ANÁLISIS DE VULNERABILIDADES EN EL SISTEMA DE SEGURIDAD FÍSICO E INFORMÁTICO DEL DEPARTAMENTO DE POLICÍA CAQUETÁ.

INGENIERA YENY PATRICIA MONTOYA SALAZAR
INGENIERO ANDRÉS FERNEY VANEGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA
2018

ANÁLISIS DE VULNERABILIDADES EN EL SISTEMA DE SEGURIDAD FÍSICO E INFORMÁTICO DEL DEPARTAMENTO DE POLICÍA CAQUETÁ.

INGENIERA YENY PATRICIA MONTOYA SALAZAR
INGENIERO ANDRÉS FERNEY VANEGAS

Propuesta de proyecto de grado para optar al título de Especialista en Seguridad Informática

Asesora: Ingeniera. Yina Alexandra González Sanabria

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA
2018

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Florencia Caquetá 27 de mayo de 2018

DEDICATORIA

A nuestros hijos, quienes son unos de los pilares fundamentales de nuestras vidas, a quienes proyectamos enseñarles a través del ejemplo y no de la exigencia insatisfecha, para que sean ciudadanos que aporten al bienestar y seguridad ciudadana de nuestro país.

A cada uno de los tutores y profesionales de diferentes disciplinas que hicieron parte de nuestra formación académica, quienes compartieron con nosotros su conocimiento y fue notorio el empeño por brindarnos un apoyo constante, dedicándonos valioso tiempo de sus vidas con el fin de impulsarnos en cada una de las etapas transcurridas durante los semestres de aprendizaje.

AGRADECIMIENTOS

Finalizado este trabajo, manifestamos nuestros más sinceros agradecimientos a todas aquellas personas que, de una u otra manera, han colaborado para su elaboración.

En primer lugar, queremos expresar nuestra gratitud a Dios por habernos dado la oportunidad de culminar esta etapa de nuestras vidas, como también los tutores quienes a través de sus conocimientos y colaboración durante este proceso nos permitieron adquirir grandes conocimientos.

Queremos agradecer a los demás profesores por contribuir a nuestra educación, y no solo en lo profesional que ahora llega a un avance significativo, sino también en nuestra formación personal. Por enseñarnos que una letra no refleja el conocimiento adquirido, por forjarnos en el trabajo de equipo y por poner a nuestro alcance un gran número de herramientas necesarias para salir adelante.

Agradecemos a nuestros padres por darnos la vida, por enseñarnos que todo lo que nos proponemos en nuestro diario vivir lo podemos alcanzar, por darnos fortaleza y alientos en los momentos difícil, por enseñarnos a ser luchadores, responsables y dedicados con nuestros proyectos, por enseñarnos a ser perseverantes y luchadores de la vida.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

AMENAZA: hecho o suceso que se presenta con el fin de causar daño a un sistema a través de la modificación de sus datos o incluso la negación de los servicios.

ARQUITECTURA DE SEGURIDAD: principios que contiene y representa los diferentes servicios de seguridad de un sistema informático ajustándose a las necesidades de los clientes, con el propósito de hacer frente a las amenazas que se presenten.

AUTENTICACIÓN: proceso que permite verificar que las transacciones informáticas no sean falsas, normalmente se emplean contraseñas, certificados o diferentes formas que lleven a que se pueda hacer la verificación de la identidad en una red de cómputos.

CONTENCIÓN DE LA AMENAZA: parámetro que permite medir la capacidad que tiene un antivirus para evitar que una amenaza presentada se propague.

CONTRASEÑA: caracteres que utilizan los usuarios como medio de protección en un sistema, a través del cual hacen su identificación y conlleva a que otros tengan restricción a información confidencial sin tener autorización.

EVALUACIÓN DE LA AMENAZA: está relacionado con los daños que causan las amenazas, el modo en cómo puede propagarse, hasta donde se ha propagado, y a qué velocidad se propaga.

EVALUACIÓN DE MEDIDAS DE SEGURIDAD: proceso mediante el cual se realiza la identificación de las diferentes medidas de seguridad con el fin de buscar estrategias que conlleven a minimizar los riesgos.

EVALUACIÓN DE RIESGOS: se encarga de realizar el cálculo de los riesgos, para verificar las vulnerabilidades que puedan causar algún daño en los activos.

EVALUACIÓN DE VULNERABILIDAD: proceso mediante el cual se realiza la identificación de las vulnerabilidades técnicas y/o ambientales de los sistemas informáticos.

INTEGRIDAD: parámetro de seguridad en la información que conlleva a que ésta no se altere de manera sin autorización.

MEDICIÓN DE RIESGOS: está basado en algoritmos eficientes que permiten la medición de los riegos en los activos.

MEDICIÓN DE VULNERABILIDADES: mediante la exposición electrónica o física se realiza la medición de las vulnerabilidades y los daños informáticos.

MEDIDA DE SEGURIDAD: procedimiento destinado a la mitigación de los riesgos informáticos.

VULNERABILIDAD: estado de los sistemas informáticos que permiten a los atacantes acceder a datos sin autorización, suplantar usuarios y realizar negación de servicios.

RESUMEN

El Departamento de Policía Caquetá es una institución al servicio de la comunidad, la cual maneja un flujo de información constante y altamente sensible abordando información confidencial de múltiples fenómenos criminales y delictivos de la región.

En este sentido, dicha información debe gozar de reserva a fin de garantizar las condiciones mínimas de seguridad para sus habitantes. Aunado a lo anterior, su infraestructura física comprende diferentes áreas que requieren de máxima seguridad para garantizar su deber constitucional (sala de cámaras, antenas etc.), por consiguiente, se hace necesario realizar un análisis del sistema de seguridad de dicha unidad con el fin de identificar las vulnerabilidades susceptibles de mejora en el ámbito físico e informático.

Con dicho análisis se pretende que una vez identificadas las principales vulnerabilidades, se adelante un plan de mejoramiento por parte de la unidad a fin de fortalecer la seguridad ciudadana en la capital Caqueteña.

Por consiguiente, el presente análisis evidencia una institución policial bastante fortalecida en el campo de la informática, cuyas principales fortalezas se establecen en el campo tecnológico y reglamentario donde existe tecnología competente y resoluciones, instructivos y directrices que aportan de manera certera a la seguridad de la información.

No obstante, las fortalezas tecnológicas y las diferentes políticas de seguridad de la información, presentan serios quebrantamientos a razón del factor humano, representado básicamente en el alto flujo de personal que maneja la institución y en la poca capacitación del mismo.

INTRODUCCIÓN

El presente proyecto busca establecer las posibles vulnerabilidades del sistema de Seguridad Informática y Seguridad Electrónica del Comando de Policía Caquetá, lo cual resulta importante teniendo en cuenta que la institución conserva un flujo de información constante, altamente sensible y confidencial, sobre fenómenos criminales y delictivos de la región, y de presentar fallas en éstos campos, podría afectarse, críticamente, no solo la seguridad ciudadana, sino también la de las personas vinculadas a la institución: particulares y uniformados.

Bajo este escenario, la información es el segundo activo de mayor importancia para el departamento de policía Caquetá, a razón de las diversas responsabilidades y compromisos sociales, lo que demanda un manejo apropiado de la misma.

Dicha unidad comprende 16 estaciones de policía conformando el nivel desconcentrado, las cuales están radicadas en los 16 municipios del departamento, comprendiendo una población estima de 465.477 habitantes.

Por consiguiente, este proyecto permite evaluar los flujos de información y los controles de seguridad existentes, de la misma manera analizar los procesos y procedimientos establecidos en los protocolos de seguridad para llegar a conclusiones que permitan estructurar un informe gerencial sobre el tema objeto de estudio y presentarlo a la unidad policial.

1. TÍTULO

Análisis de vulnerabilidades en el sistema de seguridad físico e informático del Departamento de Policía Caquetá.

2. FORMULACIÓN DEL PROBLEMA

El Departamento de Policía Caquetá maneja información relevante para la seguridad ciudadana en los 16 municipios del departamento del Caquetá y por ende, dirige las comunicaciones con las estaciones de la institución establecidas en cada municipio.

En este sentido, el presente estudio pretende establecer las posibles vulnerabilidades del sistema de Seguridad Informática y Seguridad Electrónica que pueda presentar el comando de policía Caquetá, teniendo en cuenta que las fallas en éstos campos, puede afectar críticamente la seguridad ciudadana y la seguridad de las personas vinculadas a la institución: particulares y uniformados.

En consecuencia, el problema se dimensiona en diferentes escenarios en cuanto el flujo de información del comando puede contener evidencias de diferentes delitos en la jurisdicción, también componentes y organigramas de estructuras criminales y delincuenciales del Caquetá, cuya filtración, saqueo, sabotaje o cualquier acto similar, podría afectar los derechos constitucionales de las personas allí referidas, en caso de ser inocentes o afectar cualquier operación policial en caso de estar comprometidos penalmente.

En este sentido, es necesario tener en cuenta el deber constitucional de la policía Nacional, frente a los principios de la seguridad de la información, que son: a) Confidencialidad de los datos, b) Integridad, y c) Disponibilidad.

De otra parte, es importante mencionar que las vulnerabilidades podrían presentarse desde dos ámbitos: a través de los visitantes a la unidad y a través de sus mismos funcionarios bien sea de manera intencional o accidental.

A partir del anterior planteamiento se formula el siguiente interrogante: ¿Cuál es el nivel de vulnerabilidad del sistema de Seguridad Informática y Seguridad Electrónica del Departamento de Policía Caquetá?

3. JUSTIFICACIÓN

La pertinencia del proyecto en el ámbito académico, constituye un horizonte esencial para fortalecer los conocimientos de los participantes llevado a la práctica, en una institución insignia de la comunidad con grandes retos y exigencias en materia de seguridad física y virtual a razón de su misión y función.

En lo social el reto es mucho mayor, al tener en cuenta el flujo de información relativa a la criminalidad y delincuencia del departamento, por consiguiente, con el proyecto se busca fortalecer la seguridad de la información, primero para no afectar los derechos constitucionales especialmente el derecho al buen nombre, de las personas inocentes y de quienes se podría estar almacenando información en la etapa investigativa, que de ser conocida públicamente, afectaría enormemente a la persona referida, y segundo, aportar a la seguridad ciudadana al proporcionar recomendaciones de seguridad que permitan salvaguardar la confidencialidad de la información especialmente de componentes criminales o de elementos probatorios en las diferentes conductas punibles.

En el ámbito personal, es necesario destacar que los integrantes del proyecto son beneficiarios directos de la institución policial, por consiguiente, al aportar los conocimientos al beneficio de la institución policial, se estaría haciendo un aporte significativo a lo laboral y social.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Establecer el nivel de vulnerabilidad del sistema de Seguridad Informática y Seguridad Electrónica del Departamento de Policía Caquetá.

4.2 OBJETIVOS ESPECÍFICOS

- Evaluar los flujos de información y los controles de seguridad existentes en las instalaciones objeto de estudio.
- Establecer las vulnerabilidades de seguridad informática o electrónica que se puedan estar presentando el departamento de policía Caquetá.
- Analizar los procesos y procedimientos establecidos en los protocolos de seguridad al interior del comando policía Caquetá.
- Realizar un documento para entregar donde se indique los riesgos físicos e informáticos del problema objeto de estudio.

5. ESTADO DEL ARTE

FERNÁNDEZ, Mena; JOSELYN, Carol. *Evaluación de riesgos, amenazas y vulnerabilidades en la Unidad Educativa "Policía Nacional" del Distrito Metropolitano de Quito en el periodo lectivo septiembre 2016–junio 2017*. 2017. Tesis de Licenciatura. Quito: UCE. General. (2012). {En Línea}. {Consulta realizada en Mayo del 2018} Disponible en (http://www.dspace.uce.edu.ec/bitstream/25000/13517/1/T-UCE-0020-047-2017.pdf)

Fernández Mena en una investigación sobre "*riesgos, amenazas y vulnerabilidades en la Unidad Educativa "Policía Nacional" del Distrito Metropolitano de Quito" que esta* sección educativa es una zona que se encuentra vulnerable en varios aspectos tanto humanos y materiales a varios tipos de amenaza, por lo que este trabajo investigativo ha tomado en consideración incluir la Gestión de Riesgo como parte fundamental a la educación en la Unidad Educativa Policía Nacional.

DUQUEZ, Barón; JOSÉ, Carlos. *Metodología de análisis de vulnerabilidades para la red de datos en la dirección de telemática de la Policía Nacional*. 2010. Tesis Doctoral. Universidad Militar Nueva Granada. {En Línea}. {Consulta realizada en Mayo del 2018} Disponible en http://unimilitar-dspace.metabiblioteca.org/bitstream/10654/502/1/BaronDuquezCarlos2010.pdf

De otra parte, Duquez Barón, quien "*análisis de vulnerabilidades para la red de datos en la dirección de telemática de la Policía Nacional" comenta que en* la oficina de telemática de la policía nacional se viene implementando una serie de políticas de seguridad a nivel físico, lógico y administrativo. Todas estas políticas requieren de un completo análisis de vulnerabilidades con el fin de determinar acciones correctivas y preventivas.

PALOMINO, Rodolfo; Resolución 02069, *Manual para la gestión Integral de riesgos de la "Policía Nacional", 28 de mayo del 2014*. Resolución 02069. Ministerios de defensa nacional, Policía Nacional, Dirección general. (2014). {En Línea}. {Consulta realizada en Septiembre del 2018} Disponible en (http://www.policia.edu.co/documentos/normatividad_2016/manuales/Manual%20para%20la%20gesti%C3%B3n%20integral%20del%20riesgo%20en%20la%20Polic%C3%ADa%20Nacional%20-%20Resoluci%C3%B3n%2002069%20del%2028052014.pdf)

Palomino Rodolfo en uso de sus facultades legales que le confiere el artículo °2, numeral 8 del decreto 4222 del 231106, en el *Manual para la gestión Integral de riesgos de la "Policía Nacional"* que se hace necesario la actualización del manual como herramienta para estandarizar y unificar aspectos metodológicos que se ajusten en la normas vigentes.

LÓPEZ, Rafael; *comparación del proceso de direccionamiento tecnológico de la Policía nacional frente a otros estándares de gestión de tecnologías de información.* Universidad Militar de Nueva Granada, Facultad de ciencias económicas. Especialización en control interno. Bogotá D.C. (2014). {En Línea}. {Consulta realizada en Septiembre del 2018} Disponible en (https://repository.unimilitar.edu.co/bitstream/10654/12893/1/COMPARACI%C3%93N%20DIRECCIONAMIENTO%20TECNOL%C3%93GICO%20PONAL%20FRENTE%20A%20OTROS%20ESTANDARES.pdf)

López Rafael en su investigación sobre "*comparación del proceso de direccionamiento tecnológico de la Policía nacional frente a otros estándares de gestión de tecnologías de información"* realiza la consolidación y comprensión de un proceso de gestión de tecnología como lo es el proceso de soporte Direccionamiento Tecnológico que ejecuta la Oficina de Telemática de la Policía Nacional de Colombia, inicialmente contextualizando 4 estándares de gestión de tecnología que son relevantes y exigentes en contextos de empresas privadas y públicas.

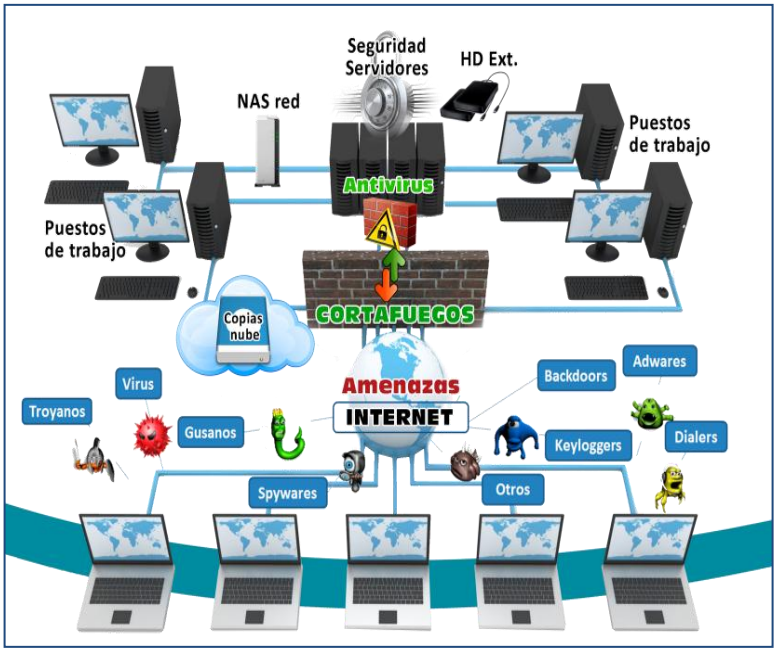
5.1 MARCO TEÓRICO

Se parte del hecho concreto de que un sistema de información, a pesar de las medidas de seguridad que se adopten siempre presentará un margen de riesgo de ser vulnerado. En este sentido Aguilera López, (2010) considera que para el establecimiento de un sistema de seguridad es necesario conocer los elementos que componen el sistema, los peligros que afectan al sistema, accidentales o provocados, y, las medidas que deben ponerse en práctica para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales.

De otra parte, la seguridad ciudadana constituye una responsabilidad social, donde compete a diferentes actores coadyuvar a construir comunidades seguras y en paz, sin embargo, frecuentemente ésta difícil labor ha sido recargada a instituciones como la Policía Nacional. El proyecto busca aportar al fortalecimiento del sistema informático y físico del comando de policía, buscando mayor seguridad

en la información almacenada y manipulada por la organización, lo cual ha de verse reflejado en resultados de mayor seguridad y convivencia ciudadana.

Figura 1. Amenazas en Internet



Fuente: DIAZ. Francisco. Tema 9.- Seguridad informática._{En Línea}. Disponible en http://fdiazuceda.blogspot.com.co/2017/05/tic-2-bachillerato-tema-9-seguridad.html

En este sentido, se pretende salvaguardar el sistema informático del comando de policía del Caquetá, protegiendo sus activos, es decir, cada uno de los recursos que hacen partes de él. Según Mifsud[1], todo esto se pueden agrupar en los hardware que comprende la parte física del sistema informático, el software que son cada uno de los elementos lógicos que se ejecutan en el hardware, los datos que hace parte de la información lógica, y otros, como lo son las personas, las infraestructuras fungibles, es decir, lo que se usa o se gasta.

[1] MIFSUD. Elvira. Introducción a la seguridad informática - Vulnerabilidades de un sistema informático. Software – General. (2012). {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3)

Por otro lado, Santana[2], explica que una vulnerabilidad hace referencia a las debilidades que se pueden ver reflejadas en los sistemas informáticos y que pueden ser utilizadas para causar daños en ellos, ya que estos pueden aparecer en cualquier elemento de una computadora, tanto en el software, como en el hardware, ya que se puede evidenciar como amenaza el cual puede causar un daño irreparable dando lugar a un ataque en el equipo, o como un riesgo que es el que conlleva a la posibilidad de que una amenaza se pueda producir.

Según Guayara[3], el hardware es el computador en donde se realizan todas las operaciones y se ejecuta una gran variedad de plataformas, que pueden ir desde los servidores, los computadores de escritorio y los portátiles, que se emplean para las diferentes configuraciones de red. Mientras que aclara que el software es el encargado de proveer todas las herramientas necesarias para realizar el almacenamiento, análisis y despliegue de toda la información, encontrando entre sus herramientas más importantes la entrada y lo que es la manipulación de la información, el sistema de análisis de administrador de bases de datos, además de las herramientas que conlleven a una búsqueda, análisis y visualización de la información. Dentro de las bases de datos se encuentra todo tipo de información que maneja una organización y que no debe de ser alterada sino protegida. Por otro lado, se encuentran los recursos humanos en el cual se debe de contar con personal especializado para operar, desarrollar y administrar los sistemas informáticos, contando con personal especializado para el manejo y mantenimiento de los sistemas.

De vulnerabilidad según Cutter[4], se puede decir que es un concepto complejo, ya que este se encarga de advertir sobre las diferentes dimensiones sociales, económicas, políticas y culturales, en la cual también se puede decir que su definición es abordada desde la parte epistemológica de diversas maneras, ciencias físicas, ecología humana, ecología política, análisis espacial, entre otras.

---

[2] SANTANA. Carlos. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. (2012). {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo)

[3] GUAYARÁ. Natalia. Sistema de información gerencial. Componentes de un sistema de información gerencial. (2014). {En Línea}. {Consulta realizada en diciembre del 2017} Disponible en http://natalia-guayaragestionempresarial.blogspot.com.co/2014/11/componentes-de-un-sistema-de.html

[4] CUTTER, S.L. (1996 b) “Vulnerability to environmental hazards”, Progress in Human Geography, vol. 20, nº 4, pp. 529-539

Bajo este escenario, se planea el hecho de poder encontrar las medidas que sean necesarias para realizar de manera apropiada el estudio de las vulnerabilidades, la distinción que hace Cutter[5], entre vulnerabilidad social (indicadores socioeconómicos, percepción del riesgo, capacidad de respuesta individual o social) y biofísica (emplazamiento y situación, proximidad a la amenaza, estructura territorial, características del medio físico) puede servir como guía para poder establecer los diferentes indicadores que conlleven a identificar las vulnerabilidades de una organización en concreto, sin dejar de un lado que las vulnerabilidades se encuentran relacionadas con los conceptos de competencia y la capacidad de respuestas de éstas, los cuales deben de medirse operativamente.

Por otro lado, Reyes[6], afirma que los sistemas informáticos utilizan diferentes tipos de componentes, desde la electricidad que es la encargada de suministrar alimentación de todos los equipos, hasta el programa del software que ejecuta los sistemas operativos de una red, exponiendo que los ataques se pueden presentar en cualquiera de éstos, siempre y cuando se presente alguna vulnerabilidad.

Garzón, Ratkovich y Vergara[7], exponen que, aunque se identifiquen los riesgos y las vulnerabilidades, una organización debe de estar preparada para poder superar cualquier tipo de eventualidades que se puedan presentar y que irrumpa las actividades habituales, a través de la aplicación de técnicas de recolección, análisis y validación de pruebas digitales.
Otro tipo de técnicas han sido desarrolladas para la detección de vulnerabilidades, Dai[8], comparte un tipo de metodología que permite la detección de vulnerabilidades a través de Fuzzing, el cual pretende que por medio de la modificación de la configuración de un programa se pueda verificar si existen

[5] CUTTER, S.L. (1996 b) “Vulnerability to environmental hazards”, Progress in Human Geography, vol. 20, nº 4, pp. 529-539

[6] REYES. Edgar. Elementos vulnerables en el sistema informático: hardware, software y datos. Seguridad informática. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://www.actiweb.es/reyes_278/archivo3.pdf)

[7] GARZÓN. Daniel. RATKOVICH. Juan. VERGARA. Alejandro. Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala. Bogotá. Pontificia Universidad Javeriana. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf)

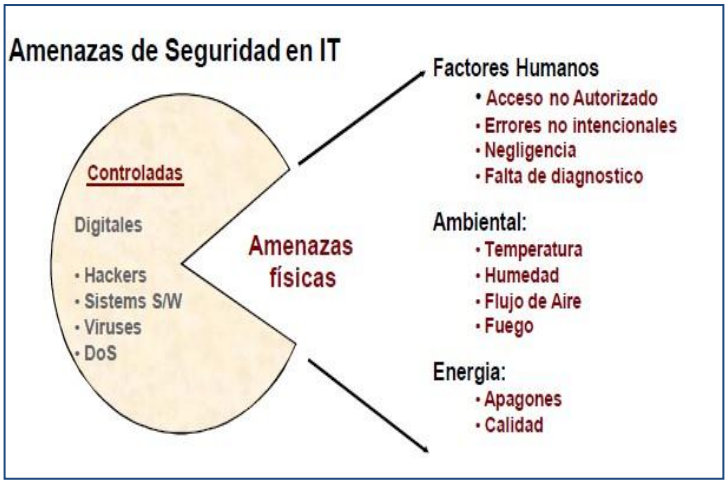
[8] DAI, MURPHY, y KAISER, Configuration Fuzzing forSoftware Vulnerability Detection, 2010 International Conference onAvailability, Reliability and Security, 525-530 (2010)

violaciones en la seguridad y así poder detectar las vulnerabilidades y corregirlas por medio de un análisis equivalente el cual es presentando en Zhang[9].

5.2 MARCO CONCEPTUAL

En cuanto al término seguro, el diccionario de la RAE trae en una sus acepciones que lo define como libre y exento de todo peligro, daño o riesgo. Esta definición es importante para el presente estudio, porque es el sentido con el cual se proyecta en cuanto a Seguridad Informática y Seguridad Electrónica.

Figura 2. Amenazas de Seguridad en IT



Fuente: ACOSTA. Victor. Impacto de las amenazas físicas y ambientales. {En Línea}. Disponible en (http://www.infosecurityvip.com/newsletter/palabras_ago10.html)

En cuanto a los conceptos de Sistemas de información y sistemas informáticos, López[10], asegura que un Sistema de Información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para

[9] ZHANG, LIU, LEI, y KUNG, CSALLNER, NYSTROM y WANG. *SimFuzz: Test case similarity directed deep fuzzing*, Journal of Systems and Software, *85*(1), 102-111 (2012a).

[10] LÓPEZ, Aguilera. Seguridad informática. Editex. P10. {En Línea}. {Consulta realizada en diciembre del 2017} Disponible en http://webcache.googleusercontent.com/search?q=cache:Ga9MXrYwWIwJ:www.editex.es/RecuperarFichero.aspx%3FId%3D19810+&cd=1&hl=es&ct=clnk&gl=co

conseguir sus objetivos; y agrega en referencia los elementos: Recursos (físicos y lógicos), equipo humano, información y las actividades que realizan en la organización, relacionadas o no con la informática. También refiriéndose al concepto de Sistema Informático, menciona que este está constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos…) y con frecuencia se incluyen también los elementos humanos (personal experto que maneja el software y el hardware).

Seguridad informática: es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. López[11].
Los problemas de seguridad se pueden dividir en amenazas y vulnerabilidades:

Amenazas: eventos que pueden afectar la información de una unidad objeto de estudio, lo cual generalmente genera pérdidas materiales, económicas, de información, y de prestigio y que atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas.

Fuentes de amenaza: Las amenazas tienen diferentes orígenes: amenazas humanas, de hardware, de software, de red y desastres naturales.
Si se tiene en cuenta el tipo de alteración, daño o intervención sobre la información. Las amenazas se clasifican en:
Interrupción: cuando busca deshabilitar el acceso a la información.

Interceptación: cuando personas, programas o equipos no autorizados, buscan acceder.

Modificación: cuando personas, programas o equipos no autorizados, buscan además de acceder al sistema modificarlo.

Fabricación: cuando se agrega información falsa en el conjunto del sistema.

[11] LÓPEZ, Aguilera. Seguridad informática. Editex. P10. {En Línea}. {Consulta realizada en diciembre del 2017} Disponible en http://webcache.googleusercontent.com/search?q=cache:Ga9MXrYwWlwJ:www.editex.es/RecuperarFichero.aspx%3FId%3D19810+&cd=1&hl=es&ct=clnk&gl=co

Según su origen se clasifican en:

Accidentales: se refiere a accidentes meteorológicos, incendios, inundaciones, fallas en los equipos, en las redes, en los sistemas operativos o en el software o errores humanos.

Intencionadas: estas amenazas siempre se presentan debido a la acción humana, como introducir al sistema un software malicioso, intrusión informática y robos o hurtos. Este tipo de amenazas pueden originarse en el exterior de la organización o en el personal interno.

Factor humano: El talento humano es la principal amenaza de los sistemas de seguridad, y generalmente está enmarcado en actos intencionales o por falta de controles eficientes.

Tipos de amenazas humanas[12].

Curiosos: personas que entran a sistemas solo por curiosidad, desafió personal, o por aprender o averiguar algo. Aunque generalmente los curiosos no tienen la intención de generar daño, la sola intrusión al sistema representa un peligro para la empresa.

Intrusos remunerados: estos atacantes se encargan de vulnerar los sistemas a cambio de dinero, estos son menos comunes, pero más peligrosos a razón que poseen conocimiento y herramientas suficientes para causar el daño.

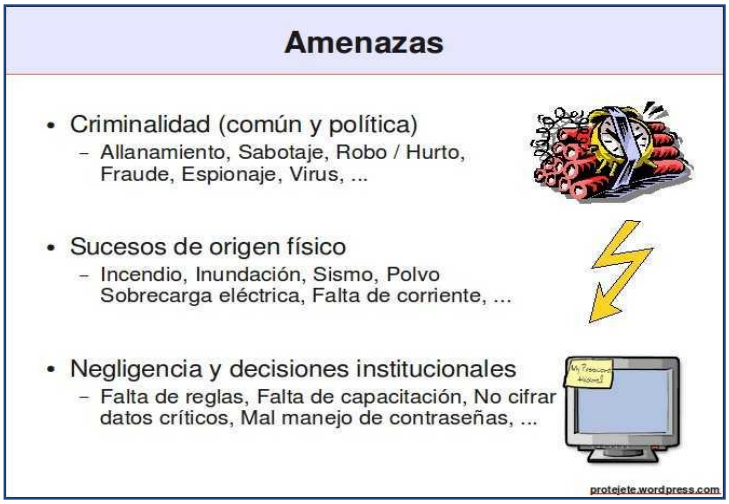
Personal enterado: es personal que tiene acceso permitido al sistema, pero su daño radica en problemas de diferentes índoles que van desde revanchas hasta pagos de personas con deseos de perjudicar la empresa.

Terroristas: personas con el fin de causar daño especialmente con fines proselitistas o religiosos.

Robo: extracción física de la información o del hardware que compone la misma.

[12] TUTORIAL DE SEGURIDAD INFORMÁTICA. Amenazas y vulnerabilidades. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html)

Figura 3. Amenazas



Fuente: Gestión de Riesgo en la Seguridad Informática. {En Línea}. Disponible en (https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/)

Tipos de amenazas de hardware[13]:

Mal diseño: Los componentes no son apropiados y no cumplen los requerimientos necesarios.

Errores de fabricación: Es cuando las piezas de hardware son adquiridas con desperfectos de fabricación y posteriormente fallan al momento de intentar usarse.

Suministro de energía: El voltaje no regulado o controlado que muchas veces presenta variaciones daña fácilmente los equipos.

Desgaste: El uso constante produce un desgaste normal de los dispositivos lo que impide un óptimo servicio.

[13] TUTORIAL DE SEGURIDAD INFORMÁTICA. Amenazas y vulnerabilidades. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html)

Descuido y mal uso: el hardware debe ser usado dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento.

Ataques: Un ataque puede ser directo o indirecto.
Se produce un ataque accidental o deliberado contra el sistema cuando se materializa una amenaza.

Los ataques se clasifican en:

Activos: cuando modifican, dañan, suprimen o agregan información, o bloquean o saturan los canales de comunicación.

Pasivos. Acceden sin autorización a los datos contenidos en el sistema.

Riesgos:

Es la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad.

Cuando existe una posibilidad de riesgo, la organización tiene tres alternativas:

Asumirlo sin hacer nada: cuando el perjuicio esperado es mínimo y el costo de aplicación de medidas es mayor al daño esperado.

Aplicar medidas para disminuirlo o anularlo.

Transferirlo: que puede ser contratando un seguro.

Vulnerabilidad:

Es la probabilidad que existe de que una amenaza se materialice. No todos los sistemas son vulnerables a las mismas amenazas. En cuanto a los datos son vulnerables a la acción de los *hackers,* mientras que una instalación eléctrica es vulnerable a un cortocircuito.

Posibles vulnerabilidades de sistemas informáticos[14]:

De diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

De implementación

- Errores de programación.
- Existencia de "puertas traseras" en los sistemas informáticos.
- Descuido de los fabricantes.

De uso

- Configuración inadecuada de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de la seguridad.
- Disponibilidad de herramientas que facilitan los ataques.
- Existencia de escenarios poco seguros en los sistemas.

[14] BARÓN. Carlos. Metodología de análisis de vulnerabilidades para la red de Datos en la dirección de telemática de la policía nacional. Universidad militar nueva granada Facultad de Ingeniería Programa de ingeniería en telecomunicaciones. Bogotá, 2010, 92p. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://unimilitar-dspace.metabiblioteca.org/bitstream/10654/502/1/BaronDuquezCarlos2010.pdf)

Diferenciación de vulnerabilidades:

- Vulnerabilidad: debilidades que pueden ser aprovechadas en determinados escenarios.
- Vulnerabilidades físicas: espacio o elemento no adecuado para el manejo de la información
- Vulnerabilidades naturales: condiciones naturales que afectan o ponen en riesgo la seguridad de la información.
- Vulnerabilidades de hardware: configuraciones erróneas o con falencias en los equipos lo que podría poner en riesgo la seguridad del sistema de información.
- Vulnerabilidades de medios de almacenamiento: condiciones no aptas ras para almacenar la información.

La información: activo principal que puede ser visual, auditivo, táctil, tangible o intangible que organizados de una determinada forma constituyen un mensaje con claridad.
La forma en que la propuesta contribuirá a la solución del problema objeto de estudio está representada en la identificación de las vulnerabilidades que el Comando de Policía Caquetá pueda estar presentando en su sistema de seguridad el cual requiere estar a la vanguardia para salvaguardar la información privilegiada que reposa en la institución policial en pro de la convivencia y seguridad ciudadana.

Políticas de Seguridad Informática.

En ítem se definen los aspectos que conforman la estrategia a seguir por la institución sobre la base de sus características propias y en conformidad con la política vigente en el país en esta materia y el sistema de seguridad diseñado, mediante el establecimiento de las normas generales que debe cumplir el personal que participa en el sistema informático y electrónico, las cuales se derivan de los resultados obtenidos en el análisis de riesgos, considerando los siguientes aspectos:

- Empleo conveniente y seguro de las tecnologías instaladas y cada uno de los servicios que éstas pueden ofrecer.
- Tratamiento que requiere la información oficial que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, según su categoría.

- Definición de los privilegios y derechos de acceso a los activos de información para garantizar su protección contra modificaciones no autorizadas, pérdidas o revelación.
- Principios que garanticen un efectivo control de acceso a las tecnologías, incluyendo el acceso remoto, y a los locales donde éstas se encuentren. e) La salva y conservación de la información.
- Conexión a redes externas a la Entidad, en especial las de alcance global y la utilización de sus servicios.
- Requerimientos de Seguridad Informática a tener en cuenta durante el diseño o la adquisición de nuevas tecnologías o proyectos de software.
- Definición de los principios relacionados con el monitoreo del correo electrónico, la gestión de las trazas de auditoría y el acceso a los ficheros de usuario.
- Mantenimiento, reparación y traslado de las tecnologías y el personal técnico que requiere acceso a las mismas.
- Regulaciones con relación a la certificación, instalación y empleo de los Sistemas de Protección electrónica.
- Regulaciones relacionadas con la certificación, instalación y empleo de los Sistemas Criptográficos, en los casos que se requiera.
- Principios generales para el tratamiento de incidentes y violaciones de seguridad.

Estadística

1) En el primer semestre del año en el país se presentaron 5235 ataques cibernéticos en el país, de los cuales el centro cibernético de la Policía Nacional respondió el 92%, y el 8% lo atendió las fuerzas militares en cabeza del Ejército Nacional.

La principal afectación, la registra el sector privado.

2) En el año 2014 el grupo Anonymous[15], se atribuyó un ataque cibernético a la Web de la Policía Nacional de Colombia, en retaliación al presunto abuso de autoridad policial, dicho ataque se presume que permaneció activo durante 18 horas.

[15] REVISTA SEMANA. Anonymous Colombia ataca página web de la Policía por "abuso de autoridad" en marchas. Bogotá. (13 de octubre, 2012). P.1

3) En el 2011 un ciberactivista publicó en redes sociales información perteneciente a la base de datos de la Policía Nacional, la información fue obtenida mediante ataque cibernético y contenía datos personales de diferentes funcionarios de la institución como dirección de residencia, celular, correos electrónicos privados, entre otros.

Figura 4. Ataques cibernéticos en Colombia

Fuente: Autor

5.3 MARCO CONTEXTUAL[16]

Una institución competitiva debe contar con pautas claras que ubiquen a los empleados y clientes sobre la perspectiva a seguir para alcanzar los objetivos planteas y la forma en que se proyecta alcanzarlos.

En este sentido toda institución debe tener una misión clara, una visión estratégica y unos principios y valores bien definidos, para alcanzar el éxito, situación a la cual no es ajeno el departamento de Policía Caquetá.

5.3.1 Misión

El Departamento de Policía Caquetá tendrá como Misión permanente dar cumplimiento a lo señalado en el artículo 218 de la Constitución Política de Colombia, que estipula:

[16] Misión, visión, mega, valores, principios, y funciones. Policía Nacional. {En Línea}. Disponible en (https://www.policia.gov.co/mision-vision-mega-principios-valores-funciones)

La Policía Nacional es un cuerpo armado permanente de naturaleza civil, a cargo de la nación, cuyo fin primordial es el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz.

5.3.2 Visión

El Departamento de Policía Caquetá en el 2022 como institución fundamental para la construcción de un país equitativo y en paz, garante y respetuoso de los derechos humanos, afianzando la convivencia y seguridad a través del control del delito, la educación ciudadana, prevención, mediación y articulación institucional e interinstitucional como ejes centrales del servicio.

5.3.3 Principios y valores éticos

El Departamento de Policía Caquetá adopta los principios establecidos en el artículo 9º. de la Resolución 02782 del 150909. Por la cual se derogan las Resolución 05293 del 04 de diciembre de 2008, mediante la cual se fortalece el Sistema Ético Policial, se incorporan los referentes éticos: Código de Buen Gobierno; Principios y Valores Institucionales; Acuerdos y Compromisos; Código de Ética; Imperativos y Directrices Éticas, o demás normas que lo modifiquen, adicionen o deroguen.

5.3.4 Principios:

1. Vida
2. Dignidad
3. Equidad y Coherencia
4. Excelencia

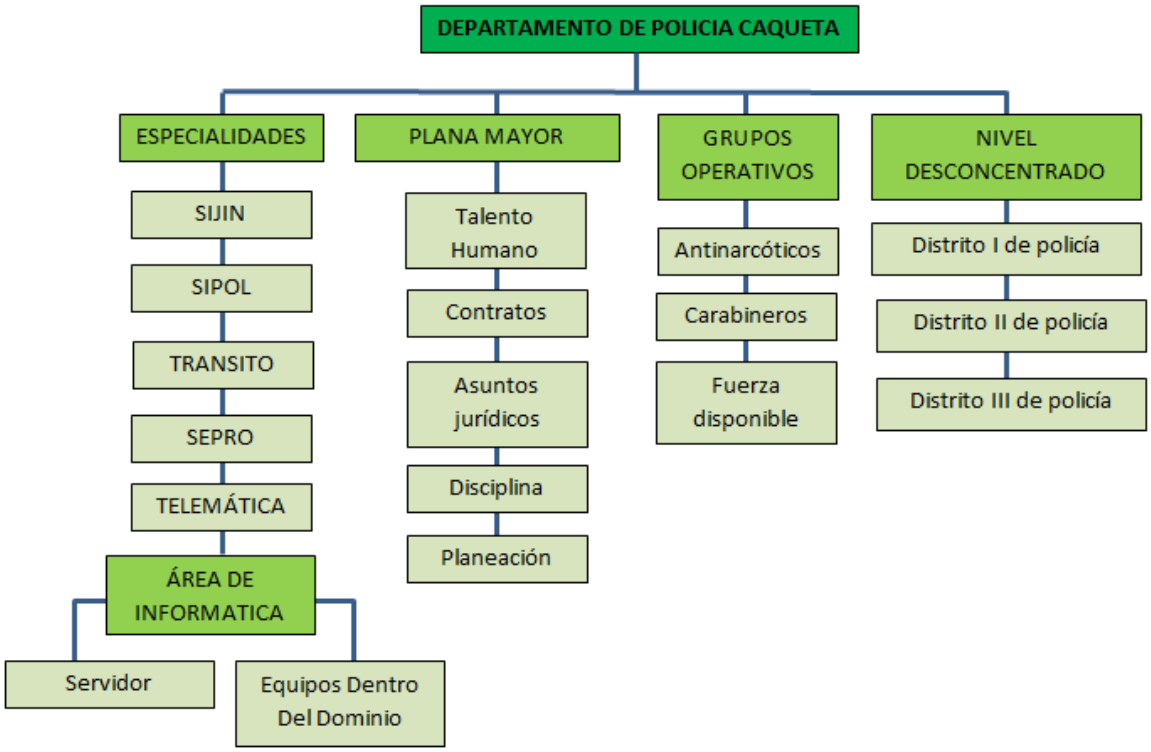
5.3.5 Valores:

1. Vocación policial
2. Honestidad
3. Compromiso
4. Honor policial
5. Disciplina
6. Solidaridad

5.3.6 Organigrama

El sistema informático y electrónico del Departamento de Policía Caquetá esta articulado entre todas las dependencias, razón por la cual la presente propuesta se sustentará en todos los activos informáticos de la unidad.

Figura 5. Organigrama Departamento de Policía Caquetá



Fuente: Autor

6. MARCO LEGAL

6.1 Ley 1273 de 2009[17]

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I
De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

[17] Ley 1273 de 2009 Nivel Nacional. 05/01/2009. Propiedad de la Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. Tomado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

7. MARCO METODOLÓGICO

Un Sistema de Seguridad Informática está constituido por diferentes medios bien sean administrativos, técnicos y humanos los cuales se interrelacionan para generar los diferentes niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

Durante el desarrollo del proyecto de Seguridad Informática y Seguridad Electrónica del Departamento de Policía Caquetá se busca en primer lugar establecer tres fases:

7.1 Fase1: Identificar las necesidades de protección del sistema informático y electrónico.

- Caracterización del sistema informático y electrónico, denotando características de procesamiento, transmisión y conservación de la información, evaluando el flujo interno y externo.
- Identificación de las amenazas y estimación de los riesgos.
- Evaluación del estado actual de la seguridad.

7.2 Fase 2: Identificar el sistema de seguridad con el propósito de minimizar los riesgos que se establezcan en la primera etapa.

- Identificar las políticas de seguridad.

7.3 Fase 3: Evaluar el sistema de seguridad actual.

- Bienes informáticos, su organización e importancia.
- Redes instaladas, estructura, tipo y plataformas que utilizan.

7.4 Fase 4: Evaluar el sistema de seguridad actual.

- Resultados del Análisis.
- Sistema de seguridad informática y electrónica
- Medios Técnicos de Seguridad
- Medidas y Procedimientos de Seguridad Informática
- Control de acceso a los activos y recursos

- Integridad de los ficheros y datos
- Seguridad de operaciones
- Controles de seguridad
- Vulnerabilidades de seguridad informática o electrónica identificadas en el departamento de Policía Caquetá
- Analizar los procesos y procedimientos establecidos en los protocolos de seguridad al interior del comando Policía Caquetá
- Informe gerencial

8. METODOLOGÌA DEL DESARROLLO

8.1 Fase 1: Identificar las necesidades de protección del sistema informático y electrónico.

8.1.1 Caracterización del sistema informático y electrónico, denotando características de procesamiento, transmisión y conservación de la información, evaluando el flujo interno y externo

El sistema informático del Departamento de Policía Caquetá, está conformado por 60 ordenadores en red sujetos a un servidor el cual se encuentra dentro de la intranet de la Policía Nacional.

Respecto al humanware, el departamento de policía Caquetá cuenta con un grupo conformado por 6 funcionarios quienes son los responsables de administrar la red local, especialmente el dominio y agilizar ante la dirección nacional, los requerimientos de fallas relacionadas respecto a la intranet y acceso a los diferentes aplicativos o sistemas de información de la policía nacional como son: SIATH (Sistema de información para la administración del talento humano) GECOP (Gestor de contenidos policiales) PSI (Portal de servicios internos) etc.

Las funciones principales de dichos funcionarios es suplir los requerimientos del DOMINIO, como usuarios y contraseñas, dificultades de acceso por políticas de seguridad, mantenimiento de computadores (preventivo y correctivo) y las fallas menores respecto el acceso al internet y la intranet.

Como políticas de seguridad se tiene restringido el acceso a internet bloqueando algunas páginas comerciales y redes sociales, de igual forma se ha implementado durante los últimos años el monitoreo del DLP “Data Loss Prevention” lo cual de cierta manera genera cultura de seguridad de la información en los funcionarios.

El DLP, tiene políticas de seguridad como control de USB, control de impresiones, control de pantallazo o print scan, control de unidad CD entre otros.

Existen protocolos establecidos para la asignación de usurarios y contraseñas, los cuales son personales y se asignan de acuerdo al cargo y perfil de cada

funcionario, teniendo en cuenta a la especialidad que pertenece y las funciones que realiza.

En el servidor se recopila toda la información que se gestiona en el comando y se guarda de acuerdo a la misión de cada especialidad, luego de procesarla y analizarla. Ésta se clasifica en información privada, restringida, secreta y ultra secreta.

De otra parte, la importancia del manejo de la información por cada dependencia radica en que éstas funcionan dentro de un sistema o engranaje que articula esfuerzos frente a los fenómenos criminales y cuyo resultado debe ser un trabajo articulado, que evite la afectación de la convivencia y seguridad ciudadana de la jurisdicción.

En cuanto a la protección de la información, cada funcionario tiene como responsabilidad proteger la información producida y recopilada como resultado de los procesos que se realizan en la Institución y está en la obligación de reportar cualquier incidente de seguridad informática que detecte.

8.1.2 Identificación de las amenazas y estimación de los riesgos.

Tabla 1. Escala de Valoración de riesgo Metodología Magerit

VALORACIÓN DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Valoración del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15

Tabla 2. (Continuación)

VALORACIÓN DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente: Metodología Magerit

Tabla 3. Valoración de Riesgo

VALORACIÓN DEL RIESGO						
IMPACTO	**MA**	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5

Tabla 2. (Continuación)

Fuente: Autor

Tabla 4. Amenazas, valoración de riesgos, controles y plan de tratamiento

Activo	Amenazas Metodología Magerit	Valoración de riesgos	Controles que se deben aplicar según el anexo a de la norma ISO 27001:2013	Plan de tratamiento de riesgos sugeridos
• Bases de datos • Data Center • Aplicaciones • Servidores • correo electrónico	[A.12] Análisis de tráfico	12	Se realiza monitoreo a todos los puertos a través de diferentes herramientas con el fin de que todos estén debidamente configurados y no quede alguno abierto punto vital en la seguridad informática.	En caso de que se detecte algún puerto abierto se debe cerrar de inmediato de igual forma si algún equipo se infecta o es remoteado se debe aislar inmediatamente de la red.
• Bases de datos • Data Center • Aplicaciones • Servidores • correo	[A.11] Acceso no Autorizado	9	El Servidor NAS debe estar en un lugar seguro, donde solo pueda ingresar personal	Copias de seguridad del servidor NAS, en caso de que algún evento llegase a ocurrir

Tabla 5. (Continuación)

Activo	Amenazas Metodología Magerit	Valoración de riesgos	Controles que se deben aplicar según el anexo a de la norma ISO 27001:2013	Plan de tratamiento de riesgos sugeridos
electrónico			autorizado, que tenga controles de acceso bien definidos, se por medio del biométrico, Token entre otros. Si se disponen de unidades de red, solo tengan acceso en forma de lectura.	solo sería restablecer los con la copia de respaldo.
• Bases de datos • Data Center • Aplicaciones • Servidores • correo electrónico	[A.6] Abuso de privilegios de acceso	16	El Servidor debe estar en un lugar seguro, donde solo pueda ingresar personal autorizado, que tenga controles de acceso bien definidos, se por medio del biométrico, Token entre otros. Solo lo debe manjar la persona encargada de Aactive Directory	Copias de seguridad del servidor NAS, en caso de que algún evento llegase a ocurrir solo sería restablecer los con la copia de respaldo.
• Bases de datos • Data Center • Aplicaciones • Servidores • correo electrónico	[A.23] Manipulación de los Equipos	9	solo pueda ser utilizadas por usuarios autorizados es decir solo los usuarios registrados a través del active	Capacitación al usuario del no uso de dispositivos extraíbles USB entre otros.

Tabla 6. (Continuación)

Activo	Amenazas Metodología Magerit	Valoración de riesgos	Controles que se deben aplicar según el anexo a de la norma ISO 27001:2013	Plan de tratamiento de riesgos sugeridos
			directory, los puertos USB se encuentran deshabilitados para la impresión y el escaneo de documento lo anterior con el fin de evitar fuga de información	
• Bases de datos • Data Center • Aplicaciones • Servidores • correo electrónico	[E.25]Perdida de Equipos	17	Todos los equipos de la empresa deben estar conectados a la red de la empresarial a través de medio guiado, las contraseñas de administrador solo la debe tener personal autorizado, los puertos USB deben estar configurados en solo lectura, el usuario debe cambiar la contraseña cada mes, esto se hará a través del directorio activo.	Se debe evaluar el alcance de la fuga de información y en que afectaría a la empresa, de igual forma se deben tomar los correctivos necesarios.

Tabla 7. (Continuación)

Activo	Amenazas Metodología Magerit	Valoración de riesgos	Controles que se deben aplicar según el anexo a de la norma ISO 27001:2013	Plan de tratamiento de riesgos sugeridos
• Bases de datos • Data Center • Aplicaciones	[E.20] Vulnerabilidad de los programas	15	Se definen los roles de los usuarios de acuerdo con labor que estos desempeñan en la empresa.	Copias de seguridad de base de datos y evaluar los roles de los usuarios
• Bases de datos • Data Center • correo electrónico	[E.19] Fugas de información	21	Debe estar en un lugar seguro, donde solo pueda ingresar personal autorizado, que tenga controles de acceso bien definidos, se por medio del biométrico, Token entre otros. Debe estar configurado correctamente con el fin de evitar accesos no autorizados.	revisar la configuración y revaluar la configuración existente
• correo electrónico	[A.12] Análisis de tráfico	20	Políticas y procedimientos de transferencia de información.	Tener los protocolos de seguridad no acordes a la necesidad.

Tabla 8. (Continuación)

Activo	Amenazas Metodología Magerit	Valoración de riesgos	Controles que se deben aplicar según el anexo a de la norma ISO 27001:2013	Plan de tratamiento de riesgos sugeridos
• Servidores	[A.6] Abuso de privilegios de acceso	5	Que estén bien configurados, que se realice un portal cautivo que permita la conexión a visitantes sin colocar en riesgo, la red empresarial y a los equipos de la compañía.	revisar la configuración y revaluar la configuración existente
• correo electrónico	[E.19] Fugas de información	25	Que estén bien configurados, que se realice un portal cautivo que permita la conexión a visitantes sin colocar en riesgo, la red empresarial y a los equipos de la compañía.	revisar la configuración y revaluar la configuración existente
• Bases de datos • Aplicaciones • Servidores • correo electrónico	[A.7] Uso no Previsto	20	autenticación de los usuarios, solo se pueda ingresar a través de equipos conectados a medios guiados	Tener en cuenta la observancia de las políticas de seguridad.

Fuente: Autor

8.1.3 Evaluación del estado actual de la seguridad.[18]

Ninguna entidad pública del Estado colombiano incluyendo la Policía Nacional, contaba con un centro de monitoreo en tiempo real de las conductas que causan incidentes de disponibilidad, integridad o confidencialidad de la información y/o las redes de datos. De igual forma, no se tenía una adecuada gestión de incidentes informáticos, evitando que se conociera de una forma eficiente la causa que los generaba.

Por otra parte, el Estado colombiano carecía de una entidad que brindara capacitación en temas de ciberseguridad, creación de equipos de respuestas a incidentes informáticos (CSIRT, CERT), de igual manera no se tenía una atención e investigación efectiva para la recuperación de éstos incidentes. Con la creación del CSIRT-PONAL, la Policía Nacional se constituye en pionera y líder de la ciberseguridad en el país.

El CSIRT- PONAL es un equipo especializado dedicado a la prevención, atención e investigación de incidentes y/o delitos informáticos. Cuenta con herramientas tecnológicas, laboratorios y metodologías basadas en estándares internacionales, dedicados a la seguridad de las tecnologías de la información.

Se enfoca en los siguientes objetivos:

- Fomentar la concientización sobre la necesidad de fijar políticas de seguridad de la información, en coordinación con los actores involucrados y usuarios de los sistemas de información a través de sensibilizaciones y eventos.
- Suministrar información que permita disminuir el impacto de vulnerabilidades y amenazas de la tecnología en el Departamento de Policía Caquetá.
- Generar estrategias de divulgación para suministrar a la comunidad un sistema de alertas tempranas, anuncios y comunicados que permitan prevenir los riesgos asociados a la seguridad de la información.

[18] ANONYMOUS. Premio Interamericano a la Innovación para la Gestión Pública Efectiva- Edición 2015. (2015). {En Línea}. {Consulta realizada en mayo del 2018} Disponible en (https://www.oas.org/es/sap/dgpe/innovacion/Banco/2015/COORDINACION/Evoluci%C3%B3n%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n%20en%20la%20Polic%C3%ADa%20Nacional.pdf)

— Proveer asistencia técnica, asesoría y apoyo a la comunidad y a las organizaciones en general, en la protección de amenazas y/o delitos informáticos.

A partir de esta iniciativa innovadora Colombia desarrolló capacidades (talento humano, doctrina, infraestructura y tecnología) que permiten afrontar las amenazas cibernéticas y los riesgos asociados, así como fortalecer las capacidades de neutralización y reacción ante incidentes o ataques informáticos que atenten contra la infraestructura crítica digital y la soberanía nacional.

En este momento, la estrategia de la Oficina de Telemática, para la vigencia 2015-2018, tiene como uno de sus pilares la seguridad de la información y la Policía Nacional tiene como uno de sus indicadores estratégicos la efectividad en la atención a incidentes informáticos y sus lecciones aprendidas, como las pruebas de resiliencia de la plataforma tecnológica institucional.

Con lo anterior, se ubica en el más alto nivel los procesos que se dedican a garantizar la confidencialidad, disponibilidad e integridad de la información y los activos críticos institucionales.

8.2 Fase 2: Identificar el sistema de seguridad con el propósito de minimizar los riesgos que se establezcan en la primera etapa.

8.2.1 Identificar las políticas de seguridad.[19]

De acuerdo a la RESOLUCIÓN No. 08310 del 28 diciembre de 2016 en su ARTÍCULO 6 la policía nacional establece como. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN lo siguiente: "La Policía Nacional de Colombia se compromete a salvaguardar sus activos de información con el fin de protegerlos de las amenazas que se ciernen sobre ellos, a través de la implementación de un Sistema de Gestión de Seguridad de la Información que permita la adecuada gestión del riesgo, la generación de estrategias de seguridad basada en las mejores prácticas y controles, el cumplimiento de

[19] DIRECTOR GENERAL DE LA POLICÍA NACIONAL DE COLOMBIA. Ministerio De Defensa Nacional Policía Nacional Dirección General. Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional. Resolución Número 08310 De 28 Dic 2016. {En Línea}. {Consulta realizada en mayo del 2018} Disponible en (http://www.policia.edu.co/sgsi/resolucion%2008310%20de%2028122016-%20manual%20sgsi.pdf)

los requisitos legales, la oportuna gestión de los incidentes, y el compromiso Institucional de mejora continua", estableciendo lo siguiente:

1. Los funcionarios de la unidad guardarán la información en EL SERVIDOR y sobre ella se garantizará la disponibilidad en caso de presentarse un daño en el equipo asignado, para las unidades que no cuentan con este servicio se dispondrá de la realización de respectivos back up coordinados por el Grupo de Telemática, la custodia de esta información será responsabilidad del dueño de los activos de información cumpliendo con las Políticas de Seguridad; la información catalogada como confidencial deberá ser guardada en medios magnéticos debidamente cifrados.

2. La Oficina de Telemática dispondrá en la carpeta de software autorizado ubicada en la intranet institucional (Polired), las copias correspondientes a los softwares utilizados por la Institución para el cumplimiento de las funciones, en caso que una unidad policial requiera la instalación de un producto que no se encuentre en este recurso, deberá contar con la autorización correspondiente del Grupo de Seguridad de la Información, el uso de programas sin su respectiva licencia e instalación sin autorización por parte del Direccionamiento Tecnológico de la Policía Nacional obtenidos por otras fuentes (internet, ejecutables portables, dispositivos USB), puede implicar materialización del riesgo por realizar acciones no autorizadas.

3. Todo software utilizado en la plataforma tecnológica debe contar con licencia y su cumplimiento debe estar acorde a las condiciones de uso establecidas.

4. El uso de dispositivos de almacenamiento masivo externo extraíble (DVD, CD, Dispositivos móviles, pendrives (USB), equipos celulares), puede generar la materialización de riesgos al ser conectados a los equipos de cómputo al llegar a transferir archivos maliciosos o generar la extracción de información Institucional no autorizada, por lo tanto la activación de los puertos USB de los equipos institucionales o conectados a la red LAN deben contar con la autorización del Grupo de Seguridad de la Información mediante previa justificación a través del Sistema de Información para la Gestión de Incidentes en TIC´s SIGMA.

5. Los usuarios son responsables de la información que administran en los equipos asignados, por lo tanto, se debe evitar el almacenamiento de información no institucional (música, videos, imágenes, software, ejecutables portables) que pueda presentar violación a derechos de autor y propiedad

intelectual, tanto en equipos de cómputo, como en servidor de archivos en los lugares donde este implementado.

6. Los funcionarios solo tendrán acceso a datos y recursos tecnológicos asignados, y serán responsables disciplinaria, administrativa y legalmente de la divulgación de información no autorizada.

7. Cada funcionario tiene como responsabilidad proteger la información contenida en documentos, formatos, y toda la producida como resultado de los procesos que se realizan en la Institución.

8. Cualquier incidente de seguridad informática debe ser reportado al grupo de Telemática de la unidad y su vez al grupo CSIRT-PONAL.

9. El uso del internet está enfocado al cumplimiento de las actividades institucionales, por lo tanto, los usuarios harán uso de los equipos y medios asignados, no se permite la conexión de dispositivos como módems externos, o equipos celulares que habilitan el acceso a internet, a no ser que se encuentre autorizado por la Oficina de Telemática para el caso de las unidades en donde el acceso a la red LAN no es viable por diferentes restricciones.

10. Los equipos de cómputo deben contar con los controles necesarios para poder acceder a los servicios de internet, como antivirus, actualizaciones y demás controles establecidos por la Oficina de Telemática.

11. Se debe ejercer un control de acceso a la red, por lo tanto, los funcionarios no usarán conexiones distintas a las que provee la Oficina de Telemática, el uso de túneles VPN o conexiones TOR como complemento de los navegadores no están autorizados, y las conexiones que se generen y se evidencien en los sistemas de control adoptados por el Direccionamiento Tecnológico tendrán las sanciones a que haya lugar.

12. Las unidades o dependencias que adquieran redes inalámbricas deben cumplir con la política y condiciones de seguridad de las redes cableadas, estas deben estar separadas de las redes LAN con el respectivo control de contenido y controles necesarios, además de estar debidamente autorizadas por la Oficina de Telemática de la Policía Nacional.

13. El acceso a redes sociales, páginas interactivas como chats se encuentra restringido por lo que solo se hará uso de las herramientas para tal fin que provee la Oficina de Telemática, en caso de ser necesario su uso para el cumplimiento de las funciones asignadas por el cargo o dependencia, debe ser solicitada previa justificación a través del Sistema de Información para la Gestión de Incidentes en TIC´s SIGMA para su respectivo análisis por parte del Grupo de Seguridad de la Información.

8.3. Fase 3: Evaluar el sistema de seguridad diseñado.

Se describirá el resultado de la caracterización realizada al sistema informático de la institución, con el objetivo de determinar qué se trata de proteger, especificando sus principales componentes y considerando entre otros:

8.3.1 Bienes informáticos, su organización e importancia.

Los bienes informáticos del comando del departamento de policía Caquetá los constituyen todos los elementos que forman su sistema: computadoras, hardware (unidades periféricas) y otros dispositivos que interpretan las instrucciones contenidas en los programas y procesan los datos en el tratamiento automático de la información (quipo de transmisión de datos).

Estos bienes están ubicados en 22 dependencias dentro del comando, en las cuales se encuentran ubicados 70 computadores (CPU) con sus respectivos dispositivos periféricos. La coordinación y control de la operación de los bienes informáticos del comando se concentra en la oficina de telemática, donde está instalado el servidor y desde donde se recopila y almacena toda la información crítica del departamento.

Estos equipos están organizados de acuerdo a la labor que cada dependencia tiene a cargo. Puede decirse que la importancia de los bienes informáticos radica en dos aspectos principales: 1- agilizan y generan mayor efectividad frente a la actividad de policía. 2- coadyuvan al deber constitucional que le atañe a la policía nacional frente a la propiedad, integridad, disponibilidad y confidencialidad de la información

8.3.2 Redes instaladas, estructura, tipo y plataformas que utilizan.

Dadas las condiciones de seguridad que debe mantener, el comando del departamento de Policía Caquetá, dispone de una Red Local o LAN, sistema de

comunicaciones que permite la interconexión de los computadores operados desde las diferentes dependencias y oficinas con el servidor.
Estructura de la red:

Figura 6. Estructura de la red

Fuente: Misión, visión, mega, valores, principios, y funciones. Policía Nacional. {En Línea}. Disponible en (https://www.infonovedad.com/wp-content/uploads/2017/08/red-lan-tipo-estrella.jpg)

Además, se maneja una red inalámbrica que se encuentra conectada a la red LAN.

La utilización de la red de internet es muy limitada, solo algunas dependencias tienen ingreso, con restricción para algunas páginas y su uso es estrictamente para labores que estén relacionadas con las actividades institucionales. También se restringe el uso de dispositivos de almacenamiento masivo externo, ya que pueden generar la materialización de riesgos al ser conectados a los equipos institucionales.

8.4 Fase 4: Evaluar el sistema de seguridad actual.

8.4.1 Resultados del Análisis.

Partiendo de la particularidad de que un “análisis” es un examen detallado de una cosa para conocer sus características o cualidades, o su estado, se hace necesario esbozar las siguientes recomendaciones según lo encontrado:

—Cuáles son los activos y recursos más importantes de la institución objeto de estudio que ameritan una atención especial desde el punto de vista de la protección.
—Cuáles son las principales amenazas que actúan sobre los activos y recursos establecidos en el análisis indicando la probabilidad de materializarse.
—Cuáles son los activos, recursos y áreas con una mayor vulnerabilidad en materia de seguridad informática y electrónica.

8.4.2 Sistema de seguridad informática y electrónica

Se analiza cómo se debe de implementar, en las áreas a proteger, las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, atendiendo a sus formas de ejecución, periodicidad, personal participante y medios.

Se describen por separado los controles de seguridad implementados en correspondencia con su naturaleza, de acuerdo al empleo que se haga de los medios humanos, de los medios técnicos o de las medidas y procedimientos que debe cumplir el personal.

8.4.3 Medios Técnicos de Seguridad:

Los medios técnicos utilizados en función de garantizar los niveles de seguridad adecuados, tanto al nivel de software como de hardware, así como la configuración de los mismos. Deben de tener en cuenta:

— Sistemas Operativos y nivel de seguridad instalado.
— Tipo de redes utilizadas y topología de las mismas.
— Conexiones a redes externas a la entidad.
— Servidores de uso interno y externo.
— Configuración de los servicios.
— Barreras de protección y su arquitectura.
— Empleo de Firewall, de Hosts Bastiones, Sistemas Proxy, etc.
— Filtrado de paquetes.
— Herramientas de administración y monitoreo.
— Habilitación de trazas y subsistemas de auditoría.
— Establecimiento de alarmas del sistema.
— Sistemas de protección criptográfica.

— Dispositivos de identificación y autenticación de usuarios.
— Protección contra programas no deseados.
— Software especial de seguridad.
— Medios técnicos de detección de intrusos.
— Cerraduras de disqueteras.
— Dispositivos de protección contra robo de equipos y componentes.
— Fuentes de respaldo de energía eléctrica.
— Medios contra incendios.
— Medios de climatización.

8.4.4 Medidas y Procedimientos de Seguridad Informática

Corresponde a las acciones que deben ser realizadas en cada área específica por el personal, adecuando las mismas a las necesidades de protección de cada una de ellas, de acuerdo con el peso del riesgo estimado para cada bien informático objeto de protección, además del procedimiento de seguridad es una secuencia predeterminada de acciones dirigida a garantizar un objetivo de seguridad. Los procedimientos deben de ser los siguientes:

— Secuencia de las acciones a realizar.
— Especificando en cada caso: qué se hace, cómo se hace y quién lo hace, así como los recursos que sean necesarios para su cumplimiento.
— Algunos procedimientos a considerar son los siguientes:
— Otorgar (retirar) el acceso de personas a las tecnologías de información y como se controla el mismo.
— Asignar (retirar) derechos y permisos sobre los ficheros y datos a los usuarios.
— Autorizar (denegar) servicios a los usuarios. (Ejemplo: Correo Electrónico, Internet)
— Definir perfiles de trabajo.
— Autorización y control de la entrada/salida de las tecnologías de información.
— Gestionar las claves de acceso considerando para cada nivel el tipo de clave atendiendo a su longitud y composición, la frecuencia de actualización, quién debe cambiarla, su custodia, etc.
— Realización de salva de respaldo, según el régimen de trabajo de las áreas, de forma que las salvas se mantengan actualizadas, y las acciones que se adoptan para establecer la salvaguarda de las mismas, de forma que se garantice la compartimentación de la información según su nivel de confidencialidad.
— Garantizar que los mantenimientos de los equipos, soportes y datos, se realicen en presencia y bajo la supervisión de personal responsable y que en caso del traslado del equipo fuera de la entidad la información clasificada o limitada sea borrada físicamente o protegida su divulgación.

— Salva y análisis de registros o trazas de auditoria, especificando quien lo realiza y con qué frecuencia.

8.4.5 Control de acceso a los activos y recursos

Se analizarán las medidas y procedimientos que aseguran el acceso autorizado a los activos de información y recursos informáticos que requieren la imposición de restricciones a su empleo, especificando:

— A que activos y recursos se le implementan medidas de control de acceso.
— Métodos de control de acceso utilizados.
— Quien otorga los derechos y privilegios de acceso.
— A quien se otorgan los derechos y privilegios de acceso.
— Como se otorgan y suspenden los derechos y privilegios de acceso.

8.4.6 Integridad de los ficheros y datos

Medidas y procedimientos establecidos con el fin de evitar la modificación no autorizada, destrucción y pérdida de los ficheros y datos, así como para impedir que sean accedidos públicamente, teniendo en cuenta lo siguiente:

— Medidas de seguridad implementadas a nivel de sistemas operativos, aplicación o ambos para restringir y controlar el acceso a las bases de datos.
— Medidas para garantizar la integridad del software y la configuración de los medios técnicos.
— Empleo de medios criptográficos para la protección de ficheros y datos.
— Medidas y procedimientos establecidos para la protección contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para evitar su generalización, especificando los programas antivirus utilizados y su régimen de instalación y actualización.

8.4.7 Seguridad de operaciones

Las medidas y procedimientos relacionados deben contener los siguientes aspectos:

— Identificación y control de las tecnologías en explotación, en particular aquellas donde se procese información clasificada.

- Control sobre la entrada y salida en la entidad de las tecnologías de información (máquinas portátiles, periféricos, soportes, etc.).
- Metodología establecida para las salvas de la información, especificando su periodicidad, responsabilidades, cantidad de versiones, etc.)
- Acciones específicas durante las conexiones externas a la entidad.
- Autorizar (denegar) servicios a los usuarios. (Ejemplo: Correo Electrónico, Internet)
- Gestión de las claves de acceso considerando para cada nivel el tipo de clave, la frecuencia de actualización, quién debe cambiarla, su custodia, etc.
- Gestión de salvas de respaldo, según el régimen de trabajo de las áreas, incluyendo las acciones que se adoptan para establecer la salvaguarda de las mismas.
- Mantenimientos de los equipos, soportes y datos en presencia y bajo la supervisión de personal responsable y en caso del traslado de equipos fuera de la entidad.
- Salva y análisis de registros o trazas de auditoria, especificando quien lo realiza y con qué frecuencia.

8.4.8 Controles de seguridad

Los controles existentes en las instalaciones se han clasificado en tres tipos para realizar un análisis detallado y objetivo de las vulnerabilidades:

Tabla 9. Controles de seguridad

CONTROLES	
Controles físicos	Cámaras de circuito cerrado Sistemas de alarmas Centinelas (Guardas de seguridad) Puertas de acero con seguros especiales Identificación avanzada - Biométrica (huellas digitales, voz, rostro, iris, o métodos automatizados).
Controles técnicos	Encriptación Software de control Data Loss Prevention Restricción de puertos
Controles administrativos	Entrenamiento y conocimiento Planes de contingencia Registros de ingreso (libros).

Fuente: Autor

8.4.9 Vulnerabilidades de seguridad informática o electrónica identificas en el departamento de policía Caquetá.

Tabla 10. Vulnerabilidades del Departamento de Policía Caquetá

Amenazas	Activos de tecnología que pueden ser afectado	Vulnerabilidades	Riesgo
Acceso no autorizado	• Bases de datos • Data Center • Aplicaciones • Servidores • correo electrónico	Falta de controles de accesos adecuados por parte de los funcionarios. La configuración incorrecta de permisos y roles a usuarios de acuerdo a sus obligaciones. Falta de configuración de una red segura con los estándares actualizados. El uso de contraseñas no seguras. La incorrecta configuración de las cuentas de perfiles de los usuarios. Falta de seguridad de los puertos de red Falta de implementación Políticas no aplicada o la no existencia de seguridad.	Robo y/o pérdida de la información por el ingreso de personal no autorizado a la información confidencial, debido a la falta de controles de seguridad. Instalación de software malicioso.
Ataques externos / internos (hacking no ético)	• Bases de datos • Servidor •Correo electrónico • Computadores	Falta de controles de accesos adecuados por parte de los funcionarios. Falla de seguridad en los componentes de red	
Cambio de privilegios sin autorización	• Bases de Datos • Directorio Activo • Servidores • Correo electrónico	El uso de contraseñas no segura La mala administración de Asignación de roles y permisos. faltas de políticas de seguridad Falta de monitoreo de acceso	

Tabla 5. (Continuación)

Amenazas	Activos de tecnología que pueden ser afectado	Vulnerabilidades	Riesgo
Divulgación de información de autenticación	• Bases de Datos • Directorio Activo • Computadores	Inadecuada Administración de Seguridad Contraseñas no seguras Falta de capacitación a funcionarios finales sobre seguridad informática. Inadecuada Administración o Asignación de roles y permisos Inadecuado mecanismo de cifrado.	
Instalación de software no autorizado	• Directorio Activo • Computadores	Políticas no aplicada o no existencia de seguridad Inadecuada Administración o Asignación de roles y permisos	
Interceptación no autorizada de información en tránsito	• Red WAN • correo electrónico	Políticas no aplicada o no existencia de seguridad Inadecuado mecanismo de cifrado	
Modificación sin autorización	• Bases de datos • Directorio Activo • Servidores • Correo electrónico.	• Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos • Inadecuado mecanismo de cifrado	
Robo de información	• Bases de datos • Directorio Activo • Servidor • Computadores	• Inadecuada Administración de Seguridad • Políticas no aplicada o no existencia de seguridad • Inadecuada Administración o Asignación de roles y permisos • Inadecuado mecanismo de cifrado • Contraseñas no seguras	

Tabla 5. (Continuación)

Amenazas	Activos de tecnología que pueden ser afectado	Vulnerabilidades	Riesgo
Error del administrador	• Bases de datos • Directorio Activo • Red WAN • Servidores • Servicios de correo electrónico	Ausencia de capacitación permanente Ausencia o inadecuado procedimiento de control de cambios Desmotivación del personal	Deficiencia en la prestación de los servicios.
Uso inadecuado de sistemas que generan interrupción	• Bases de datos • Directorio Activo • Red WAN Servidores • Servicios correo electrónico	• Inadecuada Administración de Seguridad • Cuentas de usuario sin auditar • Inexistencia de Logs de eventos de seguridad • Inadecuada Administración o Asignación de roles y permisos • Políticas no aplicada o no existencia de seguridad	
Interrupción de otros servicios y Suministros esenciales	• Computadores • Impresora • Video vid	• Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante, etc.	
Corte de suministro eléctrico	• Computadores • Impresora • Video vid	Cese de la alimentación de potencia.	
Contaminación Mecánica	• Computadores • Impresora • Mobiliario • Video vid	Polvo suciedad.	

Fuente: Autor

La utilización de las nuevas tecnologías y los diferentes recursos informáticos, en las técnicas de procesos de información, conllevan a que el campo informático respecto a la seguridad tenga más eficacia, teniendo así que implementar nuevos procedimientos que ayuden a ofrecer un control en el sistema los nuevos contextos del mercado.

Es así como los procesos más relevantes hoy en día ayudan al descubrimiento de riesgos, vulnerabilidades, fallas y/o amenazas, y no solo relacionan sus causas

sino las posibles soluciones, por lo tanto es necesario estar actualizado con los nuevos estándares como lo son MAGERIT utilizado para el estudio de peligros informáticos, actualmente encargado del análisis de riesgos de procesos, el cual es el más avanzado para establecer amenazas en el uso de la tecnología de la información (TI).

Teniendo en cuenta lo anterior, la realización de la identificación de los riesgos y la implementación de diversos controles informáticos en el departamento de policía del Caquetá es de suma importancia ya que está relacionado con la perspicacia de procesos y los conocimientos que se realizan para construir las políticas, estrategias, procedimientos y planes que conlleven al mejoramiento de los activos informáticos.

Una de las situaciones con las que más se debe de tener cuidado son las amenazas, ya que estas son los sucesos que causan desastres en un sitio en específico, muchas veces de manera irreparable, ya que este es un peligro recóndito del sistema que se encuentra expuesto, el cual es de manera indeterminado.

Actualmente se conoce una amenaza informática como una amenaza en el sistema, el cual puede ser causando por alguna persona conocida hoy en día en el mundo de las tecnologías como cracker, además también puede ser causado por un virus o un desastre natural, los cuales se aprovechan de las vulnerabilidades del sistema.

Otro aspecto muy importante que se debe de tener en cuenta son las vulnerabilidades, este es un factor interno que es causado por la pérdida de información a causa de algunas debilidades del sistema convirtiéndose en una amenaza para ello en el departamento de policía del Caquetá.

8.4.10 Analizar los procesos y procedimientos establecidos en los protocolos de seguridad al interior del comando policía Caquetá.

8.4.10.1 Acceso a la información

El acceso a la información se encuentra restringido bajo dos parámetros de seguridad:

1. Protocolo de seguridad para ingreso a la intranet corporativa, lo cual presenta un nivel acertado de seguridad.

2. Una vez en la intranet, se encuentra el monitoreo del servidor DLP, y el control del dominio, lo cual fortalece la seguridad, no obstante, se presentan algunas situaciones susceptibles de mejoras al interior de la red, donde es posible que algunos funcionarios acceden a información privilegiada de otras oficinas, cuya principal responsabilidad radica en la en la asignación de privilegios en los usuarios, donde solo se permite borrar la información a los administradores. Para el caso en particular, es necesario suministrar el permiso de borrado a todos los usuarios para que compartan y eliminen dentro de la red, pero solo la información que les corresponde.

8.4.10.2 Seguridad de la información

Aunque la entidad ha implementado el Data Loss Prevention (servidor DLP) desde hace tres años, lo cual aborda un monitoreo constante existen, comportamientos en el personal lo cual genera vulnerabilidades en el tratamiento de la información.

Dentro de la red corporativa existen “carpetas compartidas” cuyo dominio de administrador restringe algunos privilegios obligando al dueño de la información a dejarla a la deriva en la red.

No existe capacitación a los funcionarios, lo que obliga a en conocimiento empírico generando escenarios vulnerables para la seguridad informática.

8.4.10.3 Seguridad en los servicios tecnológicos

No existen protocolos de cifrado de la información, no hay control para el envió o recepción de datos a través de los correos personales de los funcionarios, brindando la oportunidad de descargar archivos potencialmente ofensivos para la red.

8.4.10.4 Administración de usuarios

Existe un control acertado para la asignación de usuarios, pero, existe una cultura generalizada de préstamo de usuarios de red, lo cual vulnera la estrategia de

seguridad y monitoreo, a la vez que dificulta la identificación de los verdaderos responsables en caso de fuga o pérdida de información.

8.4.10.5 Rol de Usuario

Los sistemas de información representados en los diferentes aplicativos (bases de datos) de dominio de la policía nacional, cuentan con un estándar de seguridad alto, cuyo protocolo establece compromisos y responsabilidades en la asignación de usuarios, para la activación del mismo, desde la ciudad de Bogotá.

9. DESARROLLO DEL INFORME

Tabla 11. Desarrollo del informe

	ANÁLISIS DE VULNERABILIDADES EN EL SISTEMA DE SEGURIDAD FÍSICO E INFORMÁTICO DEL DEPARTAMENTO DE POLICÍA CAQUETÁ.

1. Objetivo

Presentar el análisis de las vulnerabilidades del sistema informático y electrónico al comandante del departamento de policía del Caquetá.

2. Desarrollo

Teniendo en cuenta el análisis del sistema informático y electrónico del departamento de policía Caquetá, se da a conocer la apreciación y valoración de los intervinientes respecto a los riesgos y vulnerabilidades en la unidad.

Al observar la parte doctrinal, de políticas y protocolos de seguridad informática, se encuentran unos procesos y procedimientos altamente robustos en materia de seguridad, no obstante, es apreciable diversas vulnerabilidades en la actuación del personal y bajo control para verificar el cumplimiento y acatamiento de las políticas establecidas, las vulnerabilidades identificadas son las siguientes:

- Falta capacitación y concientización en los funcionarios policiales frente a la seguridad informática y electrónica, lo que vulnera las políticas de seguridad evidenciando mal uso de algunos equipos.
- La mayoría del software no tiene la respectiva licencia lo que constituye una vulnerabilidad factible en cuando a los ataques.
- Se aprecian equipos en estado avanzado de deterioro y ausencia de aseo, evidenciando que no existen planes de mantenimiento lo que podría generar fallas dejando al sistema desprotegido o inoperable.
- Los controles físicos son de mediana seguridad bajo el entendido que se presenta facilidad al accedo de los equipos de cómputo permitiendo una posible instalación de dispositivos para extraer información.

Tabla 6. (Continuación)

3. Recomendaciones

— El departamento de policía Caquetá debería capacitar periódicamente al personal sobre el manejo de los medios informáticos con que cuenta la unidad haciendo énfasis en el correcto uso de los usuarios y su respectiva contraseña a la hora de acceder tanto a la plataforma como al dominio de la Institución.

— Suministrar soporte y asistencia técnica inmediata a los funcionarios. Dicho procedimiento actualmente tarda en promedio dos o tres días, lo que incita al funcionario que tiene asignado el equipo a tratar de resolver el incidente por sus propios medios, situación que en ocasiones pone en riesgo el sistema informático de la unidad.

— Fijar una periodicidad de revista o auditoria frente al control de las políticas de seguridad establecidas (existen las políticas, pero pocas veces se verifica su cumplimiento).

— Es perentorio unificar un servidor para las unidades desconcentradas del departamento de policía Caquetá, dicha medida se presenta a razón que actualmente cada una de las 16 estaciones de policía, almacena la información en su respectivo equipo de cómputo sin las medidas de seguridad necesarias ni copias de respaldo que garanticen la disponibilidad de la misma, y la base del departamento de policía, se encuentra sometido a la LAN, con el servicio del SERVIDOR y con mayores políticas de seguridad.

— Ejercer control sobre las redes inalámbricas que se encuentran en la unidad, y están conectadas a la LAN.

— Se debería implementar el manejo de usuario en el dominio por grupos ya que actualmente se maneja la configuración de manera individual lo que dificulta realizar cambios globales inmediatos sobre las políticas de seguridad que ya se encuentran implantadas en casos como detección de brechas de seguridad, o actualización de políticas.

— Se deberían crear zonas restringidas para las ubicaciones de los dispositivos más importantes de la infraestructura informática de la Institución como lo son los servidores DNS y Proxy que se encuentran dentro del comando, al igual que los puntos de acceso, routers y Switchs, ya que se deberían encontrar en habitaciones aisladas protegidas por cerraduras de seguridad, chasis certificados, evitar las emisiones y

Tabla 6. (Continuación)

recepciones electromagnéticas de los mismos.

— se sugiere que exista un servidor de respaldo por fuera de la unidad policial con el fin de garantizar la disponibilidad de la información cuando pueda verse afectada por desastres o similares.

— Implementar un servidor de dominio raíz que administre los diferentes servidores de las unidades policiales, con el fin de que solo los usuarios autorizados puedan tener acceso a los activos y recursos con que cuenta el departamento de policía Caquetá y evitar que terceros malintencionados accedan a los recursos de la institución sin autorización previa.

— Se deberían implementar medidas y procedimientos para llevar un registro y análisis de las trazas de auditoría en las redes y sistemas instalados, con el fin de monitorear las acciones que se realicen (acceso a ficheros, dispositivos, empleo de los servicios, etc.), y detectar indicios de hechos relevantes a los efectos de la seguridad que puedan afectar la estabilidad o el funcionamiento del sistema informático.

4. Conclusiones

— Entre los principales problemas evidenciados, relacionados con la seguridad informática en el comando de Policía Caquetá, están la obsolescencia de algunos de los equipos instalados, estado de deterioro y la inexistencia de planes de mantenimiento lo que podría maximizar el nivel de fallas dejando al sistema desprotegido o inoperable.

— No se evidencian planes de capacitación y concientización en los funcionarios policiales frente a la seguridad informática y electrónica, los cual harían más eficientes los controles físicos y menos constante la posibilidad de instalación de dispositivos para extraer información.

— Los procesos de soporte y asistencia técnica son muy demorados, en la mayoría de los casos tardan en promedio dos o tres días, lo que obliga al funcionario que tiene asignado el equipo a tratar de resolver el incidente por sus propios medios, situación que en ocasiones pone en riesgo el sistema informático de la unidad.

— Las 16 estaciones municipales de policía almacenan la información de manera independiente sin copias de respaldo que garanticen su seguridad y disponibilidad. Por lo que se hace perentorio unificar un servidor para las unidades desconcentradas del departamento de policía Caquetá.

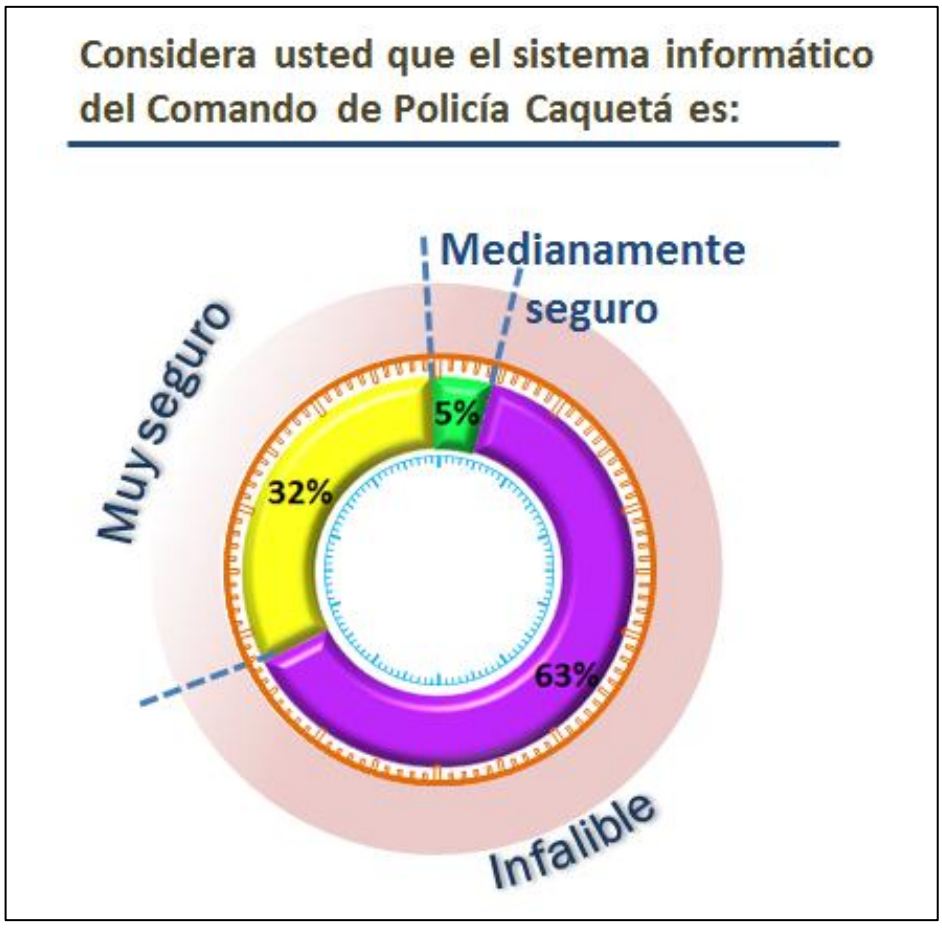
Fuente: Autor

10. RESULTADOS OBTENIDOS

10.1 Análisis de la encuesta

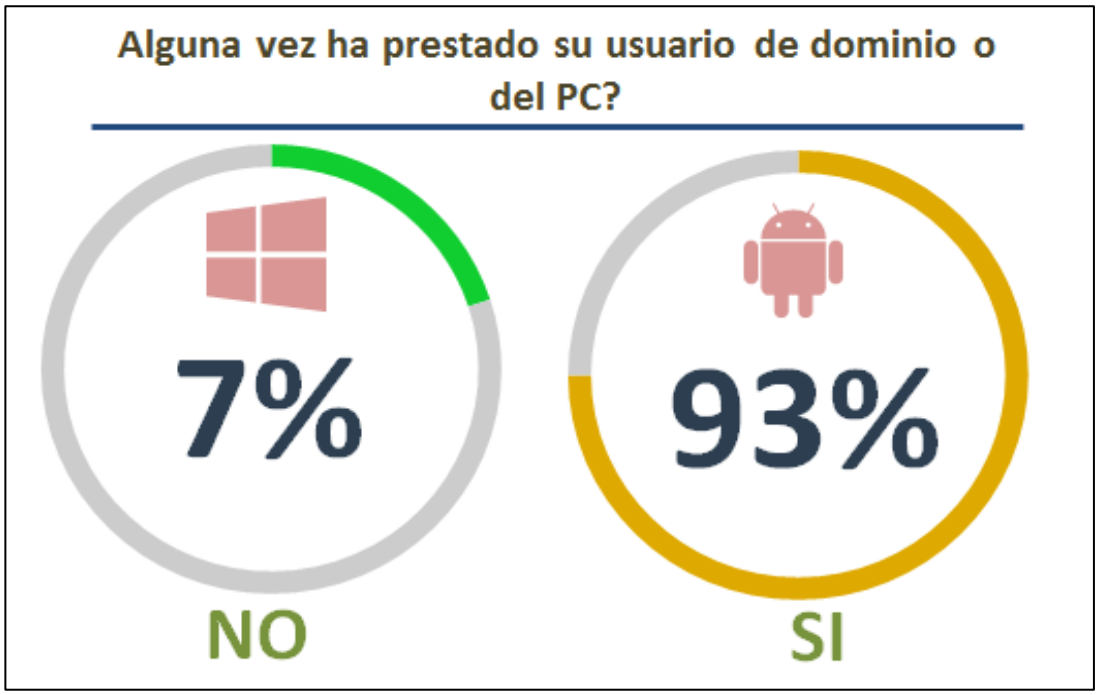
Con el propósito de establecer la percepción de seguridad informática en la base del departamento del Caquetá, se adelantó una encuesta personalizada a 100 funcionarios aleatoriamente, lo que representa una muestra poblacional del 30% de la unidad.

Figura 7. Pregunta 1



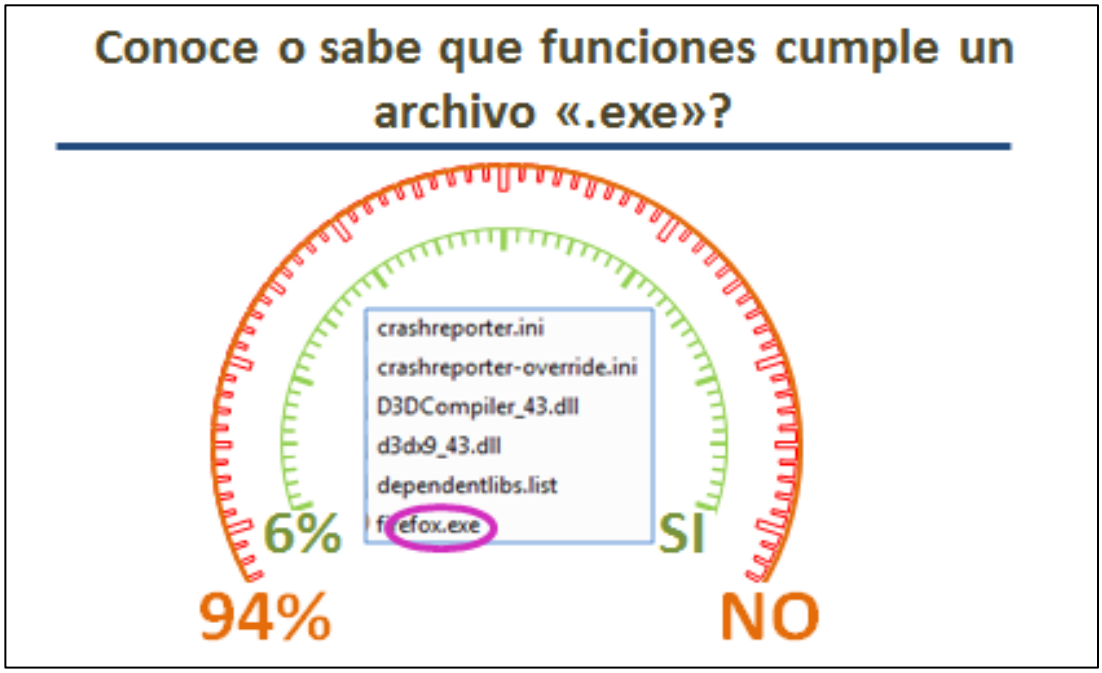
Fuente: Autor

Figura 8. Pregunta 2



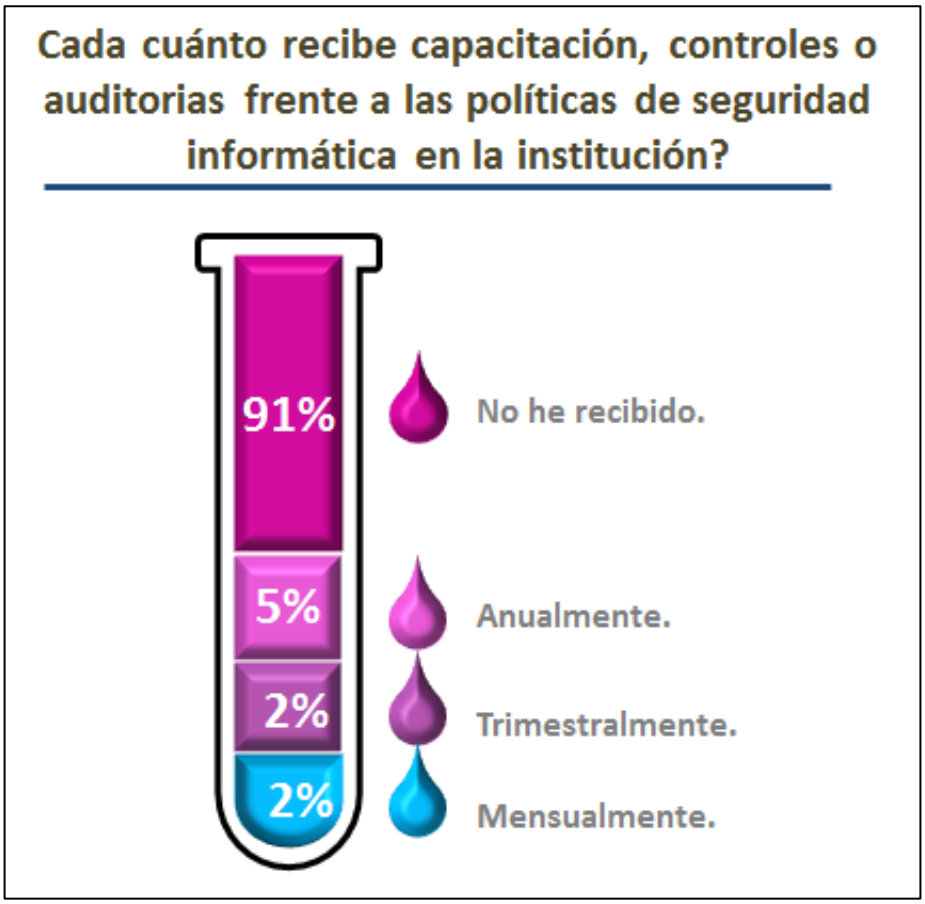
Fuente: Autor

Figura 9. Pregunta 3



Fuente: Autor

Figura 10. Pregunta 4



Fuente: Autor

10.2 Análisis a las respuestas de la encuesta.

- El hecho de que los encuestados consideren que el sistema informático en el departamento de policía del Caquetá es infalible, representa un riesgo mayor al tener en cuenta que es poca su preocupación para salvaguardar la seguridad informática de la unidad.
- La cultura y falta de responsabilidad en el manejo de los usuarios personales, constituyen otro punto crítico en el manejo de la seguridad de la información.
- Los encuestados no reconocen el potencial riesgo que representan los archivos .exe, siendo este una de las principales formas de ataque a través de archivos con nombres llamativos y que luego resultan ser ejecutables.
- La falta de capacitación en el personal, el control y la auditoría, ponen en riesgo los protocolos con que cuenta la unidad, porque el personal los desconoce haciendo más fácil su aplicabilidad.

11. CONCLUSIONES

Entre los principales problemas evidenciados, relacionados con la seguridad informática en el comando de Policía Caquetá, están la obsolescencia de algunos de los equipos instalados, estado de deterioro y la inexistencia de planes de mantenimiento lo que podría maximizar el nivel de fallas dejando al sistema desprotegido o inoperable.

No se evidencian planes de capacitación y concientización en los funcionarios policiales frente a la seguridad informática y electrónica, los cual harían más eficientes los controles físicos y menos constante la posibilidad de instalación de dispositivos para extraer información.

Los procesos de soporte y asistencia técnica son muy demorados, en la mayoría de los casos tardan en promedio dos o tres días, lo que obliga al funcionario que tiene asignado el equipo a tratar de resolver el incidente por sus propios medios, situación que en ocasiones pone en riesgo el sistema informático de la unidad.

Las 16 estaciones municipales de policía almacenan la información de manera independiente sin copias de respaldo que garanticen su seguridad y disponibilidad. Por lo que se hace perentorio unificar un servidor para las unidades desconcentradas del departamento de policía Caquetá.

12. RECOMENDACIONES

El departamento de policía Caquetá debería capacitar periódicamente al personal sobre el manejo de los medios informáticos con que cuenta la unidad haciendo énfasis en el correcto uso de los usuarios y su respectiva contraseña a la hora de acceder tanto a la plataforma como al dominio de la Institución.

Suministrar soporte y asistencia técnica inmediata a los funcionarios. Dicho procedimiento actualmente tarda en promedio dos o tres días, lo que incita al funcionario que tiene asignado el equipo a tratar de resolver el incidente por sus propios medios, situación que en ocasiones pone en riesgo el sistema informático de la unidad.

Fijar una periodicidad de revista o auditoria frente al control de las políticas de seguridad establecidas (existen las políticas, pero pocas veces se verifica su cumplimiento).

Es perentorio unificar un servidor para las unidades desconcentradas del departamento de policía Caquetá, dicha medida se presenta a razón que actualmente cada una de las 16 estaciones de policía, almacena la información en su respectivo equipo de cómputo sin las medidas de seguridad necesarias ni copias de respaldo que garanticen la disponibilidad de la misma, y la base del departamento de policía, se encuentra sometido a la LAN, con el servicio del SERVIDOR y con mayores políticas de seguridad.

Ejercer control sobre las redes inalámbricas que se encuentran en la unidad, y están conectadas a la LAN.

Se debería implementar el manejo de usuario en el dominio por grupos ya que actualmente se maneja la configuración de manera individual lo que dificulta realizar cambios globales inmediatos sobre las políticas de seguridad que ya se encuentran implantadas en casos como detección de brechas de seguridad, o actualización de políticas.

Se deberían crear zonas restringidas para las ubicaciones de los dispositivos más importantes de la infraestructura informática de la Institución como lo son los servidores DNS y Proxy que se encuentran dentro del comando, al igual que los puntos de acceso, routers y Switchs, ya que se deberían encontrar en

habitaciones aisladas protegidas por cerraduras de seguridad, chasis certificados, evitar las emisiones y recepciones electromagnéticas de los mismos.

Se sugiere que exista un servidor de respaldo por fuera de la unidad policial con el fin de garantizar la disponibilidad de la información cuando pueda verse afectada por desastres o similares.

Implementar un servidor de dominio raíz que administre los diferentes servidores de las unidades policiales, con el fin de que solo los usuarios autorizados puedan tener acceso a los activos y recursos con que cuenta el departamento de policía Caquetá y evitar que terceros malintencionados accedan a los recursos de la institución sin autorización previa.

Se deberían implementar medidas y procedimientos para llevar un registro y análisis de las trazas de auditoría en las redes y sistemas instalados, con el fin de monitorear las acciones que se realicen (acceso a ficheros, dispositivos, empleo de los servicios, etc.), y detectar indicios de hechos relevantes a los efectos de la seguridad que puedan afectar la estabilidad o el funcionamiento del sistema informático.

13. BIBLIOGRAFÍA

BARÓN. Carlos. Metodología de análisis de vulnerabilidades para la red de Datos en la dirección de telemática de la policía nacional. Universidad militar nueva granada Facultad de Ingeniería Programa de ingeniería en telecomunicaciones. Bogotá, 2010, 92p. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://unimilitar-dspace.metabiblioteca.org/bitstream/10654/502/1/BaronDuquezCarlos2010.pdf)

CASTRO. Dubán. ROJAS. Ángela. Riesgos, amenazas y vulnerabilidades de los sistemas de Información geográfica. Universidad católica de Colombia. Bogotá. (2013). 83p. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZAS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf)

CUTTER, S.L. (1996 b) "Vulnerability to environmental hazards", Progress in Human Geography, vol. 20, nº 4, pp. 529-539

DAI, MURPHY, y KAISER, Configuration Fuzzing forSoftware Vulnerability Detection, 2010 International Conference onAvailability, Reliability and Security, 525-530 (2010)

DÍAZ. María. DÍAZ. Concepción. El análisis de la vulnerabilidad en la cartografía de riesgos tecnológicos: algunas cuestiones conceptuales y metodológicas. Departamento de Geografía. Universidad de Alcalá. (2002). {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en https://core.ac.uk/download/pdf/58902381.pdf

FRANCO, David A, PEREA, Jorge L, & TOVAR, Luis C. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Vulnerability Detection Tool using Banner Grabbing. Información tecnológica, Inf. tecnol. vol.24 no.5 La Serena 2013. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (https://dx.doi.org/10.4067/S0718-07642013000500003)

FRANCO, D. A., PEREA, J. L., & PUELLO, P. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. *Información tecnológica*, *23*(3),

113-120.
Gil, R. G. Seguridad en VoIP: Ataques, amenazas y riesgos. (2012). Universidad de València. {En Línea}. {Consulta realizada en noviembre del 2017} (http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html.)

GUAYARÁ. Natalia. Sistema de información gerencial. Componentes de un sistema de información gerencial. (2014). {En Línea}. {Consulta realizada en diciembre del 2017} Disponible en http://natalia-guayaragestionempresarial.blogspot.com.co/2014/11/componentes-de-un-sistema-de.html

GARZÓN. Daniel. RATKOVICH. Juan. VERGARA. Alejandro. Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala. Bogotá. Pontificia Universidad Javeriana. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf)

ISO (*International Organization for Standardization*), ISO 27000 -1 Seguridad de la Información. ISO, 2009. {En Línea}. {Consulta realizada en noviembre del 2017}. Disponible en: (http://www.iso.org/iso/home.htm)

JONASSEN, David. Objetivismo vs. Constructivismo: ¿Necesitamos un nuevo paradigma filosófico? Tecnología Educativa: Investigación y Desarrollo. Capítulo 10. El diseño de entornos constructivistas de aprendizaje. (2000). Madrid: Mc Graw Hill. Disponible en: (https://es.slideshare.net/edmundo126/diseo-de-entornos-constructivista-de-aprendizaje-u-iii), agosto de 2017.

KENDALL, Kenneth y KENDALL, Julie. Análisis y diseño de sistemas. Sexta Edición. Pearson Educación. (2005)

LÓPEZ, Aguilera. Seguridad informática. Editex. P10. {En Línea}. {Consulta realizada en diciembre del 2017} Disponible en http://webcache.googleusercontent.com/search?q=cache:Ga9MXrYwWlwJ:www.editex.es/RecuperarFichero.aspx%3FId%3D19810+&cd=1&hl=es&ct=clnk&gl=co

MIFSUD. Elvira. Introducción a la seguridad informática - Vulnerabilidades de un sistema informático. Software – General. (2012). {En Línea}. {Consulta realizada

en noviembre del 2017} Disponible en (http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3)

POLO, B., & Cuevas, J. L. Peligbas: Sistema de Base de Datos de Peligros, Vulnerabilidad a Riesgos Geológicos y Tecnológicos inducidos. Herramienta para la gestión y el manejo de los peligros geológicos en el macizo montañoso de Guamuhaya. Memorias GEOCIENCIAS 2005 (I Convención Cubana de Ciencias de la Tierra–I Simposio de Sismicidad y Riesgos Geológicos), La Habana, 5-8 Abril. ISBN 959-7117-03-7, GEO2-16 10 pp.

REYES. Edgar. Elementos vulnerables en el sistema informático: hardware, software y datos. Seguridad informática. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://www.actiweb.es/reyes_278/archivo3.pdf)

REVISTA SEMANA. Anonymous Colombia ataca página web de la Policía por "abuso de autoridad" en marchas. Bogotá. (13 de Octubre, 2012). P.1

SANTANA. Carlos. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. (2012). {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo)

TUTORIAL DE SEGURIDAD INFORMÁTICA. Amenazas y vulnerabilidades. {En Línea}. {Consulta realizada en noviembre del 2017} Disponible en (http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html)

ZHANG, LIU, LEI, y KUNG, CSALLNER, NYSTROM y WANG. *SimFuzz: Test case similarity directed deep fuzzing*, Journal of Systems and Software, *85*(1), 102-111 (2012a).

ANEXOS

Anexo A. Autorización

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN DE INTELIGENCIA POLICIAL
SECCIONAL CAQUETÁ

TODOS POR UN NUEVO PAÍS

MINISTERIO DE DEFENSA
POLICIA NACIONAL
Unidad: DEIN-COINT
Radicado No:
Recibido por:
Fecha: 08-03-18 Hora: 12:30

No. S-2018-009987 / SIPOL – GRUCO – 29

Florencia, 08 de marzo de 2018

Coronel
JAVIER NAVARO ORTIZ
Comandante Departamento de Policía Caquetá
Calle 10ª 11-40 Barrio juan XXIII
Florencia, Caquetá

Autorizado
Jefe Telematica
Supervisor

Asunto: solicitud para realizar proyecto de seguridad informática

Teniendo en cuenta la conversación adelantada en el pasado mes de octubre, respetuosamente solicito a mi coronel estudie la posibilidad de autorizar al suboficial **ANDRES FERNEY VANEGAS C.C. 70257592** y a mi esposa **YENY PATRICIA MONTOYA SALAZAR C.C. 1045109256**, para adelantar el proyecto de seguridad informática en las instalaciones del Comando de Departamento de Policía Caquetá.

Como es de su conocimiento, dicho proyecto consiste en un **Análisis de vulnerabilidades en el sistema de seguridad físico e informático del Departamento de Policía Caquetá**, y se encuentra en el pensum académico de la UNAD dentro de la especialización en seguridad informática que adelanto con su autorización.

Por otra parte, queremos hacer una amable invitación a usted y a su equipo de trabajo para el día viernes 16/03/2018 a las 09:30 horas en la sala de juntas de la Seccional de Inteligencia, donde socializaremos las actividades y objetivos del proyecto a realizar.

Atentamente,

Andrés Vanegas

Patrullero, **ANDRES FERNEY VANEGAS**
Analista de inteligencia
Seccional de Inteligencia Policial Caquetá

Elaborado por: PT. Andres Ferney Vanegas
Revisado por: PT. Andres Ferney Vanegas
Fecha de elaboración: 08-03-2018
Ubicación: GUICON \ documentos de apoyo\comunicaciones solicitud.marzo

Calle 11A 10-40 Juan XXIII
Teléfono 4351688
epol.decap@dipol.gov.co
www.policia.gov.co

1DS - OF – 0001 Página 1 de 1 Aprobación: 07/04/2014
VER: 2

Anexo B. Socialización del proyecto en el departamento de Policía Caquetá

Anexo C. Encuesta de Percepción

MINISTERIO DE DEFENSA NACIONAL
POLICIA NACIONAL
DIRECCION DE INTELIGENCIA POLICIAL
SECCIONAL CAQUETA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

ENCUESTA

Departamento de Policía Caquetá
Seguridad Informática

1. Considera usted que el sistema informático del comando de policía del Caquetá es:

   a. Infalible
   b. Muy seguro
   c. Medianamente seguro

2. Alguna vez ha prestado su usuario de dominio o de cómputo?

   a. Si
   b. No

3. Conoce o Sabe que funciones cumple un archivo .exe?

   a. Si
   b. No

4. Cada cuánto recibe capacitación, controles o auditoria frente a las políticas de seguridad informática en la institución?

   a. Mensualmente
   b. Trimestralmente
   c. Anualmente
   d. No he recibido

Anexo D. Informe Gerencial al Comandante de Policía Caquetá. Pág. 1

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN DE INTELIGENCIA POLICIAL
SECCIONAL CAQUETÁ

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MINISTERIO DE DEFENSA
POLICÍA NACIONAL
Unidad: DECAD-COMAN
Radicado No:
Recibido por: PT GOMEZ
Fecha: 25-05-18 Hora: 8:00

No. S-2018- 007028 / SIPOL - GRUPO – 29

Florencia, 25 de Mayo de 2018

Recibido
Jefe de telemática
Hablamos

Coronel
JAVIER NAVARRO ORTIZ
Comandante Departamento de Policía Caquetá
Calle 10ª 110-40 Barrio Juan XXIII
Florencia, Caquetá

Asunto: Informe Gerencial

Teniendo en cuenta su apoyo y colaboración en el proyecto de seguridad informática n.2 el cual consistió en un análisis del sistema informático y electrónico del departamento de policía Caquetá, gustosamente les ponemos en conocimiento la apreciación y valoración de los intervinientes respecto a los riesgos y vulnerabilidades en la unidad.

Al observar la parte doctrinal, de políticas y protocolos de seguridad informática, encontramos unos procesos y procedimientos altamente robustos en materia de seguridad, no obstante es apreciable diversas vulnerabilidades en la actuación del personal y bajo control para verificar el cumplimiento y acatamiento de las políticas establecidas, las vulnerabilidades identificadas son las siguientes

1. Falta capacitación y concientización en los funcionarios policiales frente a la seguridad informática y electrónica, lo que vulnera las políticas de seguridad evidenciando mal uso de algunos equipos.

2. La mayoría de los software no tiene la respectiva licencia lo que constituye una vulnerabilidad factible en cuando a los ataques.

3. Se aprecian equipos en estado avanzado de deterioro y ausencia de aseo, evidenciando que no existen planes de mantenimiento lo que podría generar fallas dejando al sistema desprotegido o inoperable.

4. Los controles físicos son de mediana seguridad bajo el entendido que se presenta facilidad al acceso de los equipos de cómputo permitiendo una posible instalación de dispositivos para extraer información.

Por consiguiente, en aras de realizar un aporte al servicio social que presta tan reconocida institución, les hacemos unas respetuosas recomendaciones:

1. El departamento de policía Caquetá debería capacitar periódicamente al personal sobre el manejo de los medios informáticos con que cuenta la unidad haciendo énfasis en el correcto uso de los usuarios y su respectiva contraseña a la hora de acceder tanto a la plataforma como al dominio de la Institución.

2. Suministrar soporte y asistencia técnica inmediata a los funcionarios. Dicho procedimiento actualmente tarda en promedio dos o tres días, lo que incita al funcionario que tiene asignado el equipo a tratar de resolver el incidente por sus propios medios, situación que en ocasiones pone en riesgo el sistema informático de la unidad.

3. Fijar una periodicidad de revista o auditoria frente al control de las políticas de seguridad establecidas (existen las políticas pero pocas veces se verifica su cumplimiento).

Anexo E. Informe Gerencial al Comandante de Policía Caquetá. Pág. 2

4. Es perentorio unificar un servidor para las unidades desconcentradas del departamento de policía Caquetá, dicha medida se presenta a razón que actualmente cada una de las 16 estaciones de policía almacena la información en su respectivo equipo de cómputo sin las medidas de seguridad necesarias ni copias de respaldo que garanticen la disponibilidad de la misma, y la base del departamento de policía, se encuentra sometido a la LAN, con el servicio del SERVIDOR y con mayores políticas de seguridad.

5. Ejercer control sobre las redes inalámbricas que se encuentran en la unidad, y están conectadas a la LAN.

6. Se debería implementar el manejo de usuario en el dominio por grupos ya que actualmente se maneja la configuración de manera individual lo que dificulta realizar cambios globales inmediatos sobre las políticas de seguridad que ya se encuentran implantadas en casos como detección de brechas de seguridad, o actualización de políticas.

7. Se deberían crear zonas restringidas para las ubicaciones de los dispositivos más importantes de la infraestructura informática de la Institución como lo son los servidores DNS y Proxy que se encuentran dentro del comando, al igual que los puntos de acceso, routers y Switchs, ya que se deberían encontrar en habitaciones aisladas protegidas por cerraduras de seguridad, chasis certificados, evitar las emisiones y recepciones electromagnéticas de los mismos.

8. se sugiere que exista un servidor de respaldo por fuera de la unidad policial con el fin de garantizar la disponibilidad de la información cuando pueda verse afectada por desastres o similares.

9. Implementar un servidor de dominio raíz que administre los diferentes servidores de las unidades policiales, con el fin de que solo los usuarios autorizados puedan tener acceso a los activos y recursos con que cuenta el departamento de policía Caquetá y evitar que terceros malintencionados accedan a los recursos de la institución sin autorización previa.

10. Se deberían implementar medidas y procedimientos para llevar un registro y análisis de las trazas de auditoría en las redes y sistemas instalados, con el fin de monitorear las acciones que se realicen (acceso a ficheros, dispositivos, empleo de los servicios, etc.), y detectar indicios de hechos relevantes a los efectos de la seguridad que puedan afectar la estabilidad o el funcionamiento del sistema informático.

Agradecemos una vez más, su apoyo y colaboración y esperamos entonces, que nuestras sugerencias tengan acogimiento y aplicabilidad en la seguridad informática del departamento, y que de alguna u otro manera hayamos aportado para fortalecer la seguridad de la información que por mandato constitucional les atañe.

Atentamente,

Andrés Vanegas

Patrullero, **ANDRÉS FERNEY VANEGAS**
Analista de inteligencia
Seccional de Inteligencia Policial Caquetá.

Yeny Patricia Montoya S

Docente, **YENY PATRICIA MONTOYA SALAZAR**
Ingeniera Electrónica
UNAD

Elaborado por: PT. Andrés Ferney Vanegas
Revisado: PT. Andrés Ferney Vanegas
Fecha de elaboración: 30-06-2014
Ubicación: Y:\OFIINDOCUMENTOS DE APOYO\01 COMUNICACIONES OFICIALES\01 Enviados\Despuestas FER.MACO

Calle 10A 11-40 Juan XXIII
Teléfono 098-4356323
sipol.decaq@dipol.gov.co
www.policia.gov.co

Anexo F. RAE

Título de Documento.	Análisis de vulnerabilidades en el sistema de seguridad físico e informático del departamento de policía Caquetá.
Autor	Yeny Patricia Montoya Salazar – Andrés Ferney Vanegas
Palabras Claves	Seguridad físico, vulnerabilidades, seguridad informática.

CONTENIDO:

- **DESCRIPCIÓN DEL PROBLEMA:**

El Departamento de Policía Caquetá maneja información relevante para la seguridad ciudadana en los 16 municipios del departamento del Caquetá y por ende, dirige las comunicaciones con las estaciones de la institución establecidas en cada municipio.

En este sentido, el presente estudio pretende establecer las posibles vulnerabilidades del sistema de Seguridad Informática y Seguridad Electrónica que pueda presentar el comando de policía Caquetá, teniendo en cuenta que las fallas en éstos campos, puede afectar críticamente la seguridad ciudadana y la seguridad de las personas vinculadas a la institución: particulares y uniformados.

En consecuencia, el problema se dimensiona en diferentes escenarios en cuanto el flujo de información del comando puede contener evidencias de diferentes delitos en la jurisdicción, también componentes y organigramas de estructuras criminales y delincuenciales del Caquetá, cuya filtración, saqueo, sabotaje o cualquier acto similar, podría afectar los derechos constitucionales de las personas allí referidas, en caso de ser inocentes o afectar cualquier operación policial en caso de estar comprometidos penalmente.

En este sentido, es necesario tener en cuenta el deber constitucional de la policía Nacional, frente a los principios de la seguridad de la información, que son: a) Confidencialidad de los datos, b) Integridad, y c) Disponibilidad.

De otra parte, es importante mencionar que las vulnerabilidades podrían presentarse desde dos ámbitos: a través de los visitantes a la unidad y a través de sus mismos funcionarios bien sea de manera intencional o accidental.

A partir del anterior planteamiento se formula el siguiente interrogante: ¿Cuál es el nivel de vulnerabilidad del sistema de Seguridad Informática y Seguridad Electrónica del Departamento de Policía Caquetá?

OBJETIVO GENERAL.

Establecer el nivel vulnerabilidad del sistema de Seguridad Informática y Seguridad Electrónica del Departamento de Policía Caquetá.

OBJETIVOS ESPECÍFICOS.

- Evaluar los flujos de información y los controles de seguridad existentes en las instalaciones objeto de estudio.

- Establecer las vulnerabilidades de seguridad informática o electrónica que se puedan estar presentando el departamento de policía Caquetá.

- Analizar los procesos y procedimientos establecidos en los protocolos de seguridad al interior del comando policía Caquetá.

- Realizar un documento para entregar donde se indique los riesgos físicos e informáticos del problema objeto de estudio.

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

El Departamento de Policía Caquetá es una institución al servicio de la comunidad, la cual maneja un flujo de información constante y altamente sensible abordando información confidencial de múltiples fenómenos criminales y delictivos de la región.

En este sentido, dicha información debe gozar de reserva a fin de garantizar las condiciones mínimas de seguridad para sus habitantes. Aunado a lo anterior, su infraestructura física comprende diferentes áreas que requieren de máxima seguridad para garantizar su deber constitucional (sala de cámaras, antenas etc.), por consiguiente, se hace necesario realizar un análisis del sistema de seguridad

de dicha unidad con el fin de identificar las vulnerabilidades susceptibles de mejora en el ámbito físico e informático.

Con dicho análisis se pretende que una vez identificadas las principales vulnerabilidades, se adelante un plan de mejoramiento por parte de la unidad a fin de fortalecer la seguridad ciudadana en la capital Caqueteña.

CONCLUSIONES

1. Aunque existan condiciones favorables de seguridad siempre van a haber riesgos que requieren ser evaluados y tenidos en cuenta por el dueño de los activos de información.

2. El acompañamiento virtual no corresponde a las necesidades básicas que tienen los estudiantes dentro de la elaboración del proyecto.

3. El avance constante de la tecnología demanda de los profesionales una actualización constante para permanecer competitivos en el campo laboral de la seguridad informática.

4. Es dispendioso realizar un análisis previo del campo en el cual se vs a desarrollar el proyecto de grado.

RECOMENDACIONES.

La propuesta y el desarrollo del proyecto es importante que la atienda el mismo docente, porque cuando se presenta el cambio de docente se registran variaciones en el proyecto que demandan nuevas acciones por parte del estudiante.

Es bueno que el acompañamiento o asesoría de los proyectos de grado tengan como mínimo un porcentaje de asesoría presencial.

Es necesario que exista mayor claridad y coherencia entre las guías, los reglamentos y la asesoría del tutor para elaborar los proyectos, esto teniendo en cuenta que las sugerencias no son totalmente claras.

Sería apropiado que se entregue un proyecto modelo para que el estudiante a partir de este elabore su nuevo proyecto, y se facilite la presentación del mismo.