desarrollo.

Las metodologías en las que se pueden desarrollar diferentes modelados se generan en tres líneas (Lee, 2000).

- **ER** (entidad-relación), este enfoque se centra en cómo los conceptos de entidades y relaciones podrían aplicarse para describir los requisitos de información.
- **MF** (modelado funcional), el énfasis del enfoque de modelado funcional se pone en especificar y descomponer la funcionalidad del sistema.
- **O-O** (orientado a objetos), se enfoca primero en identificar objetos del dominio de la aplicación y luego en operaciones y funciones.

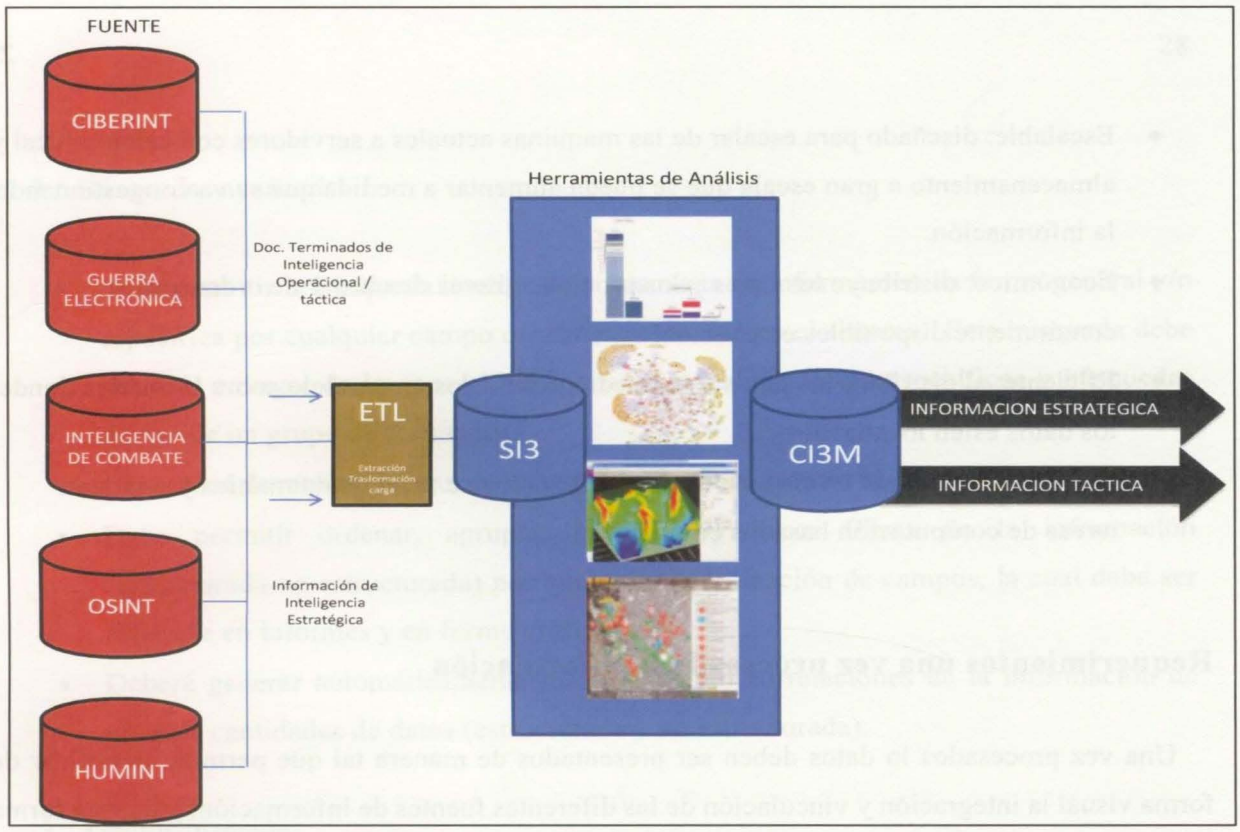


Figura 2: Diseño general del modelo de información. Fuente: elaboración propia, octubre 2018

Requerimientos para el proceso de la información

Durante la etapa de recolección y el proceso de información, los volúmenes de la misma, que se generan son muy altos entre los cuales se encuentran datos estructurados, semiestructurados o no estructurados; los cuales deben ser sometidos a análisis en tiempo real, para lo cual es necesario la aplicación de un proceso de *big data* que nos permitirá entregar productos de inteligencia garantizando principios como la oportunidad; es decir tener la capacidad de proceso de datos por medio de cálculos por ejemplo; calculo de la frecuencia absoluta en términos de estadística descriptiva de cada una de las disciplinas de la especialidad modalidades presentes en los datos de entrada al sistema, generando una salida de datos aplican procedimientos gráficos como pictogramas, diagramas de barras, etc. (Akerkar, 2019), teniendo como referencia que este procesado debe obedecer a las siguientes características:

- Escalable: diseñado para escalar de las maquinas actuales a servidores con calculo local y almacenamiento a gran escala que se pueda aumentar a medida que se va congestionando la información.
- Económico: distribuye los datos y los procesa a través de clúster de ordenadores comúnmente disponibles en el actual sistema.
- Eficiente: al distribuir los datos este pueda procesarlos en paralelo sobre los nodos donde los datos estén localizados.
- Fiable: debe generar un sistema de copias de datos de manera automática y realizar tareas de computación basados en fallos.

Requerimientos una vez procesada la información

Una vez procesados lo datos deben ser presentados de manera tal que permita identificar de forma visual la integración y vinculación de las diferentes fuentes de información; y de esta forma generar una comprensión integral de la inteligencia estratégica. La propuesta de inteligencia estratégica es concebida como un análisis integral, que contempla estudios del pasado, presente y futuro, transformando información en conocimiento útil para la toma de decisiones, a partir del análisis y así construir un plan estratégico, en el cual se brinde la posibilidad de planificar y formular estrategias ofensivas que minimicen la incertidumbre, con la finalidad de orientar exitosamente líneas operacionales en el cumplimiento de la misión institucional; por lo tanto una vez procesada la información esta se debe presentar en:

1. Con la información procesada el analista debe poder hacer seguimiento de acuerdo con los siguientes interrogantes:

   - **Observar** ¿qué está ocurriendo?
   - **Comprender** ¿por qué ocurre?
   - **Predecir** ¿qué ocurriría?
   - **Colaborar** ¿qué debería hacer el equipo?
   - **Decidir** ¿qué camino se debe seguir?

2. Búsquedas avanzadas

- Debe permitir la búsqueda inteligente y avanzada de información en forma general y/o específica por cualquier campo o criterio contenido en el sistema. Esta búsqueda debe permitir navegar de lo general a lo particular, realizar filtros específicos y búsquedas dentro de un grupo de resultados.
- Capacidad de realizar búsquedas programadas por el usuario bajo los criterios definidos.
- Debe permitir ordenar, agrupar, clasificar y hacer filtros de la información (estructurada-no estructurada) por cualquier combinación de campos, la cual debe ser reflejada en informes y en forma gráfica.
- Deberá generar automáticamente los enlaces y/o correlaciones de la información de grandes cantidades de datos (estructurada y no estructurada).

3. Geolocalización

- Debe tener la capacidad de visualización de información geográfica, con graficación de coordenadas en la información estructurada y no estructurada.
- Debe permitir el despliegue simultáneo de varias capas de información (cartográfica o georreferenciada) para graficación de escenarios.
- Debe permitir la graficación de áreas o sitios de interés (corredores de movilidad, rutas, etc.) sobre la cartografía existente, con la capacidad de ser almacenada como una capa en el sistema de información.

4. Alertas tempranas

- Debe permitir simular situaciones o alertas de posibles hechos o actividades para la adopción de medidas preventivas con base en los datos coleccionados, reglas predefinidas e interacción directa del analista con situaciones hipotéticas.
- Debe permitir exportar la información de la simulación en formato de reportes y gráficos.

- Debe tener la capacidad para realizar análisis, correlación de datos y aplicación de diferentes técnicas y algoritmos estadísticos para probabilidades, análisis de tendencias, riesgos, sesgos y creación de reglas de comportamiento para los modelos de simulación.

5. Generación de estadísticas

- Debe contar con la capacidad de generar estadística, descriptiva e inferencial
- Deberá generar e imprimir en forma tabular (datos) o en forma gráfica la información o análisis realizados, que incorporen programas y algoritmos para determinar riesgos, tendencias comportamientos de los datos, correlaciones y análisis en el tiempo.
- Debe permitir generar gráficas, reportes visuales e impresos.

Capítulo II

Requerimientos del sistema integrado de información de inteligencia y protocolos de seguridad

I. REQUERIMIENTOS DEL SISTEMA INTEGRADO DE INFORMACIÓN DE INTELIGENCIA

Para la configuración de un sistema integrado de información que cumpla con lo establecido en la ley estatutaria 1621 de 2013, este debe cumplir con los siguientes requerimientos.

1. Integración y fortalecimiento de la red de comunicaciones mediante aplicaciones criptográficas

El sistema de inteligencia cuenta con una infraestructura de comunicaciones digitales que debe ser fortalecida mediante el empleo de protocolos de comunicación que permitan el flujo de la

misma de una manera rápida, dinámica, sencilla a escala nacional y mundial, teniendo en cuenta todos los conceptos relacionados con los procesos de inteligencia entre entidades y agentes encubiertos, no encubiertos, agentes de control y área de análisis, debe hacerse mediante comunicaciones realizadas a través de las redes actuales, por lo cual, dichas comunicaciones deberían cumplir con varios de los principios de seguridad (Isaza, 2007):

- Confidencialidad.
- Autenticación.
- Integridad.
- No Repudio.
- Flexibilidad.
- Eficiencia.

Debido a lo anterior es importante que el sistema de inteligencia brinde la seguridad de su información adoptando medidas que garanticen el flujo de la información de una forma segura implementando las siguientes medidas.

1.1. Mecanismo de seguridad criptográfica

Para el desarrollo de un sistema de información seguro se deben tener en cuenta diferentes mecanismos de autenticación de mensajes, infraestructura de soporte, así como los certificados digitales e infraestructuras de clave pública o PKI (Garcia, 2014) que garantizaran que la información que se maneje en el sistema no sea comprometida por agentes externos al mismo, para lo cual debemos desarrollar mecanismos como:

1.1.1. Implementación del mecanismo de autenticación de mensajes

Para el desarrollo de mecanismos seguro de comunicación digital debemos tener en cuenta factores como la integridad, a través de la autenticación de mensajes, el cual es un servicio que garantiza que los mensajes recibidos no han sido modificados, que proceden de una fuente autentica, y con credibilidad; para lo cual se deben adicional ciertos mecanismos en donde se pueda

detectar si un mensaje ha sido retenido intencionadamente durante un tiempo, ha sido repetido o ha sido alterado; tarea que es importante a la hora de garantizar la certeza de la información. Para proporcionar este servicio vamos a tener en cuenta los tipos de cifrado: de clave simétrica o clave asimétrica:

1.1.1.1. Clave simétrica

La criptografía de clave simétrica o de llave compartida (Microsoft, 2013) permite cifrar la información o los datos con una llave que debe ser enviada al tercero para poder descifrar. Durante los procesos de inteligencia humana donde los agentes de campo, por lo general, no tienen un amplio conocimiento (o en la mayoría el conocimiento en tecnología es casi nulo), y se requiere encriptar información, se utilizará en aquellos procesos donde se requiera compartir información de una manera más rápida, la utilización de mecanismo de clave simétrica usando las funciones de tipo HMAC (Maiorano, 2010), teniendo en cuenta la fiabilidad de la fuente, toda vez que este requiere compartir una clave para el proceso de autenticación y verificación.

En razón a que las funciones HMAC utilizan internamente funciones hash (o resumen matemático o función de integridad), se puede generar un resumen de un mensaje que es función del propio mensaje y de una clave simétrica. En función del hash que lleven se denominan HMAC-MD5, HMAC-SHA (Sierra, 2014).

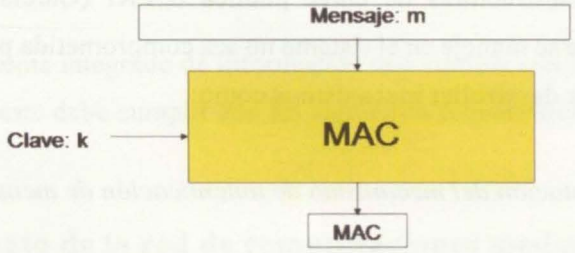


Figura 3: Proceso de validación de tipo hash. Fuente: Sierra, 2014

- Es fácil de reemplazar las funciones hash embebidas en función de la seguridad o rapidez requeridas.
- Conservar el rendimiento original de la función hash.
- El uso y gestión de las claves es sencillo.
- La fortaleza ante el análisis criptográfico del mecanismo de autenticación basado en la fortaleza de la función hash embebida. Si se descubre una debilidad de la función hash, se cambia por otra segura y el mecanismo continúa siendo fuerte.

Básicamente el procedimiento que se desarrollará para la encripcion de mensajes consistirá en introducir una clave K en un mensaje M y el sistema genera un resumen que es función del mensaje de la clave, al que denominamos HMACK(M). Este resumen es el autenticador que se envía junto con el mensaje para que el receptor pueda verificar su integridad (que no ha sido modificado) y autenticidad (lo ha generado alguien con quien comparte la clave K) (Oppliger, 2005).

Es importante tener en cuenta al momento de la configuración del algoritmo que como todo en los sistemas no son 100% seguros, en este caso el administrador de la seguridad debe tener en cuenta que la amenaza puede realizar ataques en el criptosistema en general por dos vías (Yerko, 2009):

1. Debilidades del algoritmo, si son conocidas.
2. Ataque por fuerza bruta utilizando todas las posibles claves. En este caso se requiere una media de 2k-1 intentos para una clave de k bits.

Por lo anterior es importante tener en cuenta que la fortaleza de la función MAC depende de la fortaleza de la función HASH embebida. Si se descubre una debilidad de la función hash embebida, se puede cambiar por otra más segura.

Los ataques de fuerza bruta en el caso de las funciones HMAC son diferentes a un mecanismo clásico como es un algoritmo de cifrado. Si se usa una HMAC de n bits, hay 2n posibles códigos. Si hay N posibles mensajes con N >> 2n, y existen 2k posibles claves de k bits,

Para la puesta en marcha del proceso de cifrado, debemos tener claro cómo funciona el esquema de uso, el cual consiste en dos usuarios que comparten una clave, la cual utilizan para generar un código de autenticación del menaje MAC (Message Autenticación Code). Un usuario le envía un mensaje con su MAC al otro, y el receptor genera su propio MAC con la clave compartida y verifica que coincide con el MAC recibido. La coincidencia de ambos MACs proporciona garantías de autenticación e integridad. Como puede verse en la figura 3, El emisor comparte una clave con el receptor, con la que genera el MAC del mensaje que le envía. Cuando el Emisor recibe el mensaje genera el MAC con la misma clave y verifica que coincide con el MAC enviado por el Receptor (Dent, 2004).

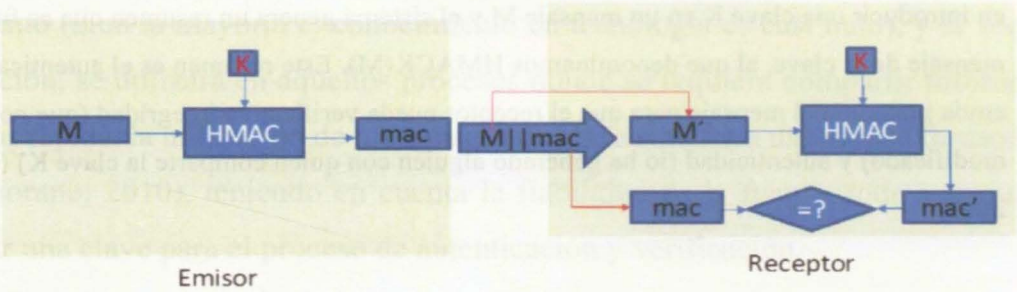


Figura 4: Esquema de uso de una función HMAC Fuente Guía de estándares Criptográficos,

Adicionalmente hay que tener en cuenta que los algoritmos basados en HMAC plantean el mismo inconveniente de gestión de clave que los algoritmos de cifrado simétrico, pero son los procesos criptográficos más rápidos y por lo tanto para la comunicación entre los agentes control y sus fuentes son los más convenientes ya que en este escalón de la cadena de producción de inteligencia requieren autenticar gran cantidad de mensajes y el tiempo de procesamiento de los mensajes es crítico dada la relevancia que pueden tener los mensajes para el proceso militar de toma de decisiones.

Con la implementación de las funciones HMAC se tendrán grandes ventajas entre las que encontramos (Dent, 2004):

- Usa funciones hash (no criptografía) cuyo código es altamente disponible.

donde k > n. Con este escenario un grupo de claves (por terminó medio 2k /2n= 2k-n) producirán el mismo resumen HMAC de un mismo mensaje (Cope, 2017).

Esto creará confusión al oponente que utilice la fuerza bruta y le obligará a probar con otro mensaje y las 2k-n claves obtenidas de la primera vuelta. Se repetirá el proceso y se obtendrá la clave cuando se hayan realizado k/n vueltas (Stevens, 2012).

En conclusión, podemos decir que para aplicar ataque de fuerza bruta en MAC requiere mayor esfuerzo que en un sistema de cifrado criptográfico con clave de igual longitud. Por terminó medio el esfuerzo para una clave longitud K es 2k, frente a 2k-1 de los sistemas de cifrado.

1.1.1.2. Clave asimétrica

Para procesos donde se requiera establecer comunicación entre niveles más altos o entre agencias, el mecanismo más recomendado es el de clave asimétrica del cual nos apoyaremos en el más habitual que es la firma digital, que además ofrece el servicio de no repudio, es decir, quien genera un mensaje firmado no puede más tarde repudiar haberlo generado.

El cifrado de clave asimétrica (Microsoft, 2013) consiste en generar un par de claves (una pública y otra privada), cada persona, agente o sistema que requiere usar dicho cifrado debe generar el par de claves, una vez generadas, el emisor envía a un receptor su llave pública, el receptor cifra la información con dicha llave y devuelve la información cifrada, el emisor toma el mensaje y lo descifra con su llave privada, en ese sentido, no es necesario la compartición de llaves.

1.1.2. Implementación del mecanismo de firma digital

Debido a la complejidad de la información que es manejada entre agencias y a la responsabilidad que recae sobre el personal de analistas y comandantes de unidades encargadas de búsqueda y

difusión de la información; es necesario cumplir con lo dispuesto en la ley estatutaria 1621 de 2013 "*Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones*" en el artículo 36 parágrafo 1 el cual dice (Senado, 2013).

"Parágrafo 1. Los jefes y directores de los organismos de inteligencia y contrainteligencia establecerán los procedimientos y controles para la difusión y trazabilidad de la información de inteligencia y contrainteligencia. La difusión deberá hacerse en el marco de los fines, límites y principios establecidos en el marco de la presente Ley".

Por lo anterior es necesario aplicar un mecanismo como la firma digital el cual es útil por la necesidad de implementar un mecanismo similar a la firma manuscrita en el ciberespacio, que garantice los tramites de productos de inteligencia como informes y alertas tempranas sobre posibles acciones terroristas las cuales son difundidas a través de la red.

La firma digital se define como un bloque de caracteres anexado a un documento que permite salvaguardar las propiedades de seguridad de autenticación, no repudio e integridad, pues permite certificar quien es su autor y la no existencia de ninguna manipulación de los datos, cuya validez puede ser comprobada por cualquier persona que disponga de la clave pública del firmante. A este bloque le hemos denominado anteriormente de forma genérica autenticador (Quiroga, 2004).

En la figura se representa un mapa de la firma digital, figura 5, utilizado en España y que puede ser un modelo para el que se emplearía en el sistema, que engloba todos los aspectos asociados a la misma (Jhon, 2018).

en el dispositivo donde se almacena, como durante la transacción realizada. Entre las modificaciones que se pueden realizar tenemos sobre escritura, borrado, corrupción de datos, etc. (Bertolin, 2008).

- **Autenticación**. Capacidad que permite garantizar que una persona, entidad o proceso es quien dice ser o bien que garantiza que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema, ya que la firma ha sido creada por el signatario mediante medios que mantiene bajo su propio control: su clave privada secreta (Wiley, 2007).

- **No repudio**. Capacidad que permite verificar al emisor del documento negar en ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema. Solo puede ser generada por el poseedor de la clave privada y puede ser verificada por cualquiera que conozca la clave pública del firmante (Kouns, 2009).

- **Imposibilidad de copia.** Capacidad que impide que nadie pueda copiar la firma de un documento a otro documento ya que se detectaría como invalida. Es dependiente del documento a firmar, no puede emplearse para firmar otro documento.

- **Trazabilidad.** Capacidad que garantiza la posibilidad de imputar las acciones relacionadas en una transacción a la persona, entidad o proceso que la ha originado.

Teniendo en cuenta lo anterior, los requisitos para que la firma digital sea compatible con lo dispuesto en la Ley 1621 de 2013 deben ser los siguientes (Aguirre, 2018).

- Debe ser fácil de generar.
- Será irrevocable, no rechazable por su propietario.
- Será única, solo posible de generar por su propietario.

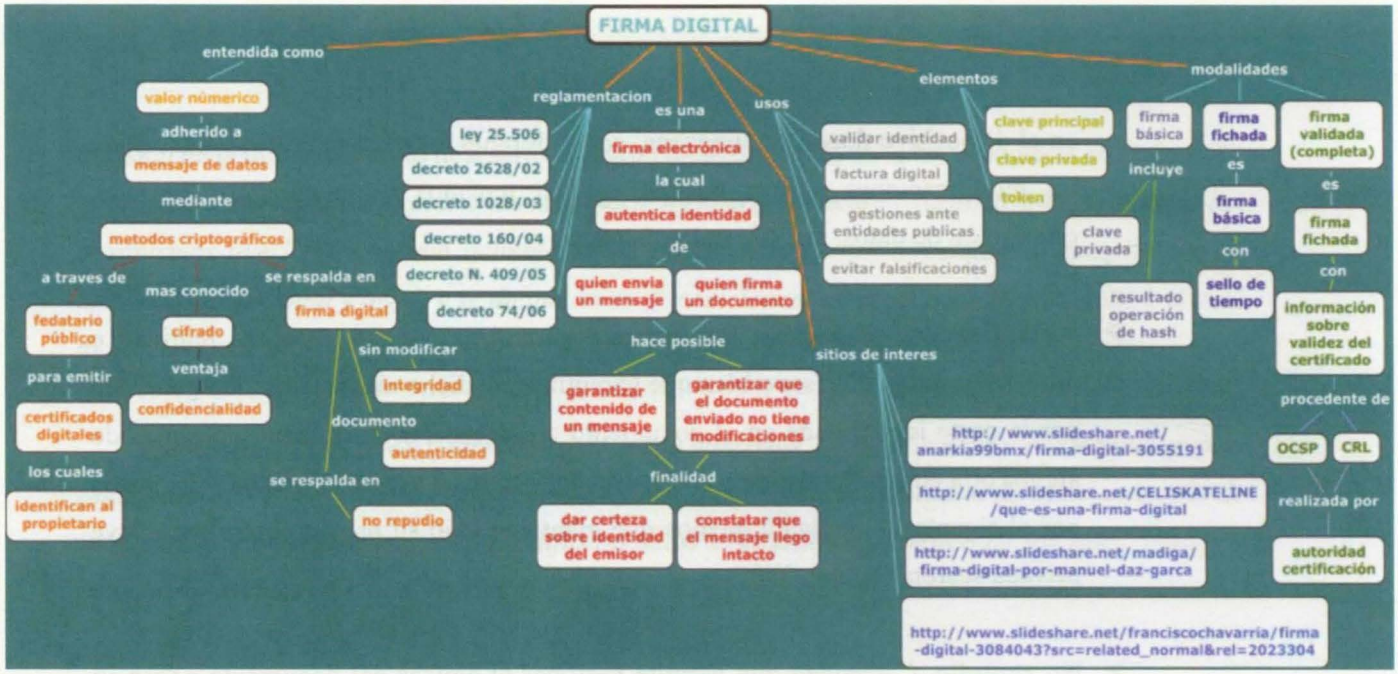


Figura 5: Mapa de la firma digital.

Fuente https://jhonf10.wordpress.com/gestion-tecnologica/mapa-conceptual-firmas-digitales/

La manera como se desarrollaría la integración de la firma digital dentro del proceso de homologación de mensajes se desarrollaría de la siguiente manera:

- Receptor genera una clave privada aleatoria, y calcula la clave pública que corresponde a esa clave privada.
- Emisor genera una clave privada aleatoria, y calcula la clave pública que corresponde a esa clave privada.
- Receptor y Emisor envían su clave pública a una base de datos, accesible a los dos. Evita el problema de ponerse de acuerdo en la clave a utilizar.
- Receptor encripta el mensaje usando la clave pública de Emisor, y se la envía.
- Emisor utiliza su clave privada para desencriptar el mensaje.

Con el uso de la firma digital el sistema tendrá las siguientes propiedades de seguridad:

- **Integridad de la información.** Capacidad que garantiza que el documento no haya sido modificado o alterado por personas, entidades o procesos no autorizados tanto

- Será fácil de autenticar o reconocer por su propietario y los usuarios receptores.
- Debe depender del mensaje y del autor. Esta última propiedad es muy importante pues protege ante la falsificación de los mensajes.

Tal y como se ha venido trabajando a lo largo del texto, es importante recalcar que la firma digital se compone habitualmente, cifrando con la clave secreta, un resumen digital del mensaje original, obtenido por funciones hash (puede ser de tipo SHA).

Como se indicó, para verificar una firma, el receptor descifra la firma con la clave pública del emisor, comprime con la función hash el texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden, el receptor tiene la garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la clave secreta (Nash, 2002).

Actualmente los algoritmos de firmas digitales más usados y extendidos son los siguientes:

- RSA. Diseñado por el CCITT dentro del diseño del sistema de autenticación para el Directorio X.500.
- El Gamal. Desarrollado por Taher El Gamal en 1984.
- DSS (Digital Signature Standard) utilizado por el U.S. National Institute of Standards and Technology (NIST), conocido como DSA.
- CCE o algoritmo de curva elíptica.

De los anteriores tendremos en cuenta el algoritmo RSA; desarrollado en 1978, debe su nombre a sus tres inventores: Ronald Rivest, Adi Shamir y Leonard Adleman, lleva las iniciales de sus apellidos RSA, basa su fortaleza en la propiedad matemática de "factorización entera" o dificultad computacional de factorizar, para la capacidad de cómputos de las máquinas de proceso de hoy en día, un número compuesto grande de (1024 bit), producto de dos primos grandes (512 bit) cuyo cálculo es fácil y rápido y a la inversa computacionalmente inviable de encontrar tales factores

primos dado tal número grande. Es uno de los esquemas de firma digital más practica y versátil de los existentes hoy en día.

El proceso de firma digital con el algoritmo RSA, para garantizar la autenticación del origen, integridad del mensaje y el no-repudio en origen, se realizará sobre un número, resultado de aplicar una función hash a un mensaje.

Para la aplicación del algoritmo RSA en el sistema integrado de información se estructurara de manera que la agencia que necesite enviar una quiere enviar un informe a otra agencia; este informe podrá ir cifrado o no, pero la agencia que envía el informe por lo dispuesto en la Ley 1621 debe firmar el informe de manera tal que la agencia que recibe el mismo, pueda estar seguro que el mensaje que le llega ha sido originado por la otra agencia y no por ninguna otra entidad o producto de una operación de engaño de la amenaza.

Para la generación de la firma digital requerida para el sistema integrado de información se deben seguir los siguientes pasos (García, 2016):

Los pasos que el Emisor con clave pública (e y n) y clave privada (d) deberá seguir para crear la firma con el algoritmo RSA son:

1. Crea un resumen (digest) del mensaje que quiere enviar, utilizando una función hash.
2. Representa este resumen como un entero R(m) entre 0 y n-1.
3. Usa su propia clave privada (d, n) para computar la firma: $S = (R(m))dmod\ n$
4. Envía esa firma S al receptor conjuntamente con el mensaje original (que puede ir cifrado o no). Evidentemente, la firma S no podrá ser manipulada por nadie una vez generada, porque si se cambia un sólo bit de la firma fallaría la verificación de ésta en destino.

Verificación:

Los pasos que el Receptor deberá seguir (figura 6) para verificar la firma con el algoritmo RSA son (Dorothy, 2019)

1. Utiliza la clave pública del Emisor para calcular.
2. Del entero V obtiene el resumen R(m) del mensaje tal y como fue computado por el emisor
3. Paralelamente, calcula el resumen R'(m) del mensaje que le ha llegado utilizando la función hash correspondiente.
4. Si ambos resúmenes R(m) y R'(m) coinciden, entonces queda verificada la firma. Entonces puede asegurarse que el mensaje solo ha podido ser originado por A y además el mensaje ha llegado íntegramente sin alterarse su contenido durante su por la red de comunicaciones hasta el receptor.

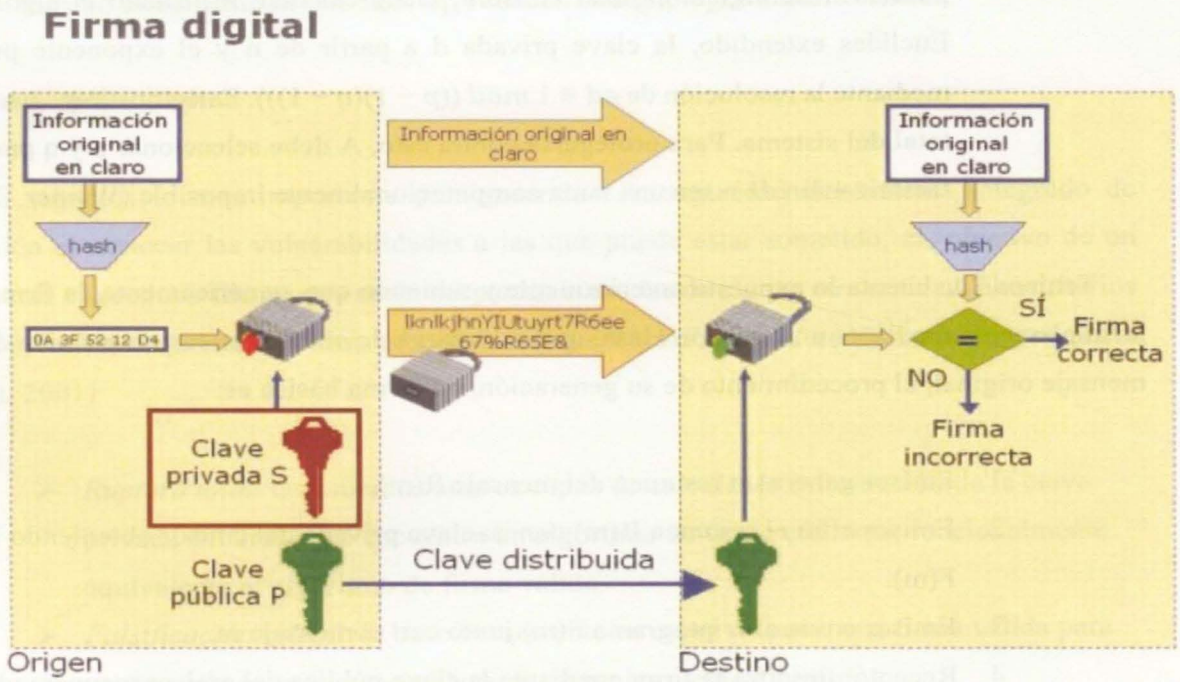


Figura 6: Firma algoritmo RSA.

Fuente: http://www.dma.fi.upm.es/java/matematicadiscreta/aritmeticamodular/rsa2.html

Debilidades del algoritmo RSA

Aunque la firma electrónica con el algoritmo RSA es bastante segura, existen varios puntos débiles que conviene comentar para tener en cuenta al momento de estructurar el algoritmo para el sistema integrado de información:

- **Ataque de firma y decodificar**. Relativo a su forma de uso, nunca se debe firmar un mensaje después de codificarlo, por lo contrario, debe firmarse primero. Existen ataques que aprovechan mensajes primero codificarlos y luego firmados, aunque se empleen funciones resumen (Phesso, 2009).

- **Factorización de enteros**. Si un ciberatacante es capaz de factorizar el módulo publico n de alguna entidad emisora puede calcular, utilizando el algoritmo de Euclides extendido, la clave privada d a partir de n y el exponente público y mediante la resolución de $ed \equiv 1 \ mod \ ((p-1)(q-1)))$. Esto constituye una ruptura total del sistema. Para protegerse contra esto, A debe seleccionar p y q para que la factorización de n sea una tarea computacionalmente imposible (Wiener, 2010).

Teniendo en cuenta lo expuesto anteriormente y sabiendo que, genéricamente, la firma digital se implementa mediante una función Hash, que se encarga de obtener un resumen único del mensaje original, el procedimiento de su generación, de forma básica es:

1. Emisor genera un resumen del mensaje R(m).
2. Emisor cifra el resumen R(m) con su clave privada del emisor obteniendo la firma F(m).
3. Emisor envía el criptograma F(m) junto con el mensaje m.
4. Receptor descifra la firma mediante la clave pública del emisor recuperando el valor de hash R(m).
5. Receptor obtiene el hash del mensaje recibido m´ para crear un segundo valor de hash R(m´). Si el mensaje no ha sido modificado m sería igual a m'.

6. Receptor verifica que R(m) = R(m'), en ese caso se puede afirmar que el mensaje es íntegro (m' = m). Además, al haber descifrado con la clave pública del emisor para obtener h(m), podemos afirmar que el mensaje es auténtico (cifrado con la clave privada del emisor).

Teniendo en cuenta el desarrollo de la estructura de firma digital para el sistema integrado de información cabe destacar que:

- Cualquiera que posea la clave pública de emisor puede constatar que el mensaje proviene realmente de él.
- La firma digital es distinta en todos los documentos: si el emisor firma dos documentos genera dos criptogramas distintos y si el receptor y el emisor firman el mismo documento m también se producen dos criptogramas diferentes.

Ataques a la firma digital

Como sabemos lo más importante para garantizar la seguridad del sistema integrado de información es conocer las vulnerabilidades a las que puede estar sometido, el objetivo de un ciberatacante es producir firmas que serán aceptadas como las de alguna otra entidad. Los criterios por los cuales un esquema de firma se considera que ha sido roto o comprometido son (Paul Oorschot, 2001)

- *Ruptura total*. Un ciberatacante es capaz de calcular la información de la clave privada del emisor, o encuentra un algoritmo de firma eficiente, funcionalmente equivalente al algoritmo de firma válido.
- *Falsificación selectiva*. Un ciberatacante es capaz de crear una firma válida para un mensaje en particular o clase de mensajes elegido a priori.
- *Falsificación existencial*. Un ciberatacante es capaz de falsificar una firma para al menos un mensaje. El ciberatacante tiene poco o ningún control sobre el mensaje cuya firma se obtiene y el firmante legítimo puede estar involucrado en el engaño

Hay dos ataques básicos contra los esquemas de clave pública de firma digital.

- *Ataques a la clave*. En estos ataques, un ciberatacante sólo conoce la clave pública del firmante.
- *Ataques al mensaje*. Aquí un ciberatacante es capaz de examinar las firmas correspondientes a los mensajes elegidos. Pueden ser subdivididos en tres clases:
  - *Ataque a mensajes conocidos*. Un ciberatacante tiene firmas para un conjunto de mensajes, pero no elegidos por él.
  - *Ataque a mensajes elegidos*. Un ciberatacante obtiene firmas válidas de la lista elegida de los mensajes antes de tratar de romper el esquema de firma.
  - *Ataque adaptado mensaje elegido*. Un ciberatacante podrá pedir firmas de mensajes que dependen de la clave pública del firmante y podrá solicitar las firmas de los mensajes que dependen de firmas o mensajes obtenidos anteriormente.

2. Implementar una infraestructura de clave publica

Para que el sistema de inteligencia pueda establecer una trazabilidad del flujo de información de manera que garantice la seguridad de la misma es necesario organizar una infraestructura tecnológica que garantice que la información llegue al funcionario que requiere la misma y así cumplir con lo descrito en el articulo 36 de la ley estatutaria 1621 de 2013 que lista los receptores de productos de inteligencia y contrainteligencia para lo cual una infraestructura de clave publica es la mejor opción; requiriendo.

2.1. Establecer un certificado digital

Para completar los requerimientos de seguridad no solo basta con adicionar un algoritmo de cifrado, si también complementarlo con mecanismos que ayuden a blindar cada uno de los niveles de seguridad ya que con solo la aplicación del cifrado generaríamos un grave problema a nivel de seguridad, relativo a la capacidad de asegurar que una clave pública pertenece a un usuario dado,

en este sentido surge la necesidad de poder vincular la clave pública de un usuario con su identidad, razón por la cual surge el concepto de "Certificado Digital" (Jalal Feghhi, 1998).

Un certificado digital se puede definir como un documento digital que contiene una clave pública y el identificador del usuario, maquina, aplicación o servicio concreto, firmado digitalmente por una autoridad de certificación (AC), que garantiza la vinculación entre ese usuario o dispositivo y su clave pública (Talens, 2019).

Para el sistema integrado de información se empleará el certificado digital estandarizado con base a la recomendación X.509 de CCITT (Consultative Committee for International Telegraphy and Telephony) llamada "*The Directory– Autentication Framework*", que data de 1988 y actualmente se encuentra en su versión 3; de la cual se extraerá la especificación del marco de autenticación para el Directorio X.500; por el cual se definirá la sintaxis de los certificados, y contemplará los siguientes campos:

- *Versión*. Versión del certificado X.509, normalmente la versión 3.
- *Número de serie*. Identificador numérico asignado por la AC emisora, que identifica unívocamente al certificado dentro del conjunto de certificados emitidos o revocados.
- *Firma*. Algoritmo utilizado por la AC para firmar el certificado y función de una sola vía hash utilizada.
- *Emisor*. Nombre del emisor identifica a la entidad que ha firmado el certificado, en formato X.500.
- *Validez*. Intervalo de tiempo, fechas inicio y final, en el que el certificado es válido.
- *Usuario o sujeto*. Nombre del propietario de la clave pública, que identifica de forma unívoca al poseedor del certificado, en formato X.500.
- *Identificador del algoritmo* y clave pública del propietario que se ha utilizado y parámetros opcionales.
- *Campos de extensión*. Permiten definir y añadir de nuevos campos a la estructura sin tener que modificar la definición del certificado.

- *Identificadores únicos de emisor y de usuario.* Cadena de bits opcional que identifica al emisor o al usuario en el caso de que su Nombre distinguible X.500, sea reutilizado con el paso del tiempo.
- *Firma digital de la AC.* Resultado de cifrar el hash del certificado X.509 con la clave privada de la AC.

Con la integración de una firma, realizada por la autoridad certificadora, permitirá que las agencias de inteligencia que deseen realizar comunicaciones entre ellas o con los diferentes agentes de control que posean un certificado, puedan comprobar que la información que éste contiene es auténtica.

Con la organización de certificados, una vez que estos han sido firmados, se almacenaran en los servidores de directorios y/o transmitidos por cualquier medio (seguros o no) para que estén disponibles públicamente para todo el sistema de inteligencia.

Los certificados tendrán un periodo de vida limitado, el cual estará especificado en el campo validez y viene determinado por la política de seguridad física del departamento de contrainteligencia de la fuerza quien tendrá línea directa con la AC emisora. Sin embargo, en algunas ocasiones especiales la seguridad de la clave privada asociada puede verse comprometida, por lo que la utilización de la correspondiente clave pública ha de ser evitada. En tal caso, la AC emisora puede revocar el certificado para prevenir su uso fraudulento. Se estructurarán diferentes tipos de certificados en función de los roles que desempeñen los funcionarios en el sistema de inteligencia (Real Casa de la Moneda, 2018)

- *Certificado personal.* Acredita la identidad de la persona física titular, puede incluir adicionalmente estado, profesión o situación
- *Certificado profesional.* Además de acreditar la identidad del titular incluye otros datos como la agencia a la cual pertenece y el cargo que ocupa.
- *Certificado de unidad.* Identifica a una agencia, batallón, compañía, etc., que utiliza el mismo.

- *Certificado de equipo seguro*. Utilizado en los servidores, equipos de escritorio, enrutadores, etc. para el intercambio de información con otros sistemas con tecnologías como IPSEC, TLS, etc., y permitirá direccionar el tráfico que viene de la agencia.

- *Certificado de firma de código*. Garantiza la autoría y la no modificación del código (Integridad) de aplicaciones informáticas empleadas en el sistema para la recolección de información o intercambio de esta.

Para cada tipo de certificado, el batallón de seguridad de la información del comando de contrainteligencia será el encargado de recoger y publicar en un documento clasificado de obligatorio cumplimiento, donde enmarque las políticas de seguridad llamado "*Documento de prácticas de certificación*", que debe estar accesible para todos los usuarios del sistema y se referencia en el propio certificado.

2.2. Configurar la infraestructura PKI

El acrónimo PKI proviene de "Public Key Infrastructure" (Infraestructura de Clave Pública) y consiste en una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas de clave pública como el cifrado, la firma digital, no repudio de transacciones electrónicas, gestión de certificados digitales, etc. y engloba tanto a la autoridad de certificación (AC) como al resto de componentes (Bertolín, 2004).

Para la gestión e la seguridad del sistema integrado de información se desarrollará una PKI que nos proporcione las siguientes propiedades de seguridad:

- Autenticación mediante firma digital.
- Integridad, mediante la capacidad de detectar si un documento firmado ha sido manipulado.
- Confidencialidad de la información intercambiada entre los usuarios.

- No repudio, de un documento firmado digitalmente o transacciones realizadas.

En la siguiente figura 7 se muestra los diversos servicios que podría proporcionar la PKI del sistema integrado de información.

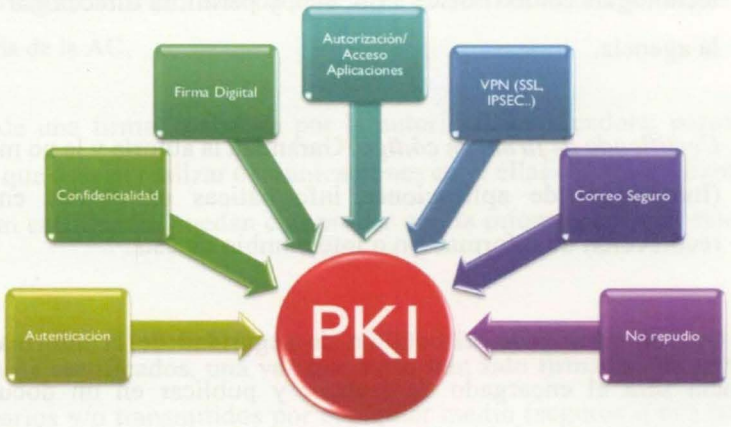


Figura 7: Servicios de una PKI. Fuente Bertolín, 2004

2.2.1. Componentes de la PKI

Para la gestión de un modelo seguro de un sistema integrado de información se debe estructurar una PKI con la infraestructura necesaria para la distribución de claves públicas a aquellas unidades que las necesiten utilizar, de tal manera que el receptor de una clave pública puede estar seguro de su integridad, autenticidad y vinculación a una entidad determinada. Para ello los esquemas de firma digital, certificados, etc., deben englobarse en una infraestructura, cuyos componentes básicos necesarios se resumen así (Valbuena, 2006).

La autoridad de certificación (CA, Certificate Authority).

Es la pieza fundamental de esta infraestructura, pues proporciona la plataforma de confianza que garantiza la validez de los certificados mediante su firma; estará constituida por elementos hardware, software y humanos y será la encargada de emitir y revocar los certificados del personal del sistema, teniendo en cuenta que actividad se encuentra desarrollando y permitirá revocar el certificado una vez que el funcionario sea asignado a otra dependencia; adicionalmente

y como rol más importante, esta dará legitimidad a la relación de una clave pública con la identidad de un usuario.

La autoridad de certificación emitirá una serie de políticas, o procedimientos operativos de certificación, que regirán el funcionamiento de la PKI del sistema integrado de información y establecerá las funciones y responsabilidades entre la autoridad certificadora y los usuarios finales. Estos documentos tendrán un carácter tanto técnico, clasificado y legal.

La autoridad de registro (RA, registration authority). Sera la responsable de verificar el vínculo entre los certificados, concretamente su clave pública, y la identidad de sus titulares. Se encarga de la publicación de certificados en un repositorio y se configuraran según la función de su ámbito en principales y locales.

Repositorios. Serán las estructuras encargadas de almacenar la información relativa a la PKI; distribuidas en dos grupos:

Repositorio de certificados. Permitirá a los usuarios operar entre ellos, como la validación de una firma digital, y es un requisito legal que cuenta con una total disponibilidad de acceso.

Lista de revocación de certificados (CRL, Certificate Revocation List). Se incluyen todos aquellos certificados que por algún motivo han dejado de ser validos antes de la fecha establecida dentro del mismo certificado.

Soporte de la clave privada. Sera la encargada de diseñar y administrar el sistema de gestión de smartcards, que permita la emisión y distribución de las tarjetas a los usuarios para que estos custodien su clave privada.

La autoridad de sellado de tiempo (TSA, Time Stamp Authority). Incluye un sello de tiempo con la finalidad de probar que existían antes de un determinado instante de tiempo.

Aplicaciones "PKI-enabled". Se denominan así a las aplicaciones software capaces de operar con certificados digitales. Estas aplicaciones son las que dan el valor real de la PKI de cara a los usuarios de esta.

Durante el proceso de construcción de la PKI se deberá partir de la definición de las políticas del comando del Ejército Nacional para el manejo de información clasificada y contemplar como requerimiento esencial el asegurar la calidad y seguridad de las operaciones de información que los usuarios finales realizan con sus claves.

3. Protocolo de seguridad para la gestión de información en la red

Uno de los grandes retos de la inteligencia es poder generar una comunicación segura por medio de un medio inseguro (que es lo normal que se tiene), que nos brinde la posibilidad de realizar manejo de información de una manera rápida, dinámica, sencilla y a escala mundial; abarcando todos los conceptos relacionados con los procesos de manejo de la información entre agencias, realizados a través de redes de telecomunicaciones y que cumplan con las principales propiedades como, la confidencialidad, la autenticación, la integridad, el no repudio, la flexibilidad y la eficiencia.

Como en el comercio electrónico, las agencias de inteligencia necesitan de las redes privadas virtuales que para establecer comunicaciones seguras y la búsqueda de información en la web que nos permita explotar las ventajas el comercio electrónico; para lo cual se proporcionara un marco de seguridad mediante la aplicación de un protocolo como el TLS.

Protocolo TLS

Transport layer security (TLS) es un protocolo estandarizado por el IETF2. Está basado en SSL v3, es totalmente compatible con el sistema, incorporando algunas mejoras, ayudando a la independencia de terceros en razón a que no es de una empresa privada.

En la actualidad se ha liberado la versión 1.3 de TLS, dado que las versiones anteriores 1.2, 1.1 y 1.0 tienen problemas de seguridad y ya fueron expuestos. TLS es un protocolo que permite el aseguramiento de los datos desde y hacia sitios web, aunque puede usarse para asegurar conexiones a nivel de red y de firmas digitales (Symantec, 2019).

La versión 1.3 de TLS soporta varios cifrados fuertes, que permiten dar garantía de confidencialidad e integridad en la comunicación, sin embargo, entre los años 2018 y 2019 se han encontrados algunas vulnerabilidades en las api de cifrado y otros componentes del protocolo, aun así; no se tiene otro mecanismo para cifrar páginas web que sea robusto (Lan, J. Xu, Z. Zhang and W. Zhu, 2019).

4. Protocolo para la red privada virtual VPN

El sistema de inteligencia debido a su despliegue nacional e internacional debe en ocasiones valerse de los enlaces de comunicaciones suministrados por las redes públicas, en este contexto se requiere de una red privada virtual (VPN) como solución de comunicaciones, en razón a que esta clase de red establece una red privada dentro de una red pública como es el caso de Internet, la comunicación se establece mediante tecnologías de encriptación y encapsulamiento que crean un canal virtual privado y seguro para comunicar datos privados, lo que se denomina típicamente túnel; combinando los conceptos de redes públicas virtuales - privadas y enlaces lógicos privados sobre la red física, independiente de esta y con su infraestructura de soporte (Gonzalez, 2006).

4.1. Objetivo de la VPN

El objetivo es valerse del soporte de una infraestructura pública de red que permita la transmisión de datos, compartiendo servicios entre los diferentes elementos del sistema los cuales se encuentran localizados en áreas alejadas y por su misión no podrían tener acceso a una terminal dentro del dominio de la red (Gonzalez, 2006).

Al configurar la VPN el agente va a poder proteger los datos durante la transmisión a través de la red, permitiendo el uso de redes públicas como si fueran privadas siendo necesario para este propósito configurar los siguientes servicios de seguridad:

Confidencialidad. Implantación de algoritmos de cifrado, tipo AES.
Integridad. Implantación del algoritmo HMAC.

Disponibilidad. Implantación de soluciones de alta disponibilidad que proporcionen redundancia en caso de fallo.

Autentificación. Mediante usuario y clave, certificados digitales etc.

4.2.Componentes VPN

La VPN requerida debe contar con los siguientes componentes básicos (Caire, 2018):

- *Servidor VPN.* Dispositivo de red, como un cortafuegos, servidor o dispositivo dedicado, encargado de la creación o terminación de una o varias VPN; el cual establece los puntos de conexión y terminación de los túneles de la VPN, este debe ser un equipo bastionado, robusto, en alta disponibilidad y libre de vulnerabilidades conocidas de seguridad.
- *Túnel,* canal virtual que encapsula o empaqueta los datos transmitidos, paquetes IP, con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta alcanzar su destino y cifrado de los mismos para asegurar la confidencialidad.
- *Conexión VPN,* punto de la conexión en la que se encapsulan y cifran los datos privados. *Red pública de tránsito*, red por donde el agente se conectará para establecer conexión con el agente control como puede ser el caso de Internet.
- *Cliente VPN*, aplicación de usuario que encapsula y cifra los datos privados.

4.3.Requerimientos VPN

Con base en lo anterior los requerimientos que deben cumplir las conexiones privadas virtuales (VPN) son (Borghello, 2002)

Escalabilidad: Esto significa poder decidir cuanta información puede manejarse al mismo tiempo, y efectivamente poder hacerlo (Sale Systems, 2018).

Rendimiento: Este uno de los puntos críticos, la VPN debe estar preparada para manejar una gran cantidad de tráfico (Avast, 2019).

Disponibilidad: Las soluciones VPN están siendo adoptadas estratégicamente por las organizaciones para proveer accesos externos y eliminar altos costos de conectividad, por lo que su disponibilidad debe estar asegurada en todo momento, mediante arquitecturas de alta disponibilidad, redundancia de enlaces de comunicaciones, etc. (Borghello, 2002).

Transparencia: La VPN necesita ser fácil de usar y entender para el usuario, que lo utilizará sin saber cómo exactamente trabaja, una vez que han sido definidos los "túneles" de protección de la información. Una buena política de distribución debe permitir a la VPN determinar cuándo encriptar y cuando enviar texto claro, pidiéndole al usuario únicamente su autentificación para proveer el acceso (Borghello, 2002).

Fácil de administrar: una VPN que se instale debe ser fácil de administrar, como todo producto de seguridad, donde la administración y el control centralizado de la solución es clave. El módulo de control debe tener una simple vía para diseñar la política de seguridad, y una fácil distribución de esa política en todos los niveles de la agencia u organización (Borghello, 2002).

Interoperabilidad: Una completa VPN debe poder comunicarse con otros productos VPN de diferentes fabricantes (Estado Unidos de America Patente nº US8151323B2, 2007).

Encriptación: La solución VPN deberá ofrecer distintos tipos de encriptación, que se utilizarán de acuerdo con las necesidades de cada segmento de la red. El estándar actual para la encriptación comercial es DES o 3DES, pero existen otras alternativas como BlowFish o CAST (168 bit) (Draper, 2016).

Seguridad: Uno de los requerimientos más importantes antes de implementar la VPN, es contar con políticas y procedimientos de seguridad definidos; el batallón de seguridad de la información será en encargado de establecer estas políticas, ya que la red virtual sólo

resuelve un problema específico de comunicación, pero su configuración va a estar basada en la política que diseño la unidad en la que contemplo el análisis del riesgo que debe atacar con la instalación de esta herramienta; y una de las formas más seguras y exequibles es combinar la flexibilidad de los protocolos VPN con la seguridad proporcionada por IPSEC (Draper, 2016).

Autenticación de usuarios. Cada unidad participante en una VPN debe de identificarse a sí misma ante otros y viceversa mediante un proceso que permite a los diversos integrantes de la VPN verificar las identidades de todos y establecer que la comunicación sea con la persona que se desea y así garantizar uno de los principios fundamentales de la inteligencia como lo es la compartimentación; para esto se pueden emplear mecanismos de autenticación como una PKI, servidor de acceso por protocolo RADIUS4, TACAS5, etc. (Draper, 2016).

Control de acceso. Conjunto de actividades y técnicas que rigen el acceso a los recursos privados de una red por parte de usuarios autorizados, se suele utilizar para ello Network Access Server (NAS) sobre el protocolo PPP6, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS (Borghello, 2002).

Administración de direcciones. Un servidor VPN debe de asignar una dirección IP al cliente VPN y asegurarse de que dicha dirección permanezca privada y protegidas con fuertes mecanismos de seguridad, como la ocultación de la dirección privada dentro de una red pública (Borghello, 2002).

Soporte de múltiples protocolos. Para que la solución VPN sea viable, es necesario también que ésta pueda ofrecer soporte a múltiples protocolos, incluso que no sean IP como pueden ser AppleTalk, IPX y NetBEUI. PPTP soporta varios protocolos de red. IPSec sólo puede ser utilizado en redes basadas en IP, pero siempre es posible encapsular los protocolos no compatibles dentro de un paquete IP, de modo que puedan ser transportados. En cuanto a L2TP, este protocolo VPN no sólo puede ser implementado en redes IP, sino también en A TM y Frame Relay (Borghello, 2002).

4.4. Arquitectura de red para la VPN del sistema de inteligencia

Existen básicamente dos tipos de arquitecturas de red para una VPN (Martinez, 2011):

VPN de sitio a sitio. Constituyen un caso normal de interconexión entre dos entidades remotas de una organización. Se implementan mediante la implantación de dos concentradores de VPN en ambos extremos, que crean túneles a través Internet.

VPN de acceso remoto. Esta es en la arquitectura que nos vamos a centrar debido a la misión que cumple la espacialidad de inteligencia toda vez que los agentes se encuentran distribuidos geográficamente en lugares diferentes; y este tipo de VPN tiene como propósito el proporcionar a los usuarios, acceso remoto a los servicios proporcionados por una intranet o extranet corporativa como es el caso del sistema integrado de información; el usuario accede a la red mediante un cliente VPN instalado en un dispositivo que le permite a este conectarse con el servidor VPN que le da acceso a los servicios y recursos de la red corporativa del sistema, a través de Internet.

Como se va a desarrollar la arquitectura de VPN de acceso remoto se implementará como medida de seguridad un elemento de filtrado de tráfico antes del concentrador de VPN para este tipo de configuración existen tres tipos de concentrador, pero solo nos vamos a basar en el que se ubica detrás del firewall o cortafuegos.

Concentrador de VPN detrás del firewall o cortafuegos. El concentrador VPN se encuentra protegido por un firewall, colocado en una DMZ por lo es necesario configurar el cortafuego para que abra los puertos que el concentrador VPN necesita, por ejemplo, los de IPSec.

4.5. Encapsulado de paquetes

Para el transporte de la información de los lugares acceso más remotos utilizaremos el *tunneling* para encapsular los paquetes de datos dentro de otro para facilitar el transporte de este, utilizando la tecnología de la red por la que viaja, con diferente esquema de direccionamiento por Internet solo agregándoles un encabezado adicional y enviando el paquete encapsulado a través de la ruta lógica, transparente a los usuarios iniciales que lo ven como una conexión punto a punto en la ruta de acceso a la red; para el proceso de tunneling seguiremos los pasos de encapsulación, transmisión - enrutamiento y desencapsulación.

Figura 8: Proceso de Túnneling. Fuente elaboración propia, octubre 2018

Cuando los paquetes encapsulados lleguen a su destino, se quita la encapsulación y se utiliza el encabezado original del paquete para enrutar éste a su destino final durante el proceso de tunneling son involucrados tres protocolos diferentes, (Delgado, 2000).

Protocolo transportado: protocolo a encapsular como TDM, PPP y SLIP.

Protocolo de encapsulamiento: empleado para la creación, mantenimiento y destrucción del túnel como encapsulamiento son L2F, L2TP, PPTP.

Protocolo portador: realiza el transporte del protocolo de encapsulamiento como IP.

Para proporcionar servicios de VPN, los túneles deben proporcionar los siguientes servicios:

- Encapsulación.
- Protección de direcciones privadas.
- Integridad y confidencialidad de los datos enviados.

4.6.Protocolo de túnneling para el sistema integrado

Los tres protocolos de túnel son los más usados para la creación de una VPN son el protocolo de túnel punto a punto (PPTP), el cual encapsula tramas de la capa de enlace de datos (PPP); el protocolo de túnel de Capa 2 (L2TP), el cual encapsula tramas de la capa de enlace de datos (PPP) y el protocolo de seguridad IPSEC, el cual encapsula paquetes IP sobre IP (Delgado, 2000).

Pero para la configuración de nuestra VPN nos basaremos en la configuración del protocolo L2TP (layer to tunneling protocol); el cual es un protocolo estándar aprobado por el IETF11 documentado en el RFC 2661, que encapsula las tramas del protocolo punto a punto PPP, para enviarse a través de redes IP, X.25, frame relay, o ATM. Fue desarrollado por Cisco y Microsoft en 1997, en base a mejorar características de los protocolos PPTP de Microsoft y L2F de Cisco (Limari, 2004).

Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN en internet. Las tramas PPP encapsuladas se pueden cifrar o comprimir. A diferencia de PPTP, la implementación de Microsoft de L2TP no usa MPPE para cifrar los datagramas PPP, se basa en IPsec en modo de transporte, analizado en el siguiente apartado, para implementar servicios de cifrado estándar que proporcionen una fuerte protección de integridad, reproducción, autenticidad y privacidad (Gabriel Diaz, 2012).

Las capacidades de L2TP son (Gabriel Diaz, 2012):

- Permite la creación de túneles únicos, para conseguir el soporte de distintos tipos de calidad de servicio.
- Permite la transmisión de mensajes IP a través de redes que no usan IP.
- Soporta direccionamiento dinámico.

- Permite trabajar conjuntamente con IPSec.

- Tanto el cliente como el servidor VPN deben ser compatibles con L2TP e IPSec; dada que la compatibilidad del cliente con L2TP está integrada en los clientes de acceso remoto de los sistemas operativos de sistemas de escritorio de Microsoft y la compatibilidad del servidor VPN con L2TP está integrada en los miembros de las familias de Windows Server 2008-2003 y se instala con el protocolo TCP/IP.

4.7. Protocolo para la seguridad de las comunicaciones

Para garantizar la seguridad en las comunicaciones para el sistema integrado de información se adaptara el protocolo IPSec (internet protocol security), el cual fue desarrollado por el IETF a principios del año 1995, y constituye un conjunto de estándares que tienen por objeto el lograr comunicaciones privadas seguras a través de redes IP mediante el uso de servicios de seguridad criptográfica, es válido para IPv4 y IPv6 el cual provee un marco que permite a dos o más partes el uso de distintos algoritmos de encriptación y métodos de autenticación en una misma sesión de comunicación. Esta flexibilidad permite incorporar esta tecnología para integrar distintos participantes, sin necesidad de dispositivos adicionales y complementarse perfectamente con la tecnología PKI (Iglesias, 2001).

Proporciona una sólida protección contra ataques a redes privadas e internet mediante la seguridad de extremo a extremo. Los únicos equipos que deben conocer que existe protección son el remitente y el receptor de la comunicación. Entre los beneficios que aporta, tenemos (Iglesias, 2001)

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.

- Ofrece al agente de inteligencia el mismo nivel de confidencialidad que dispondría en la red local del sistema, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

IPSec trabaja en la capa de red, permitiendo a un extremo remoto disponer de una dirección IP de la red del otro extremo, lo que permite a las aplicaciones y a los usuarios permanecer independientes de la infraestructura de seguridad subyacente, siendo transparentes a las mismas. Utiliza una variedad de tecnologías existentes para lograr estos objetivos, entre las que se incluyen:

- Protocolo de intercambio de claves Diffie-Hellman.
- Gestión de claves: ISAKAMP Oakley.
- Criptografía de clave pública: RSA.
- Algoritmos de cifrado simétrico: DES, 3DES, IDEA, Blowfish.
- Algoritmos resumen: MD5 y SHA-1.
- Certificados digitales: X509v3.

En cuanto a las propiedades de seguridad proporciona las siguientes:

- Autenticación de origen.
- Confidencialidad de contenido, de forma opcional.
- Integridad de los datos.
- Protección contra repetición de mensajes.

El equipo emisor protege los datos antes de la transmisión y el equipo receptor los descodifica una vez que los ha recibido. IPSec se basa en claves criptográficas (independientes de los algoritmos utilizados) y se puede utilizar para proteger equipos, sitios, dominios, comunicaciones de aplicaciones, usuarios de acceso telefónico.

Para el empleo de IPSEC se empleará uno de los dos modos existentes para la operación; el cual es el modo túnel.

Modo túnel. En el modo túnel, todo el paquete IP (datos + cabeceras del mensaje) es cifrado o autenticado y encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, VPNs a través de redes públicas o comunicaciones ordenador a red u ordenador a ordenador a través de Internet.

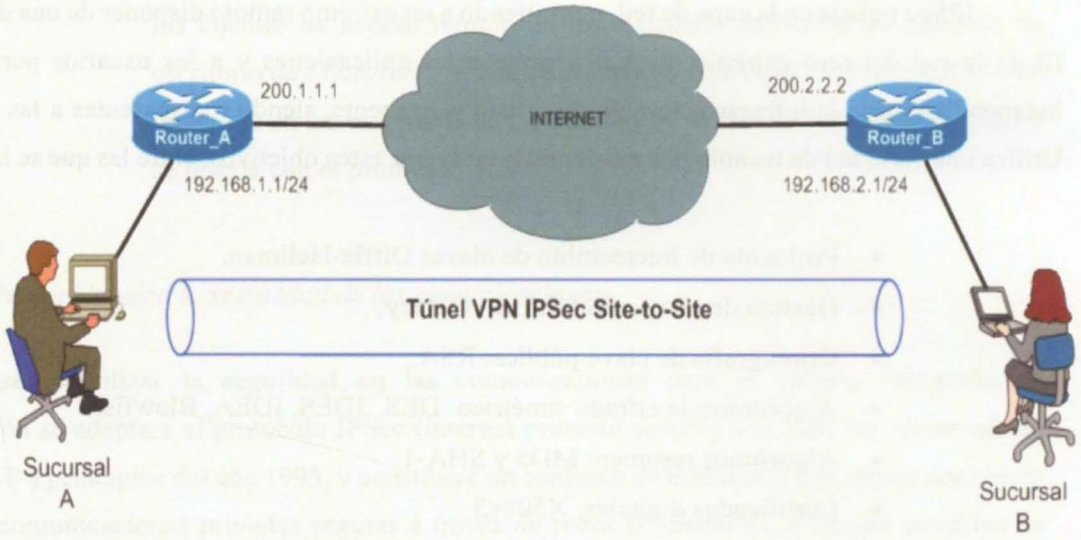


Figura 9: IPSec modo túnel, VPN sitio a sitio. Fuente: www.redescisco.net

5. Implementar terminales livianas

Al adquirir terminales livianas la información es procesada por el servidor y los usuarios tienen acceso a ella por medio de un dispositivo denominado "cliente liviano". Y lo más importante, todos los usos son controlados sobre el servidor centralizado; con esta estructura es posible el aprovechamiento de las PCs existentes ya que en el sistema no se cuenta con terminales inferiores Core I3; lo que mejora el procesamiento de la información y la agilidad con que esta se gestiona (Ayala, 2008).

6. Integración sistemas de información de inteligencia

El sistema de inteligencia a desarrollado diferentes sistemas de información en bases de datos estructuradas y no estructuradas; el objetivo es que el sistema integrado de información

permita la consulta y gestión de toda la información alojada en los servidores de las diferentes unidades de inteligencia.

7. Desarrollo del sistema integrado de gestión documental de inteligencia

Mediante la implementación del proceso de actualización, corrección y retiro de datos de archivos en los sistemas de información de inteligencia; en la actualidad la gestión documental se desarrolla por medio de correo electrónico de un único dominio; con la política de 0 papel, toda la gestión documental debe realizarse en línea por medio de los canales seguros. Para el proceso de inteligencia la gestión de documentos tanto públicos como clasificados es compleja debido a los requisitos documentales que nos exige la Ley estatutaria 1621 de 2013 donde nos ordena en el artículo 28.

Centros de protección de datos de inteligencia y contrainteligencia

Cada uno de los organismos que desarrolla actividades de inteligencia y contrainteligencia tendrá un Centro de Protección de datos y archivos de Inteligencia y Contrainteligencia (CPD). Cada Centro tendrá un responsable que garantizará que los procesos de recolección, almacenamiento, producción y difusión de la información de inteligencia y contrainteligencia estén enmarcados en la Constitución y la Ley. Para ello se llevarán a cabo los talleres de capacitación necesarios dentro de cada organismo.

Paro lo cual es necesario la implementación de un sistema de gestión documental que cubran las actividades necesarias para la gestión y organización de los propósitos establecidos en la guía No. 6 de la política de 0 papel en la gestión pública donde nos establece que en el SGDEA (sistema de gestión de documentos electrónicos de archivo) o ERMS (Electronic Records Management System) para lo cual es necesario la adecuación de un software especializado, que los conserven y les garanticen su valor probatorio y hacer que estén disponibles para su utilización. Los sistemas de archivo garantizan el mantenimiento y la conservación de la autenticidad,

fiabilidad y accesibilidad de los documentos a lo largo del tiempo. (Archivo General de la Nacion Colombia, 2018)

Para cumplir con lo anterior los sistemas deben cumplir con los requisitos dispuestos por la ley; para lo cual el comando del Ejercito promulgo el procedimiento 193 de ACR en el año 2017 donde establecen los criterios a tener en cuenta para el proceso de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia; adicionalmente esta la directiva de Ejercito 01016 del 2016 donde se emiten órdenes para la gestión documental para el ejército nacional; estableciendo la estructura de como documentar, mantener y promulgar procedimientos y prácticas de gestión de documentos de archivo que aseguren y cubran las necesidades de información, evidencia y de rendición de cuentas.

Para dar cumplimiento a lo anterior el sistema debe integrar una aplicación que permita la digitalización de la información que se encuentre física; permitiendo su gestión dentro las bases de datos estructuradas y no estructuradas, permitiéndole al analista contar en su terminal con toda la información disponible sobre un objetivo específico.

8. Fortalecimiento la defensa del sistema mediante la estrategia de defensa en profundidad.

Como es sabido uno de los principales blancos a los que va a estar expuesto el sistema integrado de información es a los ataques intrusivos, en razón a que dentro de los servidores del sistema estará alojada la información más relevante para la defensa nacional como es la información de inteligencia; también contempla las fuentes, esto último lo que supondría un grave impacto debido a que las fuentes quedarían expuestas y su seguridad correría un gran riesgo, por eso las medidas que se tomen en cuanto a la defensa deben ser proactivas y efectivas; es por esto que para este sistema se tiene contemplado el empleo de una de las estrategias de defensa más efectiva en el mundo como lo es la Defensa en Profundidad.

La implementación de la estrategia lo basaremos en la introducción de múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y así minimizar el impacto de fuga de información (CCN-STIC-400, 2013).

Dentro del sistema integrado de información se contemplara una arquitectura que constituya un entorno de ejecución donde el sistema pueda controlar los servicios con el fin de reducir y dificultar la probabilidad de que una entrada maliciosa alcance el sistema, reduciendo al mínimo la exposición de las propias vulnerabilidades tanto del software como del hardware al mundo exterior, minimizando la visibilidad externa de los componentes principales de confianza, reduciendo su exposición a las amenazas y aislando los componentes no confiables de forma que su ejecución se vea limitada y sus malos comportamientos no amenacen la operación confiable de los demás componentes del sistema.

Para desarrollar esta estrategia de defensa del sistema, se propone un enfoque defensivo que implanta protecciones o mecanismos de seguridad en todos los niveles del sistema o capas del modelo open systems interconnection (OSI); las medidas de seguridad a implementar en cada capa podrían variar en función del entorno de operación del sistema.

A continuación, se listan las medidas para tener en cuenta para las diversas capas (Viveros, 2012).

Capa de aplicación

Se aplicará a todos los dispositivos de la capa de aplicación como cortafuegos, proxy reverso, y sistemas de prevención de intrusiones de host que bloqueen las entradas maliciosas conocidas y problemáticas antes de que llegue al software; adicionalmente se configuraran otros mecanismos como los métodos de encriptación, control de acceso, autenticación y bastionados de aplicaciones.

Capa de transporte

Se establecerá un mecanismo de cifrado como transport layer security (TLS).

Capa de red

Se configurarán dispositivos de seguridad de red que protejan y dificulten las acciones de los ciberatacantes tales como cortafuegos, sistemas de protección de intrusiones (IDS/IPS) de capa de red, sistemas de gestión y correlación de eventos de infraestructura (SIEM).

Capa física

Se establecerán plataformas virtuales "sandboxes" que proporcionen un entorno aislado de ejecución para los componentes no confiables evitando que comportamientos maliciosos afecten a los componentes confiables; adicionalmente se configurara la arquitectura de alta disponibilidad y sistemas de recuperación completa de las maquinas.

9. Controles críticos de seguridad para una defensa efectiva del sistema.

Para garantizar la seguridad del sistema nos basaremos en los controles determinados por la SANZ (SANZ, 2019), tomando en cuenta las áreas de control definidas en el documento de referencia y se describen a continuación.

Control 1: Inventario de dispositivos autorizados y no autorizados; es decir los procesos y herramientas necesarias para realizar el seguimiento, prevención y control del acceso a la red por dispositivos (ordenadores, equipos de red, impresoras, etc.) basándose en su inclusión en un inventario de existencias.

Control 2: Inventario de software autorizado y no autorizado; se hace referencia a los procesos y herramientas necesarias para realizar el seguimiento, prevención y control de la correcta instalación y ejecución del software en los ordenadores y servidores de la red

basándose en las existencias definidas en el inventario de software aprobado por el Batallón de seguridad de la información para la maquina concreta.

Control 3: Bastionado del hardware y software de los ordenadores portátiles de los agentes de campo; este control se efectuara sobre estaciones de trabajo y servidores que desarrollan los procesos y contienen las herramientas necesarias para realizar el trabajo de campo en inteligencia de las cuales se les desarrollara un seguimiento, control, prevención y corrección de los defectos y debilidades de las configuraciones del hardware y software de dispositivos móviles, portátiles, estaciones de trabajo, y servidores sobre la base de un proceso de control de configuración debido a su exposición a amenazas latentes.

Control 4: Evaluación continua de vulnerabilidades y su remediación. Este proceso se desarrollara con el fin de detectar, prevenir y corregir debilidades de seguridad de las configuraciones de dispositivos respecto a una base de datos de vulnerabilidades; poco después de que una vulnerabilidad es descubierta, los atacantes crean un exploit para lanzarlo contra sus blancos de interés en este caso y teniendo en cuenta la información contenida en los servicios del sistema de inteligencia son un blanco apetecible no solo por atacantes particulares, sino también por estados que ven en Colombia una posible hipótesis de guerra y que no escatimarían recursos en la consecución de herramientas que permitan explotar estas vulneraciones, se hace necesario la implementación de estos controles; dado que cualquier retraso importante en actualizar un software con vulnerabilidades criticas proporcionara una oportunidad a los atacantes para adquirir el control de la máquina.

Actualmente están disponibles gran cantidad de escáneres de vulnerabilidades (Open VAS, Nessus, etc.) que valoran la configuración de seguridad de sistemas y comparan los resultados del examen actual con los exámenes previos para determinar cómo han cambiado las vulnerabilidades con el tiempo y en el entorno.

Control 5: Uso controlado de privilegios administrativos. Este control comprende los procesos y herramientas necesarias para realizar el seguimiento, control, correcto uso,

asignación y configuración de los privilegios administrativos de ordenadores, servidores, portátiles, dispositivos de redes y aplicaciones.

Control 6: Mantenimiento, seguimiento y análisis de registros de eventos de auditoría de seguridad. Con este control se desarrollaran los procesos y herramientas necesarios para detectar, prevenir y asegurar el correcto uso de los sistemas de información basándose en auditorias diarias de los eventos que son considerados importantes o pueden afectar la seguridad del sistema; en razón a que a menudo, las aplicaciones de registros de eventos proporcionan las únicas pruebas de un ataque exitoso; para nuestro caso y dada la importancia estratégica del sistema se recomienda guardar los registros de auditoría con propósitos de mantenimiento y no como medio de obtener datos de ataques ocurridos; para esto se deben registrar los eventos producidos diariamente y disponer de personal responsable de evaluarlos.

Control 7: Protección de navegadores web y correo electrónico. Con este control se busca minimizar los riesgos relacionados con el uso de navegadores web y de correo electrónico por medio de procesos y herramientas necesarias para este fin en razón a que estos dos vectores son puntos de entrada muy comunes para ataques muy diversos al permitir la interacción directa de los usuarios con sitios externos de distinta procedencia; orientando los controles a limitar al máximo la funcionalidad expuesta por los usuarios a la estrictamente necesaria y a definir dominios de confianza para web y correo electrónico.

Control 8: Defensas contra malware. Comprende los procesos y herramientas necesarias para detectar, estudiar, caracterizar, prevenir y eliminar la instalación y ejecución de software malicioso en los dispositivos de la red; debido a que este software malicioso es una de las amenazas y peligros más importantes de Internet ya que los atacantes usan el malware contra los usuarios finales vía Web, anexos de correo electrónico, dispositivos móviles y otros vectores, mediante el empleo del código malicioso el cual puede alterar el contenido de un sistema, capturar datos confidenciales, y propagarse a otros sistemas.

Control 9: Limitación y control de los puertos, protocolos y servicios. Con este control se desarrollan los procesos y herramientas necesarias para realizar el seguimiento, control, limitación y correcto uso de puertos, protocolos, y servicios de los dispositivos conectados a la red; debido a que uno de los vectores que los atacantes buscan en la red, son servicios accesibles y vulnerables susceptibles de obtener su control mediante el lanzamiento de un exploit; muchos paquetes de software instalan servicios automáticamente y los lanzan como parte de la instalación de la aplicación, cuando esto ocurre, el software no informa al usuario de qué servicios han sido activados, para esto los atacantes usan herramientas de escaneo de puertos, para determinar qué servicios están escuchando en la red, y así determinar qué puertos están abiertos, los escáneres pueden identificar la versión del protocolo y servicio, los sistemas defensivos del sistema deben estar en la capacidad de identificar cualquier nuevo puerto en la red abierto no autorizado.

Control 10: Capacidad de recuperación de datos. En este control se desarrollan los procesos, herramientas y metodología, de demostrado funcionamiento, necesarias para la realización de copias de seguridad y recuperación de la información crítica, en el momento oportuno.

Control 11: Configuraciones seguras para los dispositivos de red, firewalls, routers y switches. En este control se seguirán los procesos necesarios para realizar el seguimiento, control, prevención y corrección de las debilidades y defectos en las configuraciones de seguridad en los dispositivos de la red, como cortafuegos, routers y switches, basándose en los procesos de control de configuración y control de cambios.

Control 12: Defensa de los límites de la red. En esta fase se busca instalar las herramientas y establecer procesos necesarios para detectar, prevenir y corregir el flujo de la información entre redes de diferente nivel de clasificación, desde el enfoque de la seguridad de los datos con el fin de controlar el flujo del tráfico a través de fronteras de la red y buscar ataques y evidencias de máquinas comprometidas, para lo cual se debe disponer de defensas en varias capas; en estos límites deben constar de cortafuegos, proxies, zona desmilitarizada (DMZ)

y sistemas IDS/IPS de red; con el fin de evaluar estos sensores con escáneres de vulnerabilidad cada determinado tiempo.

Control 13: Prevención de fuga de datos (data leak prevention). Se busca establecer los procedimientos empleando las herramientas necesarias para realizar el seguimiento, control, prevención y correcta transmisión de datos y su almacenamiento, en función de su contenido y la clasificación asociada a cada informe.

Control 14: Acceso controlado, basado en la necesidad de conocer (need to know). Este proceso demanda la integración de personal del comando de contrainteligencia y de seguridad militar con el fin de establecer los procesos y las herramientas necesarias para realizar el seguimiento, control, prevención y acceso seguro a la información de acuerdo con la determinación formal de la necesidad, proporcionalidad y la pertinencia del acceso a los datos sensibles, basándose en los niveles de clasificación establecidos en las directivas ministeriales para tal fin, estableciendo los niveles de clasificación a cada persona, máquina o aplicación.

Control 15: Control de dispositivos inalámbricos. Comprende los procesos y herramientas necesarias para realizar el seguimiento, control y monitorización de las condiciones de seguridad de las LAN inalámbricas de ser necesarias; en razón a que por seguridad de la información estas deben ser las mínimas.

Control 16: Monitorización y control de cuentas de usuarios. En este control se verificará por medio de herramientas el uso que los agentes le estén dando a las cuentas de correo realizando las verificaciones necesarias de seguimiento, control, prevención y correcto uso de estas, el sistema integrara un control activo de cuentas de manera que se pueden listar cuentas usuarios inactivas, así como de crearlas cuando se tiene un nuevo usuario en el sistema.

Control 17: Formación de seguridad. El factor humano es el más importante para el sistema y de igual manera es el más vulnerable por tal razón en este proceso se desarrollarán

los procesos y herramientas necesarias que garanticen que el sistema dispone de técnicos de seguridad con las habilidades y formación adecuadas, incluyendo un plan integrado de formación y evaluación de estos.

Control 18: Seguridad de las aplicaciones software. Para la adquisición o desarrollo de nuevo software se desarrollaran los procesos y herramientas necesarias para detectar, prevenir y corregir los defectos de seguridad en los mismos, en razón a que un elemento importante del ciberespacio es el software o las aplicaciones que proporcionan los servicios, utilidades y funcionalidades; más sin embargo, estas aplicaciones presentan vulnerabilidades que pueden ser explotadas por atacantes de diversa índole, desde aficionados hasta organizaciones de cibercriminal o incluso para este caso estados en acciones de ciberguerra, utilizándolas como plataformas de ataque para comprometer los sistemas y redes de la organización; para evitar la aparición de vulnerabilidades en el software o las aplicaciones, se aplican una serie de técnicas según la fase del ciclo de vida, entre las que podemos destacar:

- Análisis de riesgos. Casos de abuso.
- Análisis estático de la seguridad del código fuente empleando herramientas de análisis de código fuente que informan de los defectos de seguridad.
- Análisis dinámico con pruebas de seguridad basadas en el riesgo y un test de penetración (hacking "ético") de la aplicación en tiempo de ejecución.

Control 19: Capacidad de respuesta a incidentes. Comprende los procesos y herramientas necesarias para asegurar que una organización tenga un plan correctamente evaluado y con personal con la adecuada formación para poder responder ante eventos adversos o amenazas e incidentes de seguridad.

Control 20: Pruebas de penetración y ejercicios. Comprende los procesos y herramientas necesarias para simular ataques contra una red al objeto de validar la seguridad en conjunto de una organización. Los atacantes obtienen acceso a redes y sistemas a través de ingeniería social y explotando las vulnerabilidades del software y hardware. Una prueba de

penetración supone imitar las acciones de atacantes para determinar qué clase de acceso puede conseguirse e identificar los riesgos de seguridad.

10. Establecer los mecanismos de detección para la defensa

En este aparte se determinarán los mecanismos básicos para optimizar el funcionamiento de los sistemas de defensa que se deben desplegar para la protección del sistema.

10.1. Firewall o Cortafuegos

Para garantizar la seguridad de la red se instalará un firewall o cortafuegos el cual estará ubicado entre las redes con la política de control de acceso sobre las comunicaciones entre las redes, basándose una política de seguridad establecida por la directiva de seguridad de la información; teniendo en cuenta (Suehring, 2006).

Todo el tráfico entre la red confiable y la que no, y viceversa, debe pasar por el cortafuego, con el fin que este puede establecer el control sobre el tráfico que pasa por él; sólo el tráfico autorizado, definido por la política de seguridad, es permitido, el restante es denegado.

El cortafuego será la barrera de protección encargada de proteger la red confiable de una que no lo es, es decir va a controlar todo el tráfico que llega desde Internet, y será el dispositivo central de protección perimetral del sistema.

Aprovechando la capacidad que tendrá este que toda la información entrante y saliente pase a través del dispositivo, se configuraran los servicios de seguridad adicionales como el cifrado del tráfico de la red mediante la implementación de las VPN; para el sistema instalaremos los siguientes tipos de cortafuegos.

Cortafuegos de capa de red; se encargará del filtrado en función de la dirección de origen, destino y puerto de cada paquete IP, manteniendo la información respecto del estado de las conexiones que están activas a través de él, se desarrollara mediante el filtrado de direcciones y

puertos, trabajando en las capas de transporte y de red del modelo OSI; estará conectado a ambos perímetros (interior y exterior) de la red con el fin que pueda realizar las funciones de:

a. *Filtrado de Paquetes.* De la misma manera que los routers, implementara filtros y reglas basadas en políticas establecidas previamente y a listas de control (ACL) de acceso filtrando los paquetes en base a los siguientes criterios:

   - Dirección IP de origen y de destino.
   - Puerto TCP–UDP de origen y de destino (Protocolos utilizados).

   Con el filtrado de paquetes mediante puertos y protocolos se podrá establecer qué servicios estarán disponibles al usuario y por qué puertos; como, por ejemplo, se puede permitir leer el correo (SMTP 25), pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

b. *Inspección de paquetes (stateful).* Cada paquete que circule por la red será inspeccionado, así como también su procedencia y destino, adaptando las reglas básicas de firewall para acomodarse a las necesidades específicas de cada protocolo, manteniendo un registro de las conexiones, las sesiones y su contexto, este módulo estará ubicado entre la capa de transporte y red.

   Con el cortafuegos en la capa de aplicación, filtran por características propias de un protocolo, como puede ser peticiones DNS o HTTP, bloqueando o cambiando el resultado; adicionalmente se configurará un cortafuegos de aplicación web (WAF), para no permitir el tráfico directo entre redes, manteniendo una elaborada auditoría y registro del tráfico que pasa a través de ellos, adicionalmente con la configuración él se estará en capacidad de:

   - Traducción de direcciones NAT.
   - Monitorización y análisis de registros y eventos.
   - Realización de estadísticas del ancho de banda consumido por el tráfico de la red.

- Generación de alarmas.
- Reverse Path Forwarding (Filtrado de camino inverso) permite verificar el origen de una dirección que entre por una determinada interfaz.
- Rutas de descarte. Permite enviar el tráfico especificado a una interfaz virtual de descarte.

A pesar de que los firewalls no realizan inspección de contenidos, por lo que no son eficaces contra la filtración de software o archivos infectados con virus, se debe configurar la máquina, donde se aloja el firewall, de un antivirus apropiado.

10.1.1. Filtrado de paquetes

La instalación de un cortafuegos en sí; no es la solución completa, si pensamos en un cortafuegos, la idea que en primer lugar viene a nuestra mente es un dispositivo que permite definir reglas para bloquear tráfico. En realidad, esto es el mecanismo de filtrado de paquetes, que es sólo una parte de lo que constituye un cortafuegos.

Con el dispositivo de filtrado de paquetes se definirán los selectores de tráfico, que delimitan el conjunto de tráfico de red sobre el que el sistema va a actuar, sobre los que actuarán las acciones disponibles en el cortafuegos, que genéricamente serán aceptar o rechazar.

En un selector de tráfico, se incluirán los campos de cualquier capa de red, para así, poder incluir la dirección IP origen o destino, el protocolo de transporte, los números de puerto o las interfaces de entrada o salida; como también incluir los módulos para que soporten los protocolos de capa de aplicación para poder extender el filtrado a esos protocolos, teniendo en cuenta incluso el propio funcionamiento del protocolo.

Es importante tener en cuenta que el router va a estar en el cortafuegos, como una router de protección (screening router), con el fin que aparte de analizar las direcciones IP de destino de cada paquete y de acuerdo con las tablas de encaminamiento, determinar por qué interfaz debe salir el paquete, se requiere que además este realice un análisis exhaustivo de cada paquete con el

que determine no sólo si puede sacarlo (es decir, si hay un regla de encaminamiento que aplica al paquete) sino también si debe sacarlo.

10.2. Servidor PROXI

Un servidor proxy es por definición un elemento que actúa de intermediario entre un cliente y un servidor, en nuestro caso cuando un cliente (agente de inteligencia) que quiera acceder a un servidor, se impondrá el uso de un proxy, el cliente no conectara directamente con el servidor, sino que debe conectar con el servidor proxy, y será el servidor proxy el que se comunica con el servidor, el obtendrá una respuesta, la cual procesara y la devolverá al cliente; durante el procesamiento se deben incluir acciones diversas que dependerán del cometido para el que se desplego el servidor proxy: como el caché, control de contenidos, seguridad, funcionando como el Gateway de la capa de aplicación.

La idea del servidor proxy es la de controlar la forma en que usan los diferentes protocolos, controlar las opciones del protocolo, contenidos intercambiados y formas de acceso; con el fin de proteger a los servidores frente a peticiones maliciosas y a los clientes de respuestas maliciosas; con este mecanismo el administrador del sistema va a tener un control más a fondo de cada protocolo (Wang, 2004).

10.3. Mecanismo de prevención de fuga de información

Para prevenir la fuga de información se configurara un DLP (data loss Prevention) con el fin de proteger información sensible y proporcionar una perspectiva del uso de contenidos dentro del sistema, teniendo en cuenta que no toda la información del sistema se encuentra clasificada, con la configuración del DLP el sistema establecerá los distintos tipos de información que maneja, permitiendo su clasificación y la gestión de contenidos (Gomez, 2003).

Adicionalmente podemos distinguir entre productos que incorporan algún tipo de capacidad DLP, aunque su propósito principal sea otro por ejemplo, el gestor documental y aquellas

soluciones o suites específicas para DLP, en función de los recursos y necesidades que vayan surgiendo durante la implantación del sistema; es importante resaltar que con la solución del DLP se podrá efectuar un control efectivo contra las malas prácticas del personal que integra el sistema como por ejemplo, intercambios de información sensible con terceros sin utilizar cifrado y contra descuidos o errores, pero mucho menos contra actividades maliciosas (Galindo, 2009).

10.3.1. Implementación del DLP

Al momento de implementar la solución DLP tenemos dos posibilidades, la primera es la opción de aprovechar la funcionalidad DLP que pueden ofrecer herramientas como la plataforma de correo corporativo o un gestor documental o bien podemos optar por desplegar una solución específica.

Para el sistema integrado de información la solución de DLP debe permitir capacidades como:

- Control centralizado
- Creación de políticas
- Definición de flujos de trabajo
- Verificaciones específicas orientadas a la protección de la información y los distintos contenidos.

La instalación de esta herramienta en el sistema estará orientada a resolver los problemas tanto técnicos como desde el punto de vista del flujo de información derivados de la inadecuada protección y clasificación de la información y los documentos.

Por otro lado, los productos que incorporan funcionalidades de DLP nos ofrecerán las capacidades técnicas de detección e incluso restricción de ciertos contenidos, pero no ofrecen una funcionalidad integrada de protección de la información que está alineada con las políticas del sistema.

En el caso del sistema la solución para le adecuación del DLP será una solución dedicada, ya que la responsabilidad de clasificación y protección de los contenidos suele recae en el personal de la unidad de protección de datos y archivos, los cuales se encuentran fuera del área de TI.

10.3.2. Funcionamiento de la solución DLP

Para tener claro el funcionamiento de la solución DLP, se debe distinguir entre contenido y contexto, la solución DLP debe ser capaz de extraer elementos de información de cada documento o pieza de información intercambiada, en otras palabras, entender el contenido, pero también debe tener en cuentan el contexto en que se sitúa origen, destino, tamaño, remitentes y destinatarios, fechas y cualquier otro tipo de metadatos, el contenido y el contexto serán igual de importantes para la definición de políticas del DLP.

10.3.3. Análisis de Contenido

El primer paso que debemos tener en cuenta es la extracción del contenido, el motor de análisis debe ser capaz de extraer e interpretar el contenido, esto es inmediato si estamos tratando con ficheros de texto, pero es más complicado cuando tratamos con ficheros binarios, es aquí donde incluimos también la capacidad de extraer documentos incrustados dentro de otros, como por ejemplo, analizar una hoja de cálculo Excel incluida dentro de un documento Word que a su vez se distribuye comprimida, es necesario la inclusión de las herramientas de análisis y extracción de información para los distintos tipos de archivo y las distintas codificaciones posibles, una vez hemos extraído los contenidos, el siguiente paso es analizar el mismo, por medio de las técnicas de análisis como las siguientes:

Análisis basado en reglas. Analiza el contenido buscando patrones o reglas específicas. como, por ejemplo, podemos citar coordenadas de lugares donde se han reportado sucesos de relevancia para la inteligencia, marcaciones de los sistemas de radiogoniometría u otra información específica; esto permitirá realizar una detección rápida de ciertas situaciones, aunque también está sujeta a una tasa alta de falsos positivos y no es útil para implementar políticas complejas.

Relacionada con la anterior, podemos indicar la técnica de búsqueda de coincidencias con los resultados almacenados en una base de datos, en este caso, no se buscará una correspondencia con un patrón, sino una coincidencia exacta que permitirá un manejo adecuado de la información.

Coincidencias exactas entre ficheros. Se dispondrán de una lista de hashes de un conjunto de ficheros y cada vez que se localice un nuevo fichero el sistema comprobara si su hash corresponde con alguno de los almacenados.

Frente a la técnica anterior, se podrán aplicar técnicas que analizan el contenido de los ficheros, así es posible buscar coincidencias parciales del texto de un documento en otros y de esta manera, no sólo protegemos el sistema de una filtración del documento íntegro sino también se podrá detectar la aparición de fragmentos del documento dentro de correos electrónicos, mensajes de mensajería instantánea o dentro de otros documentos incluso, se suelen emplear mecanismos de análisis lingüístico o hashes parciales de distintos segmentos del fichero original permitiendo proteger todo tipo de documentos con información no estructurada, pero es necesario definir inicialmente el conjunto de ficheros cuyo contenido se debe proteger.

Análisis estadístico permiten analizar un conjunto de documentos para encontrar contenidos que sean parecidos o estén relacionados con contenidos protegidos, esta técnica es apropiada para el contenido no estructurado, en particular cuando el sistema maneja un conjunto de documentos lo suficientemente grande como para que no sea práctico emplear la búsqueda de coincidencias parciales o porque no sea fácil aislar documentos individuales para buscar.

10.4. Sistema de detección de intrusiones (IDS/IPS)

Por la complejidad de la información que maneja el sistema de inteligencia adicional a los controles previos es necesario la instalación de un sistema de detección de intrusos que nos permita detectar actividades inapropiadas, incorrectas o anómalas desde el exterior al interior del sistema permitiendo:

- Inspeccionar el tráfico de la red buscando posibles ataques.

- Controlar el registro (logs) de los servidores para detectar acciones sospechosas
- (tanto de intrusos como de usuarios autorizados).
- Mantener una base de datos con el estado exacto de cada uno de los archivos (integrity check) del sistema para detectar la modificación de estos.
- Controlar el ingreso de cada nuevo archivo al sistema para detectar Caballos de Troya o semejantes.
- Controlar el núcleo del Sistema Operativo para detectar posibles infiltraciones en él, con el fin de controlar los recursos y acciones de este.
- Avisar al administrador de cualquiera de las acciones mencionadas.
- Prevenir comportamientos injustificados o maliciosos por usuarios internos.
- Detectar en "tiempo real" para mitigar o anular el impacto de este.
- Detectar comportamientos o acciones previas a la realización de un ataque, como, por ejemplo: Escaneo de Puertos.

El IDS del sistema estará compuesto por:

- Fuentes de información, de las cuales se extraen los distintos eventos que serán analizados.
- Motor de Análisis, encargado de examinar los eventos recopilados para identificar signos de intrusiones.
- Componentes de Respuesta, para ejecutar las acciones que se definan como reacción ante una intrusión detectada.

Un IDS (figura 10) puede tener una arquitectura muy variada, en función de la implementación de los componentes mencionados. Podemos agrupar estas posibilidades en función del tipo de fuentes de información del que se alimenta el IDS.

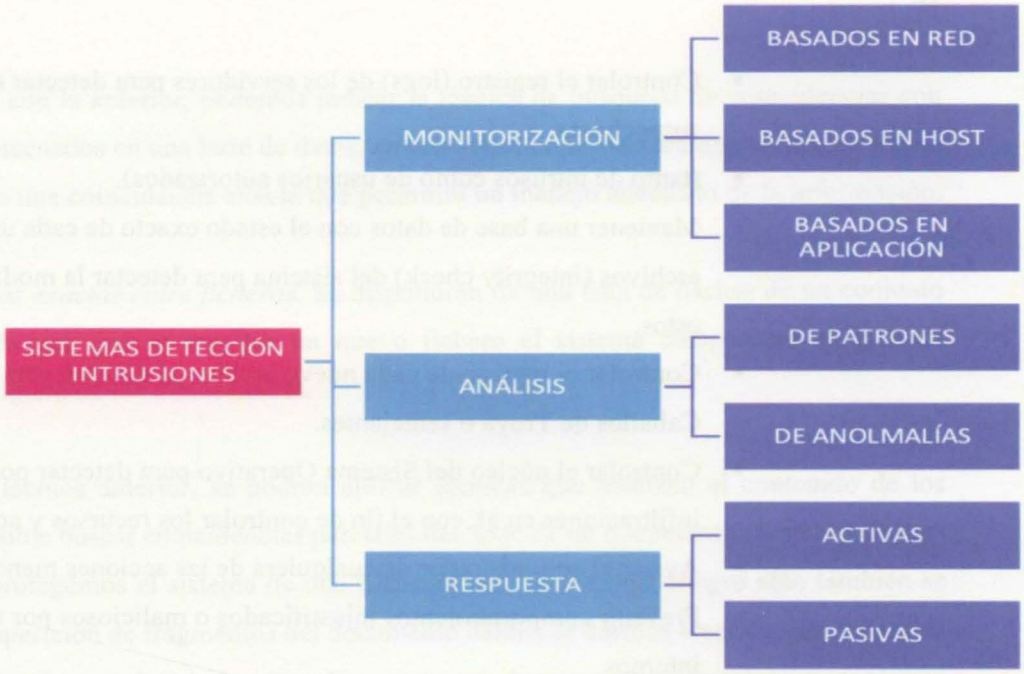


Figura 10: Arquitectura de un IDS. (Gomez, 2003)

El IDS (figura 11) requerido para el sistema es el basado en red, podemos ver un ejemplo de arquitectura básica de un IDS basado en red.

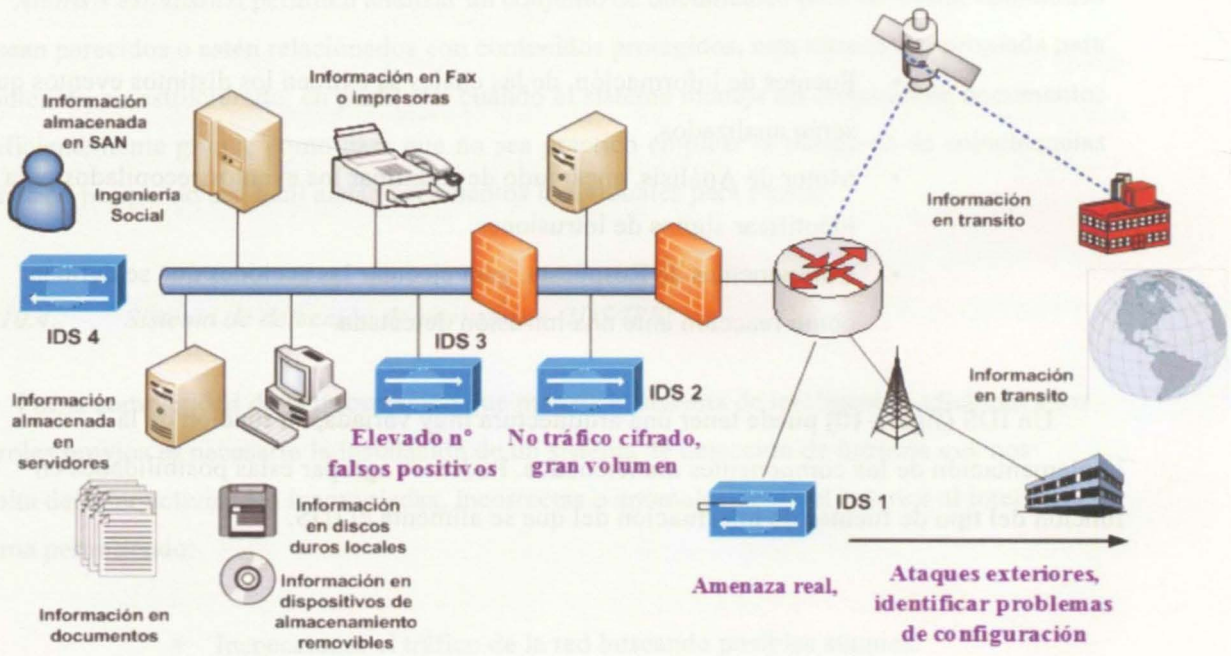


Figura 11: IDS de red. Gómez, 2003

El IDS-1 se encargaría de detectar y avisar del escaneo de puertos, y si es del tipo IPS reactivo podría enviar un mensaje al dispositivo de gestión de logs de la organización para que genere la alerta correspondiente al administrador de seguridad. El IDS-2 se encargaría de vigilar la zona desmilitarizada y analizar el tráfico que reciben los servidores instalados en esa zona. Los otros dos IDS se encargarían de la red interna, el IDS-3 de la totalidad de la red, y el IDS-4 de una subred (Gomez, 2003).

II. PROTOCOLOS DE SEGURIDAD

Con el fin de garantizar el correcto funcionamiento del sistema integrado de inteligencia se deben seguir los protocolos para cada área que se describe a continuación.

1. Operadores del sistema

Control

Las responsabilidades y funciones del personal que interactúa con el sistema como analistas, agentes de inteligencia, técnicos y demás personal que hace parte del sistema de inteligencia e interactúa con él se les debe definir y documentar sus roles en concordancia con la política de seguridad de la información de la organización (Organización Internacional de Normalización, 2017).

Lineamientos para la implementación

Los roles y responsabilidades que debe cumplir el personal del sistema deben contemplar:

a) Implementar y actuar en concordancia con las políticas de seguridad de la información.

b) Proteger la información contra el acceso no autorizado, divulgación, modificación o destrucción.

c) Establecer protocolos de seguridad para el personal ajeno al sistema.

d) Verificar que cada persona tenga una responsabilidad asignada dentro del sistema.

e) Establecer un canal de comunicación ágil que permita reportar eventos de seguridad o eventos potenciales u otros riesgos de seguridad para el sistema en tiempo real.

f) El personal que será encargado de la seguridad debe ser sometido a todas las pruebas de confiabilidad que establecidos por el Comando de Contrainteligencia del Ejercito.

g) Se debe establecer claramente los roles y responsabilidades para las personas que no son parte del sistema pero que por necesidades del servicio deben trabajar para nosotros.

h) Los usuarios y administradores del sistema deben ser conscientes de sus responsabilidades de seguridad, ya que ellos pueden causar un daño considerable al sistema.

2. Responsabilidades del mando

Control

La persona que tenga bajo su comando el sistema integrado de información de inteligencia debe garantizar que el personal que va a interactuar con el sistema cumpla con los siguientes lineamientos (Organización Internacional de Normalización, 2017):

Lineamientos para la implementación

a) Que el personal este informado sobre su rol y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información.

b) Que el personal reciba lineamientos para establecer las expectativas de seguridad de su rol dentro del sistema.

c) Que el personal esté motivado para cumplir con las políticas de seguridad toda vez que un personal motivado tiene más probabilidades de ser más confiable y causar menos incidentes de seguridad de la información.

d) lograr un nivel de conciencia sobre seguridad relevante para sus roles y responsabilidades dentro dl sistema.

e) Que el personal cumpla con los términos y condiciones del cargo, los cuales incluyen la política de seguridad de la información del Ejercito y los métodos de trabajo apropiados.

f) Mantengan un nivel de entrenamiento y capacitación alto y actualizado durante su asignación al cargo.

3. *Capacitación del personal que administra el sistema integrado de información.*

Control

Los administradores del sistema, y cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

Lineamientos para la implementación

a) La capacitación y el conocimiento debieran comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad del sistema antes de otorgar acceso a la información o servicios.

b) La capacitación constante debiera incluir los requerimientos de seguridad, responsabilidades legales y controles estructurales, así como la capacitación en el uso correcto de los medios de procesamiento de información; por ejemplo, procedimiento de registro, uso de paquetes de software e información sobre los procesos disciplinarios a que se viere inmerso al incumplir los protocolos de seguridad.

c) Las actividades de entrenamiento y capacitación deben ser adecuados para el rol, responsabilidades y funciones de la persona, incluyendo información sobre amenazas conocidas, a quién contactar para mayor consultoría sobre seguridad y los canales apropiados para reportar los incidentes de seguridad de información.

d) La capacitación para aumentar la conciencia y conocimiento tiene como objetivo permitir a las personas reconocer los problemas e incidentes de la seguridad de la información, y responder de acuerdo con las necesidades de su rol en el trabajo.

4. Mantenimiento de equipo

Control

Se debe mantener correctamente el equipo para asegurar su continua disponibilidad e integridad.

Lineamientos para la implementación

Se deben considerar los siguientes lineamientos para el mantenimiento de equipo (Organización Internacional de Normalización, 2017):

a) El equipo se debe mantener en concordancia y especificaciones de servicio recomendados en el diseño del sistema.

b) Sólo el personal de mantenimiento de la institución está autorizado para llevar a cabo las reparaciones y dar soporte al equipo.

c) Se debe llevar una bitácora con los registros de todas las fallas sospechadas, fallas reales, mantenimiento preventivo y correctivo.

d) Cuando un equipo se programe para mantenimiento se deben efectuar los protocolos y controles necesarios, teniendo en cuenta, si su mantenimiento es realizado por el personal del sistema o por personal ajeno al mismo, revisando la información confidencial del equipo y resguardando la misma.

5. *Vulnerabilidades, ciberataques y alternativas de seguridad*

Los sistemas de información como se ha indicado presentan múltiples eventos de ciberseguridad que pueden alterar el funcionamiento racional del sistema y el flujo de información; a continuación, se describen algunos riesgos informáticos y de la información (no exhaustivos) y los posibles controles que deben ser implementados para reducir los niveles de exposición al riesgo (Organización Internacional de Normalización, 2017).

Riesgos Informático y de la información	**Posible control**
Scanning	Sistemas criptográficos, transporte seguro de información
DoS / DDoS	Sistemas anti-DoS, control de entrada/salida, monitoreo, controles en el firewall
Acceso no autorizado	Control de acceso, proceso de identificación, autenticación y autorización, control de roles y perfiles, control de contraseñas (fuertes), control en el acceso remoto.
Phishing	Control en el sitio Web, aseguramiento de la plataforma Web
Suplantación	Control de acceso en la autenticación y autorización
IP Spooging	Monitoreo de redes

Password Craking	Criptografía, monitoreo periódico de accesos.
Ingeniería social	Planes de cultura en seguridad
Ataque de hombre en el medio – MiTM	Criptografía
Robo de datos desde/hacia móviles	Aseguramiento de móviles, cifrado, autenticación
Inyección de código	Instalación de parches, control de campos de entrada y salida, aseguramiento de la base de datos.
Alteración de información	Control de acceso, monitoreo de integridad de datos y comandos sensibles.
Malware / Ransonware	Antivirus, anti-spy, control de acceso, control de memorias USB, control de conexiones remotas por fuera del firewall
Robo de información	Criptografía, registro de ingreso.

Tabla 1: Riesgos y controles sobre la información. Fuente: elaboración propia, octubre 2018

Capítulo III

Implementación, verificación y evaluación del sistema

I. IMPLEMENTACIÓN

Para la implementación del sistema integrado de información es necesario seguir un grupo de políticas y protocolos para la implementación del sistema de manera que permita la gestión de la información de manera confiable cumpliendo con los protocolos requeridos de acuerdo a la norma NIST 800-53 y sus controles establecidos en el capitulo 3 de mencionada norma para brindar seguridad al sistema; para lo cual determinaremos el nivel de impacto de un sistema de información de la siguiente manera (NIST, 2013).

- *Primero*, determine los diferentes tipos de información que el sistema de información procesa, almacena o transmite. La publicación especial NIST 800-60 proporciona tipos de información comunes.
- *Segundo*, usando los valores de impacto en la Publicación 199 de FIPS y las recomendaciones de la Publicación Especial NIST 800-60, clasifica la confidencialidad, integridad y disponibilidad de cada tipo de información.
- Tercero, determine la categorización de seguridad del sistema de información, es decir, el valor de mayor impacto para cada objetivo de seguridad (confidencialidad, integridad, disponibilidad) entre las categorizaciones para los tipos de información asociados con el sistema de información.
- Cuarto, determine el nivel de impacto general del sistema de información a partir del valor de impacto más alto entre los tres objetivos de seguridad en la categorización de seguridad del sistema.

1. Políticas y normas de seguridad de la información para la implementación del sistema integrado de información de inteligencia

1.1. Políticas

Todas las áreas destinadas al procesamiento de la información según los niveles de clasificación establecidos por el sistema de inteligencia en su directiva de clasificación de la información (Organización Internacional de Normalización, 2017), deben contar con:

1. Protecciones físicas o perímetros de seguridad de acuerdo con la necesidad de aseguramiento, clasificación y valoración de los activos de información (tales como paredes, puertas de acceso controlado, recepcionistas, cámaras de seguridad), éstas deben cubrir con las necesidades en cuanto a:

   1.1. Controles de entradas físicos,

   1.2. Seguridad de oficinas, espacios y medios,

   1.3. Protección contra amenazas externas y ambientales.

2. El Sistema debe contar con perímetros de seguridad en las áreas donde se encuentren instalados los centros de procesamiento de la Información, Suministro de Energía Eléctrica, de Aire Acondicionado (Organización Internacional de Normalización, 2017), y cualquier otra área considerada crítica para el correcto funcionamiento del sistema.

3. Los equipos de Cómputo del sistema deben estar protegidos frente a posibles fallas en el Suministro de Energía Eléctrica, para asegurar la continuidad del servicio de los equipos.
4. El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe estar protegido contra intercepción o daño.

1.2. Seguridad física y ambiental

1.2.1. Áreas seguras

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con la información.

1. Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad físicos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia.

2. Los perímetros de seguridad deben estar delimitados por una barrera, como, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas para controles de acceso físico.

3. Se deben ubicar las instalaciones de procesamiento de información dentro del perímetro de construcción físicamente sólida. Las paredes externas del área deben ser sólidas y casi todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, (Mecanismos de control, vallas, alarmas, cerraduras, entre otras).

4. El responsable de la Seguridad de la Información debe llevar un registro actualizado de las Áreas Seguras, donde se indique la identificación del Edificio y Área, principales Activos de información a proteger y medidas de protección física

1.2.2. Controles de acceso físico

Todas las áreas destinadas al procesamiento o almacenamiento de información confidencial y secreta, así como aquellas en las que se encuentren los equipos y demás infraestructura que

soporte a los sistemas de información y comunicaciones debe ser protegida con medidas de control de acceso físico tales como:

1. Los Centros de Cómputo debe contar con mecanismos de control de acceso tales como puertas de seguridad, cerradura, sistemas de control con tarjetas inteligentes, sistema de alarmas o controles biométricos.

2. El ingreso de terceros a los Centros de Cómputo y Centros de Cableado debe estar debidamente registrado mediante una bitácora.

3. Todos los funcionarios, Contratistas y/o Terceros deben portar el carnet que los acredite que prestan sus servicios al sistema, no deben intentar ingresar a las áreas donde no tengan la debida autorización.

1.2.3. Protección contra Amenazas Externas y Ambientales

1. Las Oficinas e instalaciones donde se procesa y/o almacena la información confidencial o secreta debe contar con sistemas de alarmas y cámaras de seguridad, sistema de detección y extinción automáticas de incendios.

2. Se debe mantener buena ubicación de los equipos, aislado de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

3. Los equipos del Centro de Cómputo deben tener control de los niveles de temperatura y humedad, estos deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada.

4. Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipo que registre información, a menos que hayan sido

formalmente autorizadas por el responsable del proceso involucrado y el responsable de Seguridad Información.

5. No se permite comer, beber y/o fumar dentro de las instalaciones de procesamiento de la información del sistema integrado.

1.2.4. Seguridad en los Servicios de Suministro Eléctrico

1. Disponer de múltiples enchufes o líneas de suministro de energía eléctrica regulada.

2. Contar con un Sistema de Energía Interrumpible UPS y/o plantas eléctricas, para asegurar la disponibilidad cuando el fluido eléctrico sea cortado y asegurar la disponibilidad del sistema mientras se restablecen las fallas en el suministro de energía eléctrica.
3. El sistema debe contar con iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

4. El sistema debe contar con protección contra descargas eléctricas en los edificios donde se ubica.

1.2.5. Seguridad del Cableado

1. Cumplir con los Requisitos Técnicos Vigentes de la República de Colombia.

2. Realizar las Conexiones Adecuadas para la Energía Eléctrica y la Red De Datos.

3. Proteger el Cableado de red contra Intercepción no Autorizada, el cableado debe contar con conductos como canaletas para su adecuada protección.

4. El cableado Eléctrico debe estar separado del cableado de Red para Evitar posibles Interferencias.

1.2.6. Mantenimiento de Equipos

1. Se debe establecer y dar cumplimiento al programa de mantenimiento a los equipos del sistema.

2. Los trabajos de mantenimiento de redes eléctricas, cableado de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.

3. Se deben someter a las estaciones de trabajo, portátiles, servidores, equipos de comunicaciones, al mantenimiento preventivo, de acuerdo con el cronograma establecido y las especificaciones del proveedor, con la debida autorización formal del responsable del proceso Gestión de Tecnologías de la Información del sistema

4. El responsable del proceso Gestión de Tecnologías de la Información y la Comunicación deberá tener un listado con las especificaciones o características de los equipos, así como también la fecha en la que cada equipo requiere actividades de mantenimiento.

5. Registrar las fallas de los mantenimientos de las estaciones de trabajo, portátiles, equipos de comunicaciones y operaciones ya sean preventivo o correctivos, este tipo de registro debe indicar la fecha en la que fue realizado el mantenimiento, falla que presentó y quien realizó el mantenimiento.

1.2.7. Seguridad para los sistemas de procesamiento de información

Se deben utilizar perímetros de seguridad (barreras tales como paredes, rejas de entradas controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

Se deben implementar los siguientes lineamientos para los perímetros de seguridad físicos (Organización Internacional de Normalización, 2017):

1. Se deben definir claramente los perímetros de seguridad los cuales estarán ligados a los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo.

2. El área donde se ubicará el centro de cómputo principal debe estar construido en materiales solidos que permitan su protección y no sean de fácil acceso; con accesos protegidos contra ingresos no autorizados mediante mecanismos de control; y autenticación.

3. Debe contar con un área de recepción que permita controlar el acceso físico al área de procesamiento de información solamente al personal autorizado.

4. Los sistemas de detección de intrusos deben estar configurados según estándares nacionales, regionales e internacionales, los cuales deben ser probados regularmente.

5. Los sistemas que procesan información sensible deben ser operados por personal orgánico del ministerio de defensa y deben estar físicamente separados de los equipos administrados por terceros.

1.2.8. Controles de ingreso físico

Las áreas seguras deben protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado, considerando los siguientes lineamientos:

1. Se debe llevar un registro del personal que ingresa y sale de las instalaciones donde se encuentren los centros de cómputo registrando la fecha y la hora de entrada y salida de los visitantes, a quienes sólo se les permitirá el acceso por propósitos específicos y autorizados.

2. En las áreas donde se procesa o almacena información sensible el acceso es restringido sólo a personas autorizadas; implementando controles de autenticación para autorizar y validar todos los accesos.

3. El personal de servicio de apoyo de terceros se les otorgara acceso restringido a las áreas seguras o los medios de procesamiento de información confidencial, solo cuando sea necesario; este acceso debiera ser autorizado por el jefe de seguridad militar y monitoreado por el mismo.

4. El administrador de la seguridad física debe verificar los accesos a áreas seguras actualizándolos regularmente, y revocados cuando sea necesario.

1.2.9. Ciberseguridad y seguridad de la información

1) Gestión de riesgos

Se debe crear y/o adecuar un procedimiento para la gestión de riesgos en ciberseguridad, se sugiere tomar como referencia la ISO/IEC 27005 o la MAGERIT. El proceso de gestión de riesgos debe comprender la identificación, evaluación, calificación, obtención de mapa de riesgos, niveles de aceptabilidad y planes de tratamiento al riesgo, así como el proceso de seguimiento y mejora continua.

2) Seguridad en el recurso humano

El personal debe contar con un proceso antes, durante y después de la contratación, en dónde se evalúe como mínimo la perfilación propia del cargo. Una vez sea retirado, se deben cancelar todos los permisos y privilegios sobre los sistemas y la información. Debe existir cláusulas de confidencialidad y no divulgación de información, que comprenda mínimo 10 años de no divulgación.

3) Seguridad en los activos de información

Se debe contar con un sistema de información para el inventario de activos y estos deben ser protegidos de forma física y lógica a través del control de acceso y permisos acorde al nivel de criticidad del activo. Cada activo debe ser clasificado acorde a las definiciones a nivel nacional para la clasificación de información.

4) Planes de cultura y sensibilización

Se deben desarrollar de forma periódica planes de cultura y sensibilización a todos los empleados y terceros que tengan acceso o contacto con la información y los sistemas de procesamiento. Dichos planes deben contener la divulgación de las políticas de seguridad, toma de conciencia sobre los riesgos en ciberseguridad y los posibles controles, no divulgación de contraseñas y accesos a terceros, no compartir claves, así como la responsabilidad de cada empleado sobre la información que maneja, usa o custodia.

5) Control de acceso a los sistemas

Se deben definir roles y perfiles para el acceso a la información, un flujo de aprobación para otorgar privilegios, control de contraseñas fuertes con cambio periódico, mecanismos de autenticación como biométricos o token, doble factor haciendo uso del celular o el correo electrónico, control de contraseñas temporales de tipo One-time-pass

6) Criptografía

Se debe tener una estrategia para el cifrado de información (local y en tránsito), a través de software de cifrado (simétrico superior a 256 bit y asimétrico por encima de 2048 bit), se deben resguardar las lleves criptográficas de forma segura, se prohíbe la compartición de las llaves maestras, renovación periódica de certificados digitales. Crear una estrategia de firma digital para documentos de alta confidencialidad. Uso de VPN (redes privadas virtuales) para la conexión hacia los sistemas de información.

7) Seguridad en las comunicaciones

Los sistemas de comunicación (router, swith, AP) deben tener seguridad física y lógica, control de acceso, control de parches y mecanismos de cifrado.

8) Seguridad en los sistemas de procesamiento

Sistemas antivirus, control de parches y actualizaciones, control de acceso al sistema operativo y las carpetas de almacenamiento de información, registros de auditoria y seguimiento de acceso.

9) Manejo y respuesta de incidentes de seguridad lógica

Se debe crear un procedimiento para el manejo de incidentes de seguridad y un equipo de respuesta ante dichos incidentes (CSIRT), dicho equipo de respuesta debe estar sincronizado con el CSIRT nacional.

10) Alta disponibilidad y planes de contingencia

Se debe crear un proceso para la continuidad de las operaciones en casos de fallo o catástrofe en los sistemas, así como el diseño de planes de contingencia y continuidad ante eventualidades. Se debe definir el RTO y RPO, las personas claves y la definición de los roles a cumplir, procedimiento para la gestión de crisis.

1. Análisis preliminar

En esta etapa se debe establecer los alcances de la verificación a realizar, si es el primero que se realiza, se tomará como base todas las necesidades y procesos de implementación. Para un ciclo posterior, se deben tomar las acciones de mejora del proceso anterior y sobre estás realizar las revisiones.

2. Construcción del plan de auditoria

En esta etapa es necesario hacer el cronograma de ejecución del plan, establecer los hitos y entregables, así mismo, definir las personas responsables de la ejecución. Es importante definir la escala de calificación para los hallazgos.

3. Preparación de la auditoria

3.1. Las auditorías deben ser comunicadas mediante correo electrónico a los líderes de proceso, con copia a los jefes de área que participan en el proceso y al auditor líder principal.

3.2. El Plan de Auditoría, se elaborará teniendo en cuenta el Programa de Auditoría aprobado por el Comité de Calidad y debe contener:

3.2.1. Objetivo, alcance, tiempo de ejecución de la auditoría, documentos de referencia.

3.2.2. Reunión de apertura

3.2.3. Auditoría al líder del proceso después de haber auditado a los demás funcionarios del proceso y una vez clasificados los hallazgos evidenciados.

3.2.4. Reunión de cierre con el líder de proceso, inmediatamente haya sido auditado.

II. VERIFICACIÓN Y EVALUACIÓN DEL SISTEMA

Para realizar la validación en cuanto a la implementación de las medidas propuesta, se debe ejecutar un plan de auditoría técnica y procedimental (figura 12) en la cual se logre tener una medición del estado de la implementación, así como los planes de mejoramiento.

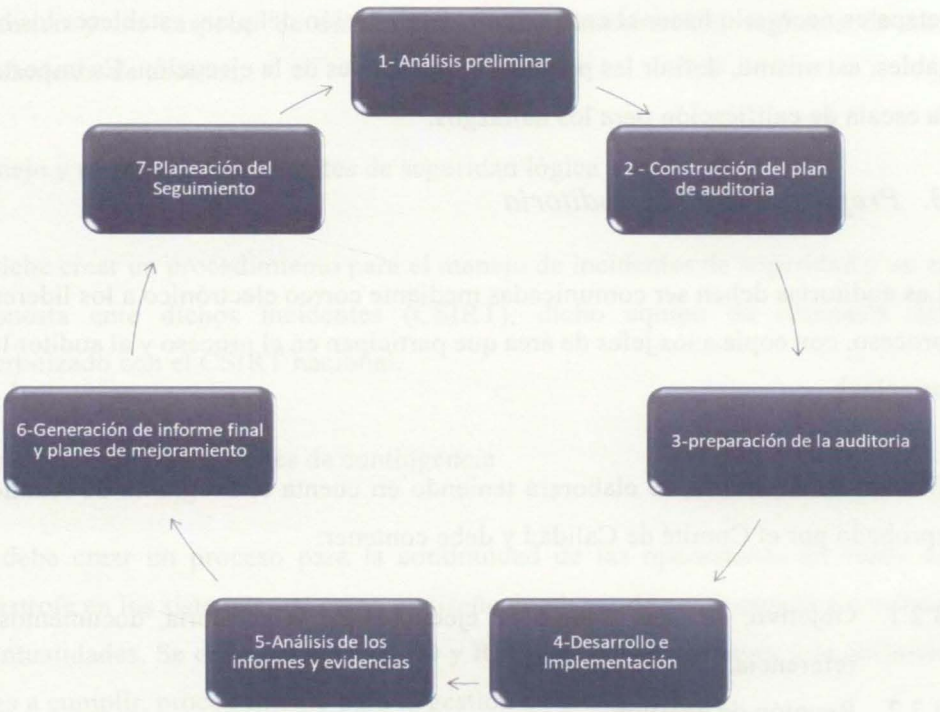


Figura 12: Plan de auditoria técnica y procedimental. Fuente: elaboración propia, noviembre 2018.

3.3. En el evento en que, en un mismo ciclo, se programe auditoría a más de un proceso por líder, puede coordinarse entre los auditores líderes respectivos, una sola reunión de apertura por líder de proceso.

3.4. El equipo auditor revisa la información del SGI y del proceso asignado en el aplicativo del SGI, los informes de auditorías anteriores y, de ser posible, en los aplicativos que soportan el proceso respectivo y elabora listas de chequeo por rol a auditar.

3.5. En desarrollo de esta fase, el Auditor Líder puede solicitar información al Líder del proceso y/o a los jefes de las dependencias objeto de auditoría. Para lo anterior, solo es necesario que se hubiere divulgado el Plan General de Auditoría.

3.6. Los hallazgos evidenciados en esta etapa se incluyen en la lista de chequeo y se revisarán en la auditoría que se realice al Líder del proceso.

3.7. Se debe establecer si la auditoria (o parte de ella) se tiene contemplado la ejecución de alguna herramienta técnica de tipo Ethical Hacking, para lo cual, es necesario hacer la selección de acuerdo con el alcance y las necesidades, de igual manera es necesario contemplar el procedimiento para la ejecución de las pruebas y/o si están deben ser contratadas con un tercero.

3.8. Los entregables de esta fase son:

- Plan de auditoría específico
- Correo emitiendo plan
- Listas de Chequeo preparadas y revisadas por el Auditor Líder Principal.

4. Desarrollo e implementación de la auditoria

En el desarrollo de esta fase el comité debe realizar los siguientes pasos:

4.1. Realizar la reunión de apertura. En la cual los encargados de seguridad de la información diligenciaran las respectivas actas de promesa de reserva y demás protocolos establecidos para garantizar la confidencialidad de la información.

4.2. Entrega de la información. La información debe ser suministrada por los auditados quienes son los responsables de entregar la información requerida por los auditores y de cumplir con el plan de auditorías.

4.3. La información y/o registros deben ser consultados por parte del auditor en los sistemas de información con que cuenta el sitio de la auditoría; ya que por la sensibilidad de la información esta no debe salir de los centros de almacenamiento y procesamiento.

4.4. En las Listas de chequeo se registra el resultado de la auditoría realizada a cada uno de los funcionarios auditados y debe firmarse tanto por el auditado como por el auditor. En el evento de encontrarse un posible hallazgo, se registra allí la evidencia que respalda el hallazgo.

4.5. Los hallazgos de la auditoría interna pueden clasificarse en fortalezas, oportunidades de mejora, no conformidades y/o salidas no conformes.

4.6. En la reunión de cierre, la cual debe quedar documentada en la proforma acta de reunión el auditor líder presenta al líder del proceso los hallazgos y aclara las inquietudes sobre los hallazgos y evidencias encontradas:

- Fortalezas encontradas en desarrollo de la auditoría y que sería importante que el proceso conservara.
- Oportunidades de Mejora para aumentar la capacidad y optimizar el desempeño del proceso.
- No Conformidades y/o Salidas No Conformes encontradas, junto con las evidencias que soportan dichos hallazgos; deben ser subsanados a través de correcciones y/o acciones correctivas.

Los entregables de esta segunda fase son:

- Acta de reunión y/o Control de asistencia de la reunión de apertura de la auditoría del proceso.
- Actas de promesa de reserva legal
- Listas de Chequeo firmadas por auditores y auditados.
- Acta de reunión de cierre firmada por el Auditor Líder y Líder de proceso con los hallazgos encontrados en las auditorías.
- Papeles de trabajo.
- Lista asistencia a reunión general de cierre y documento resumen.

5. *Análisis de los informes y evidencias, Informe final*

Una vez realizada la reunión general de cierre y si no existieran diferencias, el equipo auditor debe enviar el informe de la auditoria en sobre de seguridad al comando superior con el fin de tomar las medidas pertinentes de acuerdo con lo ordenado por la inspección general de comando Ejercito. Con base en los informes de auditoría interna por proceso se elabora el informe de auditoría interna los cuales deben estar soportados por evidencias competentes y debidamente documentadas, pero garantizando el secreto debido a que de ser filtrada la información podría poner en evidencia las vulnerabilidades del sistema.

Una vez finalizada la auditoria será el batallón de seguridad de la información quien se encargará de desarrollar los planes correctivos teniendo en cuenta la información requerida (análisis de Causas, objetivo del Plan de Acción y objetivo de mejoramiento, actividades, responsable(s) de cada actividad, fecha de compromiso de cada actividad), para evaluar la pertinencia de estos y la apertura de las investigaciones penales o disciplinarias si las observaciones lo ameritan.

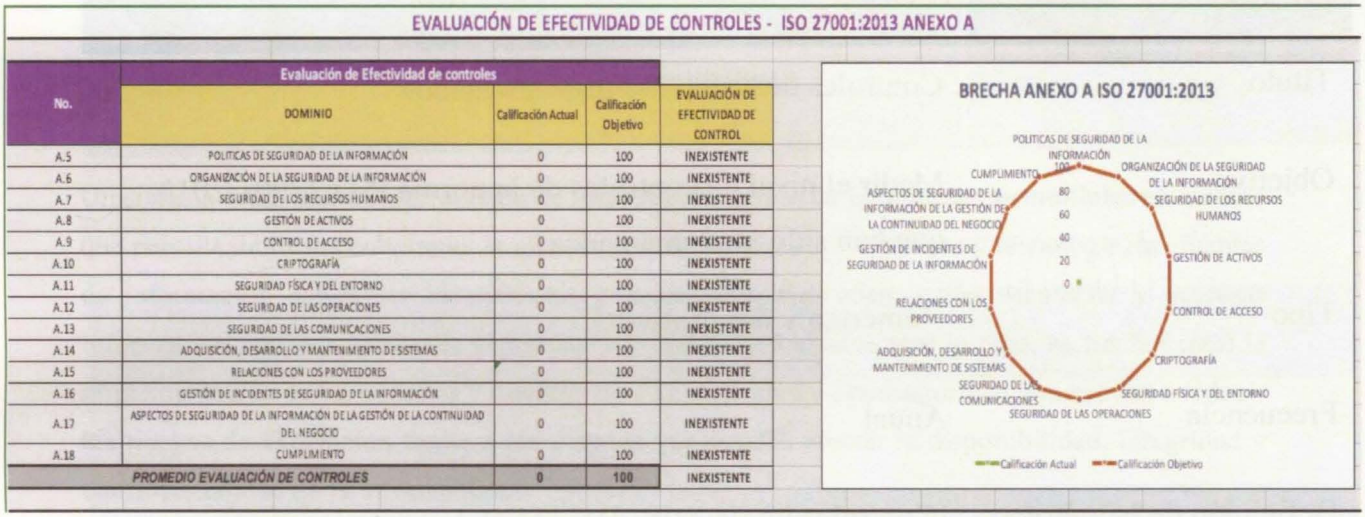
El cumplimiento de las actividades definidas para atender los hallazgos de la auditoría, y la evaluación de la eficacia de las acciones implementadas por los procesos, se hará según lo establecido en los procedimientos mejoramiento del Sistema de Gestión Integrado.

Los entregables de esta fase son:

- Informes de Auditoría por proceso y del SGI (E-PI-PLA-060 y E-PI-PLA-055).
- Cierre de Hallazgos de Auditoría Interna (E-PI-PLA-053)
- Evaluación de Auditores del SGI (E-PI-PLA-056).

6. Medición de la evaluación y seguimiento

El seguimiento a la implementación de controles de seguridad se hará con base en la norma internacional ISO 27001:2013 (figura 13) y las recomendaciones de la NIST en cuanto a identificar, proteger, detectar, responder y recuperar (figura 14), en la cual se medirá el nivel de implementación del control.



EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	0	100	INEXISTENTE
A.8	GESTIÓN DE ACTIVOS	0	100	INEXISTENTE
A.9	CONTROL DE ACCESO	0	100	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	INEXISTENTE
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	INEXISTENTE
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	INEXISTENTE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	0	100	INEXISTENTE
	PROMEDIO EVALUACIÓN DE CONTROLES	0	100	INEXISTENTE

Figura 13: Nivel de medición de controles con base en la ISO 27001:2013. Fuente Ministerio TIC

Figura 14: Niveles de calificación acorde a la NIST. Fuente NIST

6.1. Indicadores

Para la evolución de la implementación de los controles, es necesario definir un grupo de indicadores, para lo cual, se entrega la plantilla a diligenciar, en ella, se entrega un indicador ejemplo en la tabla 2:

Variable	Comentario / definición
Titulo	Controles de seguridad implementados
Objetivo	Medir el nivel de controles de la norma ISO 27001:2013 que han sido implementados.
Tipo	Numérico y descriptivo
Frecuencia	Anual
Definición de la métrica (formula)	[Controles implementados] / total de controles propuestos en 1 año
Unidad de medida	Porcentaje
Responsable	Área de seguridad / ciberseguridad o responsable de implementación
Meta	80 % de los controles implementados en 75%
Recursos necesarios, fuentes y áreas de apoyo	Herramienta de mesa de ayuda, informes, modelo financiero, sistemas de procesamiento, equipo del proyecto.

Tabla 2: Propuesta de construcción de indicadores de seguridad. Fuente: Elaboración propia, octubre 2018

6.2. Planes de seguimiento

Una vez obtenido el informe final, es necesario establecer los responsables de la ejecución de las acciones de mejora, igualmente, establecer el plan de seguimiento considerando fechas de seguimiento, cronograma, responsables, hitos a verificar, si la acción es preventiva, correctiva o de mejora.

CONCLUSIONES

Un sistema integrado de información de Inteligencia debe estar compuesto de múltiples elementos que permita de forma coherente, la interacción entre procesos – personas y tecnología, las fuentes de información deben ser identificadas y aseguradas, con ellos, poder recolectar y procesar información con los niveles de seguridad informática adecuados, por lo cual, es fundamental la implementación de las políticas y lineamientos de seguridad y ciberseguridad que ayuden a reducir los riesgos de exposición frente a los eventos que puedan afectar la disponibilidad, integridad y confidencialidad de la información.

Diseñar un sistema integrado de información de Inteligencia, que permita la gestión de la información de Inteligencia militar del Ejército, mediante la integración de las tecnologías existentes que permitan disponer de la información de manera segura, completa, confiable y oportuna cumpliendo con la ley 1621 de 2013.

Conclusiones del objetivo general

En relación con el objetivo general de este "*Diseñar un sistema integrado de información de Inteligencia, que permita la gestión de la información de Inteligencia militar del Ejército*", se concluye que fue posible el diseño de un sistema que permite, a través de su implementación, la gestión de la información con base en las necesidades encontradas. Para realizar una implementación de este tipo de sistemas deben tenerse en cuenta los tres aspectos fundamentales para este proceso:

-Logística
-Recursos económicos
-Tecnología
-Seguridad informática y de la información.

Desde el aspecto de seguridad informática y de la información se debe hacer hincapié en aspectos como concientización a nivel de operadores y a su vez una importante inversión en IDS y sistemas que permitan generar alertas, correlacionador de eventos que permitan al personal encargado del área de seguridad anticiparse a cualquier posible evento que comprometa el sistema en alguno de sus tres pilares fundamentales (integridad, confidencialidad y disponibilidad).

1. Identificar del problema, oportunidades, objetivos y determinación de los requerimientos de información.

Una vez realizado el trabajo y realizando un levantamiento de datos para identificar con que se cuenta dentro del Ejército Nacional para realizar un adecuado tratamiento de los datos recolectados a través del proceso de búsqueda de información de inteligencia militar podemos evidenciar que en la actualidad no existe un sistema que supla esta necesidad por tal razón el poder llevar a feliz término un sistema integrado representa una oportunidad que a mediano plazo se verá representada en la mejora de los siguientes objetivos:

- Austeridad en el recurso económico
-Optimización de los tiempos para los tratadores de información
-Adecuada toma de decisiones en el alto mando.

Para poder llevar a cabo este modelo se hizo realizo un levantamiento de datos técnicos y de información que nos permitieron determinar las principales necesidades para su futura implementación.

2. Establecer los requerimientos tecnológicos para pruebas y mantenimiento del sistema.

Respecto al segundo objetivo específico, "Establecer los requerimientos tecnológicos para pruebas y mantenimiento del sistema", el presente trabajo final ofreció insumos conceptuales que permitieron definir de manera prospectiva los principales requerimientos para tener en cuenta desde el punto de vista de las tecnologías de la información y la comunicación que nos lleven a

realizar con un criterio adecuado las pruebas de funcionamiento y un mantenimiento oportuno del sistema.

Una vez finalizado este trabajo, se puede concluir que para la implementación del sistema se requiere:

A. Se requiere la integración segura de los elementos tanto de software, como de hardware y la adecuación de la planta física que permitan un óptimo y seguro funcionamiento de los equipos.
B. Durante el proceso de pruebas y mantenimiento se debe estar estrictamente ceñidos a los controles establecidos para operarios y directivos que intervengan en los procesos que lleva el sistema integrado de información.
C. El propósito de cualquier prueba o mantenimiento del sistema está encaminado en una mejora continua del mismo por lo cual se debe asumir una responsabilidad en el mando en cuanto a cronogramas, gestión del recurso humano y técnico para tal fin.

3. Definir el protocolo de implementación, seguimiento y evaluación del sistema.

Respecto al tercer objetivo específico, "Definir el protocolo de implementación, seguimiento y evaluación del sistema", se orientó la toma de decisiones en cuanto a las políticas y normas de seguridad que se deben tener como lo son:

- Protecciones físicas.
-Áreas perimétricas seguras.
- Redundancia (TIER) en el suministro de energía de los equipos de cómputo.

Adicional a las políticas establecidas todo empleado debe regirse por normas internas y estándares internacionales que permiten la gestión del riesgo.

De manera transversal se debe implementar un plan de auditorías periódicas que permitan la oportuna intervención para mitigar riesgos o amenazas que puedan llegar a comprometer el sistema integrado de información.

RECOMENDACIONES

Para iniciar con el desarrollo del proyecto del sistema integrado de información para la inteligencia se deben tener en cuenta los siguientes aspectos

1. Debe ser un proyecto escalable que permita la implementación por etapas de manera que puede llegar de manera no traumática a todos los procesos del sistema; permitiendo generar un esquema organizacional de la Inteligencia Militar, racionalizando la planta de personal y ajustándola acorde a las necesidades surgidas en la implementación.

2. Centralización de los archivos de Inteligencia y Contrainteligencia Militar mediante la adecuación de las instalaciones actuales para la implementación del sistema integrado de información.

3. Capacitar y entrenar al personal del sistema integrado de información, en gestión, seguridad y análisis de la información, gestión archivística, generación de información geográfica y desarrollo de software que permita garantizar el flujo de la información y el sostenimiento del equipamiento adquirido.

4. Proteger la información del Sistema de Inteligencia y Contrainteligencia ante eventos que vulneren la integridad, disponibilidad y confidencialidad, mediante la aplicación de políticas orientadas al fortalecimiento del liderazgo del hombre de inteligencia en el uso adecuado y oportuno de herramientas de gestión de información.

5. Es fundamental que, en la implementación, se definan indicadores que permitan la medición del sistema en políticas, procedimientos, implementación de tecnologías, y desarrollo del talento humano; y con ello, poder medir por medio de estadísticas comparativas la evolución del sistema.

GLOSARIO DE SIGLAS

TIC: Tecnologías de información y comunicaciones

FFMM: Fuerzas militares

UIAF: Unidad de Información y análisis financiero

SISPRO: Sistema integrado de información de la protección social

CONPES: Consejo Nacional de Política Económica y Social

ISO: Organización Internacional de Normalización

IEC: Comisión Electrotécnica Internacional

GIS: Sistema de información geográfica (siglas en ingles)

AO: Área de operaciones

VPN: Red privada virtual (siglas en ingles)

PKI: Infraestructura de clave pública (siglas en ingles)

MAC: Código de autenticación de mensaje (siglas en ingles)

AC: Autoridad de certificación (siglas en ingles)

RA: Autoridad de registro (siglas en ingles)

TSA: Autoridad de sellado de tiempo (siglas en ingles)

TLS: Seguridad de la capa de transporte (siglas en ingles)

IPSEC: protocolo de internet seguro (siglas en ingles)

CPD: Centro de protección de datos

SGDEA: sistema de gestión de documentos electrónicos de archivo

ERMS: Sistema de gestión de registros electrónicos (siglas en ingles)

ACR: Actualización corrección y retiro

OSI: Sistemas abiertos de interconexión (siglas en ingles)

SIEM: sistema de gestión de información y eventos de seguridad (siglas en ingles)

BIBLIOGRAFÍA

Asobancaria. (2016). Ciberdefensa y Ciberseguridad: de la política pública a las acciones concretas. Bogotá.

ACIS. (2017). Seguridad digital. retos y desafíos en una realidad digitalmente modificada. Bogotá.

Ayala, L. E. (2008). Implementación de redes con el uso de clientes livianos.

Aguirre, J. (2018, diciembre 10). Coursehero. Retrieved from Coursehero.com: https://www.coursehero.com/file/38719350/C4pdf/

Avast. (2019). blog.avast. Retrieved from blog.avast: https://blog.avast.com/es/avast-secureline-aumenta-la-velocidad-y-el-rendimiento

Archivo General de la Nación Colombia. (2018). Guía para la implementación de un sistema de gestión de documentos electrónicos de archivo SGDEA. Bogota .

Akerkar, R. (2019). Big Data Computing. CRC press.

Bonilla, D. N. (2015). Inteligencia en teoría: manuales, reglamentos e instrucciones sobre doctrina y procedimientos (Francia, Reino Unido y Estados Unidos, 1870-1945). Revista universitaria de historia militar.

Borghello, C. (2002, junio 26). Seguridad informática sus implicancias e implementación . Seguridad informática sus implicancias e implementación . Madrid , España.

Blanco, J. M. (2011). Seguridad e inteligencia 10 años después del 11-S.

Bertolin, J. A. (2008). Seguridad de la información . Madrid: Parainfo.

Bertolín, G. A. (2004). Identificación y análisis en torno a PKI. Revista Española de electronica, 62 - 66.

Caire, R. (2018, octubre). Powerfast.net. Retrieved from ftp://ftp.powerfast.net/pub/manuales/vpn/introvpn.pdf

CCN-STIC-400. (2013, mayo). Manual STIC Norma de seguridad de las TIC. Manual STIC Norma de seguridad de las TIC. Madrid, España: Centro Criptologico Nacional España.

Cope, C. R. (2017, febrero 10). Warfare in the fifth domain: A realistic threat or hyperbole. Warfare in the fifth domain: A realistic threat or hyperbole. London, England: Royal Holloway University of London.

Dent, A. (2004). User's Guide to Cryptography and Standards. Boston: Artech House.

Delgado, M. S. (2000, noviembre). Redes privadas virtuales, estudio de sus principales algoritmos de encripcion y protocolos e implementación. Redes privadas virtuales, estudio de sus principales algoritmos de encripcion y protocolos e implementación. Quito , Ecuador: EPN2000.

Dorothy, D. (2019, enero 25). Dma.fi.upm.es. Retrieved from dma: http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/bibliografia.html

Draper, G. (2016). Characterization of Encrypted and VPN Traffic using Time-related Features. Characterization of Encrypted and VPN Traffic using Time-related Features. New Brunswick, Canadá.

Ejercito Nacional de Colombia . (2017). Manual fundamental del Ejercito 2.0 Inteligencia. Bogotá: CEMIL.

Fraguas, R. (1991). Servicios secretos y razón de estado. Claves de razón practica.

García, P. G. (2014). Hacia una propuesta de mecanismos para la autenticidad de objetos de aprendizaje en plataformas Learning Content Management Systems. Bogotá , Colombia .

Gabriel Díaz, F. M. (2012). Seguridad en las comunicaciones y en la información. Madrid: UNED.

Galindo, C. J. (2009). Diseño y Optimización de un Sistema de Detección de Intrusos Híbrido. Diseño y Optimización de un Sistema de Detección de Intrusos Híbrido. Almeria, España.

García, F. (2016, febrero 8). Desarrollo de librerías de firma ciega para OpenSSL. Desarrollo de librerías de firma ciega para OpenSSL. Madrid, España.

Gómez, D. G. (2003, julio). Sistema de detección de intrusiones. Sistema de detección de intrusiones. Boston, Estados Unidos : GNU.

González, A. (2006, mayo). Redes privadas virtuales VPN. Redes privadas virtuales VPN. Pachuca, Hidalgo, España.

Hancke, G. (2006). Secure Internet access to gateway using secure socket layer. Pretoria: IEEE.

Harris, J. (2007). Estado Unidos de America Patent No. US8151323B2.

Iglesias, S. P. (2001, noviembre). Análisis del protocolo IPSec: el estándar de seguridad en IP. Análisis del protocolo IPSec: el estándar de seguridad en IP. Madrid, España.

Isaza, E. (2007). Estándares de seguridad basados en XML para servicios web y web semántica. Vector.

Jalal Feghhi, J. F. (1998). DIGITAL CERTIFICATES Applied Internet Security. Addison - Wesley.

Jhon. (2018, Diciembre). INFO10. Retrieved from https://jhonf10.wordpress.com/gestion-tecnologica/mapa-conceptual-firmas-digitales/

Kahn, D. (2001). Ah historical theory of intelligence.

Kalchev, S. (2019, septiembre 10). http://www.tuj.asenevtsi.com/Public/EIM.pdf.

Kouns, J. (2009). Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. England: John Wiley & Sons, Inc.

Limari, H. (2004). Protocolos de Seguridad para Redes Privadas Virtuales (VPN). Protocolos de Seguridad para Redes Privadas Virtuales (VPN). Valdivia, Chile.

Lee Y. Tina. (2000). Information modeling: from design to implementation. Gaithersburg, USA

Martínez, A. (2011). Estudio de tecnologías VPN para la interconexión de sitios remotos . Estudio de tecnologías VPN para la interconexión de sitios remotos . Riobamba , Ecuador.

Masback, K. J. (2002). Intelligence, surveillance and reconnaissance journal. Retrieved from http://www.afji.com/ISR/Mags/2002/Issue1/transforming.html

Maiorano, A. (2010). Criptografía técnicas de desarrollo para profesionales. segu info.

Navarro, M. (2015). Gestión del Conocimiento y servicios de inteligencia: la dimensión estratégica de la información.

Nash, A. (2002). PKI infraestructura de claves públicas. Bogota: Mcgraw hill.

Nieto, I. (2018). La letalidad del ciberterrorismo. Revista general de la marina, 133 - 142.

Organización Internacional de Normalización. (2017, agosto 2). ISO 27002 El dominio política de seguridad. ISO.

Oppliger, R. (2005). Contemporary Cryptography. Boston : Artech House.

Paul Oorschot, S. V. (2001). Handbook of applied cryptography. Palm Beach: Crc Press.

Phesso, A. (2009). An Efficient Attack on a Code-based Signature Scheme. An Efficient Attack on a Code-based Signature Scheme. Paris, France: Bordeux.

Quiroga, M. M. (2004, marzo). Seguridad en las transacciones electrónicas. Seguridad en las transacciones electrónicas. Bogotá, Cundinamarca, Colombia.

Real Casa de la Moneda. (2018, junio 13). Declaración general de practicas de servicios de confianza y de certificación electrónica . Declaración general de practicas de servicios de confianza y de certificación electrónica . Madrid, Madrid, España.

SANZ. (2019, febrero 25). sans.org. Retrieved from sans.org: https://www.sans.org

Sale Systems. (2018, enero). Salesystem.es. Retrieved from https://salesystems.es/una-vpn-ventajas/

Senado. (2013). Ley estatutaria 1621 de 2013. Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". Bogotá, Colombia.

Sierra, M. M. (2014, Julio 18). CONCURSO NIST ANÁLISIS DEL CONCURSO (2007-2012). ANÁLISIS DEL CONCURSO (2007-2012). Leganes, Madrid , España.

Suehring, S. (2006). Linux Firewalls 3rd edition. Indianapolis : Novell.

Stevens, M. (2012). Attacks on Hash Functions and Applications. Leiden: CWI.

Talens, S. (2019, enero 10). uv.es. Retrieved from https://www.uv.es/~sto/articulos/BEI-2003-11/certificados_digitales.pdf

Thomas, T. (1992). The correct definition of intelligence . international journal of intelligence .

Valbuena, C. (2006, noviembre). Modelo de gestión de servicios PKI basada en una arquitectura orientada a servicios. Modelo de gestión de servicios PKI basada en una arquitectura orientada a servicios. Bogotá , Colombia .

Vázquez, J. M. (2002). morales-vasquez.com. Retrieved from morales-vasquez.com: https://www.morales-vazquez.com/pdfs/ssl.pdf

Viveros, J. (2012). Defensa en profundidad para proteger la información de la red corporativa. Bogota, Colombia.

Warner, M. (2002). Wanted: a definition of inteligence. Defense Technical information Center.

Wang, F. Y. (2004). Efficient Web Content Delivery Using Proxy Caching Techniques. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, 270.

Wiley, J. (2007). Digital Data Integrity: The Evolution from Passive Protection to Active Management. The atrium: John Wiley & Sons Ltd.

Wiener, M. (2010). Cryptanalysis of Short RSA Secret Exponents. Transactions on Information Theory, 72.

Yerko, M. M. (2009). Algoritmos HASH y vulnerabilidad a ataques. Revista de Información, Tecnología y Sociedad.