Análisis de la gestión de la ciberseguridad en la Policía Nacional de Colombia

Yenni Alejandra Cardozo Garzón

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

ANÁLISIS DE LA GESTIÓN DE LA CIBERSEGURIDAD EN LA POLICÍA NACIONAL DE COLOMBIA

ALUMNO: YENNI ALEJANDRA CARDOZO GARZÓN

DIRECTOR: ING. IVÁN RODRIGO VARGAS RAMÍREZ

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTÁ – COLOMBIA

2019

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

ANÁLISIS DE LA GESTIÓN DE LA CIBERSEGURIDAD EN LA POLICÍA NACIONAL DE COLOMBIA

ALUMNA: YENNI ALEJANDRA CARDOZO GARZÓN

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA
BOGOTÁ – COLOMBIA
2019

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

Análisis de la Gestión de la Ciberseguridad en la Policía Nacional de Colombia

Alumna: Yenni Alejandra Cardozo Garzón

Director: Ing. Iván Rodrigo Vargas Ramírez

Maestría en Ciberseguridad y Ciberdefensa

Trabajo de Grado para Optar el Titulo de Magister en Ciberseguridad y Ciberdefensa

Bogotá – Colombia

2019

Dedico este trabajo a Dios y a mi familia por haberme prestado todo el apoyo y lograr la culminación de estudios y gozar de buena salud.

Agradecimientos

Agradezco a Dios por iluminarme y fortalecerme en los obstáculos que se me han presentado durante el trasegar institucional y por ser el guía de mi vida.

A mis padres y hermanas, por haberme educado, corregido y acompañado en mi formación como persona y profesional, por su paciencia y apoyo incondicional en el transcurso de mi vida, pero sobre todo por la perseverancia que en sus demostraciones me enseñaron a no desfallecer ni rendirme ante las adversidades.

Al Ing. Iván Rodrigo Vargas Ramírez, por su valiosa guía y asesoramiento en la realización del presente trabajo de grado.

A la Escuela Superior de Guerra por permitirme adquirir conocimientos y fortalecer mi perfil profesional desde diferentes ámbitos de la ciberseguridad y la ciberdefensa.

Y gracias a todas las personas que me acompañaron y apoyaron en el desarrollo y realización de este proyecto.

Resumen Ejecutivo

La tecnología y la digitalización crean un mundo globalizado gobernado por ordenadores, dispositivos y herramientas de las Tecnologías de la Información y comunicación (TIC), presentes en todas y cada una de las actividades que el hombre realiza, convirtiéndose en elementos integrales que son inherentes al progreso y desarrollo de la humanidad; bajo este contexto los delitos trascienden del plano físico al plano digital, así aparece el concepto de ciberseguridad como aquella seguridad que busca garantizar la navegación segura de los usuarios de las redes en el mundo virtual.

El objetivo de esta investigación se basa en el análisis del proceso de gestión de la ciberseguridad en la Policía Nacional de Colombia, en la era digital; para cumplir con este propósito se procede a aplicar una metodología investigativa que implica un enfoque cualitativo, con una investigación de tipo exploratorio y descriptivo, enfocada a 25 funcionarios policiales que dirigen o coordinan labores de ciberseguridad en la ciudad de Bogotá, además de los jefes de las unidades, como la Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales (CiberGAula), Equipo de Respuesta a Incidentes Cibernéticos (CSIRT) y Centro Cibernético Policial (CCP) los cuales son expertos en el tema de Ciberseguridad; estas unidades cuentan con investigadores, analistas, peritos informáticos, ingenieros, desarrolladores, abogados e inclusive funcionarios que sin tener titulación, tienen un alto nivel de experiencia en el tema ciber. Estos profesionales son capacitados en distintos contenidos relacionados con delitos informáticos y del ciberespacio, así como en el manejo de herramientas tecnológicas, todo esto conforme al rol y responsabilidad que desarrollan cada uno de los grupos en busca de contrarrestar los fenómenos de criminalidad focalizada en la utilización de nuevas tecnologías.

Este estudio reviste de gran importancia en la medida que se requiere fortalecer las competencias de cada uno de los policías, conociendo algunas de las estrategias de prevención de delitos informáticos generados por los ciberdelincuentes, la detección de amenazas latentes a nivel nacional e internacional y la respuesta a los Ciberdelitos que se forjan en el ciberespacio y que no han sido detectadas por la Institución.

Los resultados evidencian que las estrategias y competencias del personal, aplicadas por la

Policía Nacional para la prevención de fugas de datos, control de acceso y seguridad en la red, se enfocan a la aplicación de la Norma Internacional emitida por la Organización Internacional de normalización (ISO 27001), lo cual es importante para la identificación, prevención y control de ataques cibernéticos, desarrollados mediante diferentes técnicas de espionaje, intrusión, difusión interna, ataques, etc. En tanto que las tácticas de gestión de las vulnerabilidades y el monitoreo continúo utilizadas por la Policía Nacional se realizan a través de controles, con el fin de prevenir la fuga de la misma, persiguiendo tráfico malicioso en búsqueda de correlación de ips.

Los mecanismos de respuesta de la Policía Nacional en casos que impliquen recuperación de información y contramedidas se fundamentan en el mantenimiento y uso software diseñados para la seguridad cibernética, análisis de seguridad y uso forense.

Palabras claves: gestión, ciberseguridad, ciberespacio, ciberdelincuente, ciberdelitos, software, análisis, seguridad, forense.

Abstract

Technology and digitalization create a globalized world governed by computers, devices and tools of Information and Communication Technologies (TIC), present in each and every one of the activities that man performs, becoming integral elements that are inherent to the progress and development of humanity; in this context, crimes transcend the physical plane to the digital plane, thus the concept of cybersecurity appears as that security that seeks to guarantee the safe navigation of the users of the networks in the virtual world.

The objective of this investigation is based on the analysis of the process of managing cybersecurity in the Colombian National Police, in the digital age; in order to fulfil this purpose, a research methodology involving a qualitative approach is applied, with exploratory and descriptive research, focused on 25 police officers who direct or coordinate cybersecurity work in the city of Bogotá, in addition to the heads of the units, such as the Special Unit for the Investigation of Crime of Kidnapping and Extortion through Digital Environments (CiberGAula), Cyber Incident Response Team (CSIRT) and Police Cyber Center (CCP), which are experts in cybersecurity; these units include researchers, analysts, computer experts, engineers, developers, attorneys and even officials who, without qualifications, have a high level of experience in the subject of cyber. These professionals are trained in different content related to computer crime and cyberspace, as well as in the handling of technological tools, all this according to the role and responsibility developed by each of the groups in order to counteract the phenomena of criminality focused on the use of new technologies.

This study is of great importance in that it is necessary to strengthen the competencies of each police officer, knowing some of the strategies of prevention of cybercrime generated by cybercriminals, the detection of latent threats at the national and international levels and the response to cybercrimes forged in Cyberspace that have not been detected by the Institution.

The results show that the strategies and competencies of the personnel, implemented by the National Police for the prevention of data leaks, access control and security in the network, focus on the implementation of the International Standard issued by the International Organization for Standardization (ISO 27001), which is important for identification, prevention and control of cyber-attacks developed through different

techniques of espionage, intrusion, internal diffusion, attacks, etc. While the vulnerability management and monitoring tactics used by the National Police continue to be carried out through controls in order to prevent the escape of the police, pursuing malicious traffic in search of Ips correlation. The response mechanisms of the National Police in cases involving retrieval of information and countermeasures are based on the maintenance and use of software designed for cybersecurity, security analysis and forensic use.

Keywords: management, cybersecurity, cyberspace, cybercriminal, cybercrime, software analysis, safety, forensic.

Lista de abreviaturas

AMERIPOL:	Comunidad de Policías de América
BEC:	Business Email Compromise, que significa correos electrónicos corporativos comprometidos y que consiste en suplantar
CCD:	(**C**harged **C**oupled **D**evice), Dispositivo de Carga Acoplada.
CCP:	Centro Cibernético Policial
CONPES:	Consejo Nacional de Política Económica y Social
CSIRT:	Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad Informática)
EUROPOL:	Oficina Europea de Policía
FBI:	Federal Bureau of investigation – Departamento de Investigación Criminal de los Estados Unidos.
FTK:	Forensic Toolkit - Software de Informática Forense.
INTERPOL:	International Pólice – Policía Internacional
IPS:	Intrusión prevention Sistem (sistema para prevención de intrusos).
ISO:	International Organization for Standarization (Organización Internacional de Normalización)
O.I.P.C:	Organización Internacional de Policía Criminal
OEA:	Organización de los Estados Americanos
OTAN:	Organización del Tratado del Atlántico Norte
SGSI:	Sistema de Gestión de Seguridad de la Información.
SSH:	Secure Shell (Consola segura)
WAF:	Web Aplication Firewall (Firewall de aplicaciones web)

Contenido

Lista de tablas

Lista de figuras

Lista de anexos

Introducción

Esta investigación contempla analizar el proceso de gestión de la ciberseguridad en la Policía Nacional de Colombia, en la era digital, para conocer y entender el proceso que realiza la institución para prevenir, detectar y dar respuesta a los ciberdelitos que se constituyen en amenazas por parte de grupos delictivos, actividades ilegales o delincuentes, con el fin de enfocar estrategias del sistema educativo policial, garantizando la formación y capacitación integral para el desarrollo de competencias, logrando potenciar la gestión del conocimiento, innovación e implementación en el uso sostenible de las tecnologías de la información y la comunicación (TICS). De forma específica se buscó realizar un diagnóstico de conocimientos y competencias específicas de los integrantes de Policía Nacional en temas de Ciberseguridad, seguido en determinar las estrategias aplicadas por la entidad para la prevención de fugas de datos, control de acceso y seguridad en la red, además conocer las tácticas de gestión de las vulnerabilidades y monitoreo continúo utilizadas para identificar los mecanismos de respuesta en casos que impliquen recuperación de información y contramedidas.

La ciberseguridad se fundamenta en cibernética ya que "es una teoría interdisciplinar centrada en el estudio de las interrelaciones entre la persona y la máquina y que en la actualidad se encuadra dentro del ámbito más general de la teoría de control, el automatismo y la programación de ordenadores. Esta teoría abría un campo de reflexión interdisciplinar que aportaba distintos criterios a numerosas áreas de la tecnología" (Wiener, 1947, pág. 23). En tanto que para la ADC (2016) el concepto de ciberseguridad involucra una conceptualización que puede verse desde tres enfoques, el primero tiene que ver con la protección o defensa de las infraestructuras de organismos (públicos y privados), sus redes, datos y usuarios; la segunda como el trabajo que realizan las fuerzas de seguridad en investigación, prevención y acción contra delitos en el ámbito digital (cibercrimen); y una tercera relacionada con la actividad de vigilancia llevada a cabo por los organismos de inteligencia.

En términos generales el documento consta de siete capítulos de desarrollo, el primer capítulo hace referencia a los antecedentes de la investigación donde se expone la problemática, los objetivos, la justificación y la metodología, en el segundo capítulo se precisa una conceptualización teórica y legal,

donde se enfatiza en el conocimiento de la Cibernética y los temas, el Ciberespacio, la Ciberseguridad y la gestión de la Ciberseguridad; también se refiere obviamente a las normas legales que tienen como finalidad regular el comportamiento de los individuos en el ciberespacio.

El tercer capítulo entre tanto refiere a un diagnóstico de la situación colombiana en materia de ciberseguridad, en la cual se exponen una serie de condiciones delitos o situaciones que se presentan en Colombia, referentes a los actos delictivos que circundan el Ciberespacio y el notable incremento de denuncias en las principales ciudades de Colombia, referente al hurto, violación de datos personales y acceso abusivo a sistemas de información.

El cuarto capítulo entre tanto, hace relación al diagnóstico del conocimiento y las competencias específicas, ligadas a la evaluación de los cargos que sustenta el cruce de los requerimientos del cargo con el perfil de los funcionarios policiales en temas de ciberseguridad, este análisis se aborda a través de competencias instrumentales y competencias sistémicas unidas al modelo de gestión del talento humano, buscando con ello fortalecer la competitividad que tienen los funcionarios policiales cuando se trata de responder a situaciones que afectan el ciberespacio y que atentan contra la integridad individual y colectiva de los colombianos

El capítulo quinto refiere directamente a la estrategia de afianzamiento y gestión de la ciberseguridad en la etapa inicial, es decir, *la etapa de prevención*, en la cual se hace un análisis del control de acceso y gestión de servicios de tecnologías de información y comunicación (TIC), la identificación y prevención de ataques de hackers a la red, la preparación de la Policía para atender un asalto cibernético en Colombia y las herramientas dispuestas por la Policía para la prevención de la ciberseguridad enmarcada dentro del actuar policial y cooperación de entidades publico / privadas.

El sexto capítulo refiere a la segunda etapa, es decir, *la etapa detección* o tácticas de gestión de vulnerabilidad y monitoreo continúo utilizadas por la Policía Nacional, en él se relaciona el proceso de vigilancia, las medidas tomadas para minimizar las amenazas que se registran con la aparición de nuevos programas maliciosos y las herramientas dispuestas por la Policía para detectar los ataques ciber delincuenciales.

El séptimo capítulo refiere a la tercera y última etapa de la gestión de la ciberseguridad, en donde se analizan *los mecanismos de respuesta* en el proceso de innovación de la Policía Nacional en casos que implican recuperación de la información, por tanto, se analizan las medidas tomadas en la fuga de datos, sistemas de recuperación de la información, las contramedidas para ataques, el papel de la entidad en la prevención y detección de respuesta a los problemas de ciberseguridad y las herramientas dispuestas por la policía para responder efectivamente a un ataque.

Capítulo I: antecedentes del estudio

1.1 Problema

Según estudios realizados, el principal problema en materia de seguridad en Colombia es "la insuficiencia en la capacidad actual del Estado para enfrentar las amenazas que atentan contra la Ciberseguridad y Ciberdefensa Nacional" (Huertas, 2014, pág. 28). Es así, como esta problemática se despliega desde tres ejes a saber, los cuales abarcan efectos en el incremento de la delincuencia y accesos indebidos que afectan la continuidad y el funcionamiento de la información y de los servicios, tales como: "1) Las iniciativas y operaciones en ciberseguridad y ciberdefensa no están coordinadas adecuadamente; 2) Debilidad en la oferta y cobertura de capacitación especializada en ciberseguridad y ciberdefensa. 3) Debilidad en regulación y legislación de la protección de la información y de los datos" (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011, pág. 17), evidenciadas en el sector público y privado visualizados desde las limitaciones y falta de coordinación en el desarrollo de operaciones por la ausencia de concienciación y generación de cultura en prevención en busca de entrenamiento y formación en aras de potenciar la normatividad y la respuesta eficaz de los delitos cibernéticos.

De forma específica, se observa en la institución policial que hay deficiencias en la gestión de algunos procedimientos propios de la labor ejercida por los funcionarios en el tema Cibernético, esto se debe al acelerado desarrollo que ha tenido la tecnología, la cual sobrepasa los conocimientos y competencias de los policías, quienes tienen que vivir día a día nuevos retos en materia de gestión de la ciberseguridad, retos que implican nuevas y novedosas técnicas que permitan el control de acceso, la prevención de fugas de datos, minimización de la vulnerabilidad, monitoreo continuo, estrategias de recuperación y contra-respuesta; técnicas que son claves en la eficiencia y eficacia de los resultados en la lucha contra la Ciberdelincuencia, pero que no son conocidas por todos aquellos que hacen uso del Ciberespacio.

Con fundamento en esta problemática se plantea la siguiente pregunta:
¿Cómo contribuir al proceso de gestión de la ciberseguridad en la Policía Nacional de Colombia, en la era digital?

1.2 Objetivos del Proyecto

1.2.1 Objetivo general. El objetivo principal del proyecto consiste en contribuir al proceso de gestión de la ciberseguridad en la Policía Nacional de Colombia, en la era digital; mediante una propuesta de curso para capacitación. El alcance de este objetivo se logrará mediante los siguientes objetivos específicos:

1.2.2 Objetivos específicos

1. Realizar un diagnóstico de conocimientos y competencias de los integrantes de Policía Nacional en temas de ciberseguridad

2. Determinar las estrategias aplicadas por la entidad para la prevención de fugas de datos, control de acceso y seguridad en la red

3. Conocer las tácticas de gestión de las vulnerabilidades y monitoreo continúo utilizadas.

4. Identificar los mecanismos de respuesta en los casos que impliquen recuperación de información y contramedidas.

5. Realizar una propuesta para mejorar las competencias de ciberseguridad de los funcionarios de la Policía Nacional y con ello optimizar la gestión de sus unidades.

Para el desarrollo de dichos fines, el proyecto contempla un desarrollo en cinco pasos:

1) Análisis de documentos oficiales y objetivos relacionados con el tema de ciberseguridad en la Policía Nacional.

2) Diseño y aplicación de una encuesta a funcionarios de las unidades de ciberseguridad en la ciudad de Bogotá.

3) Diseño y aplicación de una entrevista a los jefes del Centro Cibernético Policial (CCP), el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT PONAL) y unidad especializada, encargada de investigar los delitos de secuestro y extorción a través de entornos digitales (CiberGAula).

4) Diseñar la propuesta acorde al diagnóstico de las necesidades

5) Consolidación de la información conforme a objetivos propuestos.

1.3 Justificación

La relevancia de este trabajo se fundamenta en las competencias que soporta el modelo de gestión humana afianzada en conocimientos, experiencia y habilidades a los que se deben enfrentar los funcionarios y ciudadanía en la nueva era digital; en otras palabras, aunque todos estamos inmersos en el mundo de la digitalización y somos usuarios habituales de la tecnología para el desarrollo de nuestras actividades educativas, comerciales, sociales, entre otras, no se tiene en cuenta las nuevas modalidades del obrar delincuencial, algunos funcionarios de la institución desconocen las herramientas y los mecanismos que la Policía Nacional utiliza para la protección de la seguridad y bienestar de la ciudadanía, previniendo que la comunidad sea víctima de crímenes y delitos que se tejen en el ciberespacio.

Con el cumplimiento de los fines u objetivos propuestos en esta investigación no sólo se logra evidenciar el proceso que tiene la gestión de la ciberseguridad en la Policía Nacional de Colombia, vista a través de los directivos de las unidades de ciberseguridad descritas a esta entidad, sino también, se propone una estrategia fundamentada en la capacitación, mediante la cual los policías pueden mejorar sus competencias, y contar con instrumentos para poder enfrentar los retos que se generan en el ciberespacio en materia de cibercrimen y ciberdelincuencia.

De igual forma, para la institución es importante dar a conocer a sus funcionarios los procesos y herramientas que desarrollan y ofrecen para evitar que la delincuencia afecte la población y se genere en la comunidad un empoderamiento que limite el accionar delictivo de aquellos que buscan hacer un mal uso de la tecnología.

1.4 Metodología

Esta investigación tiene un enfoque cualitativo, de tipo exploratorio y descriptivo, comprendiendo un proceso de exploración en donde se hace un acercamiento al objeto de estudio, que para este caso, son los funcionarios policiales, por consiguiente la descripción que "tiene como objetivo primordial la descripción de la realidad y afianzamiento de estrategias de protección; siendo sus principales métodos de recogida de información a través de la observación y la encuesta" (Mas, 2012, pág. 91); en contexto permite conocer el proceso de gestión de la ciberseguridad y la creación de estrategias de protección en la Policía Nacional de Colombia, en la era digital; se tomó esta investigación, teniendo en cuenta que "este tipo de investigación trabaja sobre realidades de hecho, y su característica fundamental es la de presentarnos una interpretación correcta" (Tamayo, 2004, pág. 56), lo cual es pertinente al caso.

El cumplimiento de los objetivos reviste el desarrollo de una investigación de enfoque cualitativo, de la misma manera en que "los estudios cualitativos tienden a comprender la realidad social como fruto de un proceso histórico de construcción, visto a partir de múltiples lógicas presentes en los diversos y heterogéneos actores sociales" (Eugenia, 2004, pág. 24), así y para el caso se procedió a realizar un diagnóstico de conocimientos y competencias específicas de los integrantes de Policía Nacional en temas de ciberseguridad, para luego determinar las estrategias aplicadas en la prevención de fugas de datos, el control de acceso y la seguridad en la red, así como conocer las tácticas de gestión de la vulnerabilidades, monitoreo, mecanismos de respuesta en casos que impliquen recuperación de información y contramedidas.

Los instrumentos a utilizar para la recolección de la información y el cumplimiento de los fines de la encuesta, la entrevista y el análisis documental en medio electrónicos de la Policía Nacional, con los que se logró tener una amplia visión sobre la forma como la Policía Nacional de Colombia viene

gestionando la ciberseguridad en Colombia a través de la prevención, detección y respuesta inmediata a las ciber amenazas. De forma específica, como previene las fugas de datos, forja la seguridad en la red, detecta amenazas, minimiza las vulnerabilidades, monitorea la red y que sistemas de recuperación y contramedidas de ataque utiliza.

El universo está compuesto por los funcionarios de la Policía Nacional que en su función Policial ejercen una labor relacionada directa e indirectamente con la ciberseguridad desarrollando procesos que implican prevención, detección y respuesta inmediata a las ciber amenazas. Para el caso se utilizó un muestreo probabilístico, es decir, se seleccionaron los sujetos teniendo en cuenta la población, muestra, nivel de confianza, probabilidad a favor y en contra y el error muestral, de esta forma, se seleccionó el total de los 25 funcionarios que dirigen o coordinan labores de ciberseguridad en la ciudad de Bogotá y tres jefes de las unidades encargadas de la ciberseguridad en la Policía Nacional de Colombia.

Este proyecto se limita al cumplimiento de los objetivos propuestos, de esta forma, lo que se buscó es conocer el proceso de gestión en materia de ciberseguridad y afianzar estrategias fundamentadas en el modelo de gestión del talento humano de la Policía Nacional de Colombia en el contexto de la era de la digitalización, por ende se procede a realizar un diagnóstico de conocimientos y competencias de los uniformados encargados del área; para luego abordar el tema de la gestión desde tres contextos básicos que son: 1) la prevención, 2) la detección y 3) la capacidad de respuesta, en el caso de la prevención se habla del controles implementados; en tanto que la detección refiere a la gestión de las vulnerabilidades y el monitoreo continuo; finalmente la capacidad de respuesta se enfoca los sistemas de recuperación de la información en caso de ser asaltada por la ciberdelincuencia, en contraste con las contramedidas que se toman no sólo desde el punto de vista proactivo, sino también reactivo.

Con motivo de la ejecución del proyecto se logró conocer el proceso de gestión que desarrolla la Policía Nacional en materia de ciberseguridad, identificando si dicho proceso efectivamente garantiza la seguridad de los ciudadanos y la nación en general, con estrategias adecuadas de prevención, detección y capacidad de respuesta oportuna.

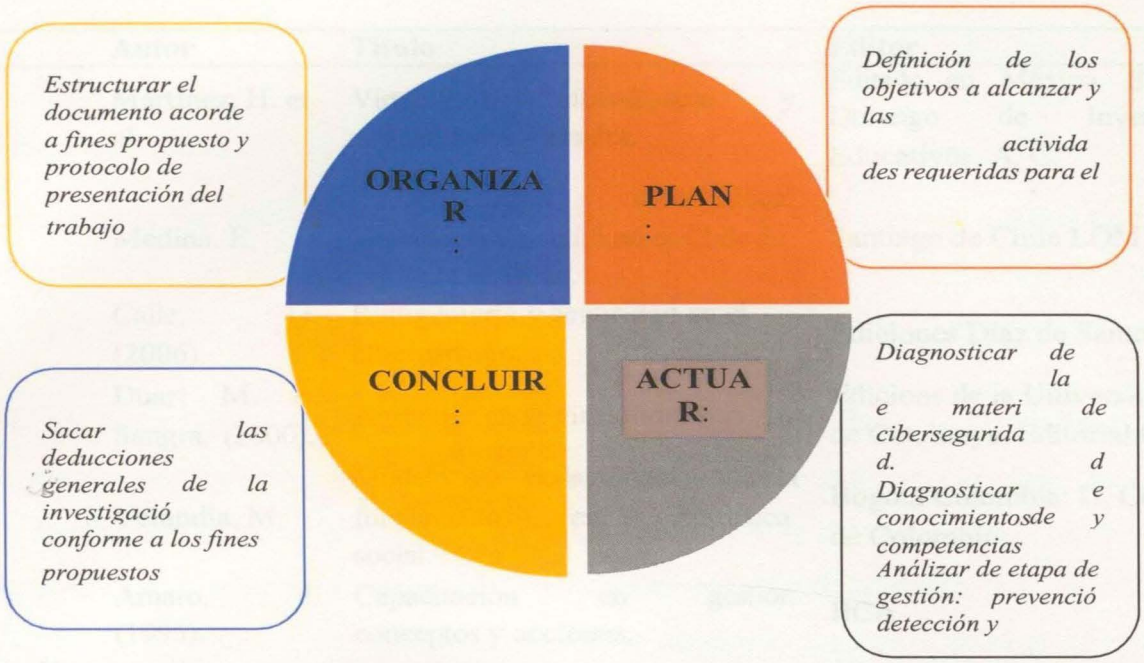


Figura 1. Ciclo de la investigación. Recuperado del Ciclo de la investigación: metodología y procesos. Morales Ramos Eduardo. 2006. Pàg.37.

Para el desarrollo del ciclo del a investigación y el fortalecimiento de esta, fue preciso tomar como referencia principal los siguientes documentos bibliográficos:

Tabla 1. Principales textos bibliográficos de referencia

Año	Autor	Titulo	Editor
Revistas			
2016	Castillejos, L., Torres, G. & Lagunes, D.	La seguridad en las competencias digitales de los millennials.	Revista Apertura, 8(2). pp. 54-69
2016	Llorens, M.	Los desafíos del uso de la fuerza en el ciberespacio.	Anuario Mexicano de Derecho Internacional, vol. XVII, pp. 785-816
2015	Regalado, M. & Regalado, M.	Retos en informatización y ciberseguridad para la Universidad de Ciencias Médicas de La Habana.	Revista Habanera de Ciencias Médicas versión On-line ISSN 1729-519X. 14(4) jul.-ago.
Libros			
2016	Giant, N.	Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones.	Madrid España: Narcea Ediciones.
2015	Tomas et al.	Retos del derecho ante las nuevas amenazas. Seguridad y Defensa	Librería-Editorial Dykinson.

Año	Autor	Titulo	Editor
2014	Martínez, H. et al.	Virtualidad, ciberespacio y comunidades virtuales.	Editado en México. Editor: Red Durango de Investigadores Educativos, A. C.
2013	Medina. E.	Revolucionarios cibernéticos: Tecnología y política en el Chile de Salvador Allende.	Santiago de Chile LOM Ediciones
2006	Calle, G. (2006).	Reingeniería y seguridad en el ciberespacio.	Ediciones Díaz de Santos
2006	Duart M. & Sangra. (2000).	Aprender en la virtualidad.	Edicions de la Universitat Oberta de Catalunya. Editorial Gedisa.
2005	Velandia, M.	Modelo pedagógico con fundamentos en cibernética social.	Bogotá Colombia: U. Cooperativa de Colombia.
1995	Amaro, J. (1995).	Capacitación en gestión conceptos y acciones.	IICA
Publicación			
2012	Casar, C.	El ciberespacio un nuevo reto de confrontación.	Madrid España: Ministerio de Defensa.
2012	Fundación Telefónica.	El debate sobre la privacidad y seguridad en la red: regulación y mercados.	Fundación Telefónica
2011	Joyanes et al.	Ciberseguridad: retos y amenazas a la seguridad nacional en el ciberespacio.	Madrid España: Ministerio de Defensa
Web			
2017	Cañizares, E.	Los profesionales de la ciberseguridad.	www.redseguridad.com
2017	Fernández, E.	Ciberseguridad sencilla, integrada y automatizada.	www.redseguridad.com
2017	INTERPOL.	Hacia una ciberseguridad sencilla, integrada y automatizada. El Complejo Mundial de INTERPOL para la Innovación.	www.interpol.int
2014	Ministerio de la TIC	Agenda estratégica de innovación: ciberseguridad. Expertos en ciberseguridad de la ONU concluyen informe sobre información y telecomunicaciones.	www.mintic.gov.co
2015	OCDE	Perspectivas de la OCDE sobre la economía digital 2015.	www.oecd.org

Fuente: Elaboración propia

Capítulo II: marco teórico y legal

2.1 Marco normativo

En materia de ciberseguridad en Colombia se han emanado varias normas que buscan establecer criterios de prevención y corrección en lo que compete al uso del ciberespacio. Dentro de estas normas son de gran relevancia:

Como toda regulación en Colombia la normatividad parte de la Constitución Política de Colombia para el caso el artículo 15 que refiere "todas las personas tienen derecho a su intimidad personal y familiar y a su buen que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales; así como el derecho a la información consagrado en el artículo 20. En esta misma línea, se desarrolló un marco jurídico que incluye el reconocimiento nombre, y el Estado debe respetarlos y hacerlos respetar" (Colombia. Presidencia de la República. 1991. Constitución Política) y el artículo 20 que expresa "se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social" (Colombia. Presidencia de la República. 1991. Constitución Política). De esta forma, la Ley 1581 de 2012 tuvo por objeto desarrollar dicho derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos" (Colombia. Congreso de la República. 2012. Ley 1581) de los datos e información como bien jurídico tutelado.

Sin embargo, los antecedentes legales de la ciberseguridad se remontan a la Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Validez jurídica y probatoria de la información electrónica. Actualmente se cuenta con diversas que regulan el uso y apropiación de las TIC dentro de las cuales sobresalen:

- Ley 1150 2007 por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. En esta ley se refiere a seguridad de la información electrónica en contratación en línea.

- Ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Habeas data financiera, y seguridad en datos personales.

- Ley 1341 de 2009 por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Tecnologías de la Información y aplicación de seguridad.

En lo referente a otras normas, Colombia enmendó el Código Penal en 2009, mediante la Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", y el Código de Procedimiento Penal en 2011, mediante la Ley 1453 de 2001 por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. Es decir, se cuenta con una legislación procesal que aborda algunos delitos cibernéticos, y reconoce los tratados internacionales con INTERPOL y EUROPOL.

De igual forma existen otros decretos y actos administrativos relevantes que regulan diversas actividades relacionadas con el entorno digital, tales como la Circular Externa de la Superintendencia Financiera de Colombia 052 de 2007 (estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios), las Resoluciones CRC 3066 y 3067 de 2011 (Régimen integral de protección de los derechos de los usuarios e indicadores de calidad para los servicios de telecomunicaciones), Decreto 1704 de 2012 (interceptación legal de comunicaciones), Decreto Ley 019 de 2012 (entidades de certificación digital), Resolución de la Superintendencia de Industria y Comercio de Colombia (SIC) No. 76434 de 2012 (protección de datos personales), Decreto 2573 de 2014 (Gobierno en línea),

Además de las normas y códigos definidos se cuenta con unas políticas públicas que buscan fortalecer la ciberseguridad y la ciberdefensa, dichas políticas están instituidas en los CONPES 3710 Y 3854:

CONPES 3701 (lineamientos de política para ciberseguridad y ciberdefensa) "Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema" (Ministerio de Tecnologías de la Información y las Comunicaciones, 2011, pág. 3)

CONPES 3854 (política nacional de seguridad digital) "el objeto de este documento cambia el enfoque tradicional al incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Esto lo hace bajo cuatro principios fundamentales y cinco dimensiones estratégicas, que rigen el desarrollo de esta política. De los primeros destaca que la política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas. Principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. Para lograrlo, se implementarán acciones en torno a cinco ejes de trabajo" (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, pág. 3).

Resolución No. 00937 del 10/03/2016 (Por la cual se establece el Manual de Funciones para el personal uniformado de la Policía Nacional, la metodología de evaluación para el perfil de los cargos y se derogan unas disposiciones). "Se constituye como un instrumento de gerenciamiento del talento humano, que brinda elementos descriptivos de los cargos: identificación del cargo, propósito principal, funciones y perfil que se requiere para el logro de la misionalidad institucional a través de desempeños individuales y de grupo, enmarcados en los principios de calidad, cercanía a la comunidad y mantenimiento de la seguridad y convivencia ciudadana" (Policía Nacional , 2016, pág. 3), "evaluados a través de la metodología que evalúa el perfil del cargo a través del Módulo Perfiles de cargos del Sistema de Información para la Administración del Talento Humano" (SIATH) (Policía Nacional , 2016, pág. 3).

2.2. Marco teórico

Para analizar el proceso de gestión de la ciberseguridad en la Policía Nacional de Colombia, en la era digital, se precisa la referencia teórica relacionada directamente con la ciberseguridad, la cual encierra otros conceptos como la cibernética, el ciberespacio y la inteligencia artificial.

2.2.1 Cibernética y los sistemas. Caracterizados por la búsqueda de objetivos generados a partir del comportamiento sistemático creado a partir de los mecanismos de comunicación y control en las máquinas en las que buscan la regulación automática de los seres humanos y sistemas "Los más avanzados ordenadores electrónicos y los más sofisticados robots constituyen el último episodio de esa imparable carrera en la que los hombres se han trazado como meta simplificar hasta el máximo esfuerzo que realizan para conocer, controlar y dominar la naturaleza. Los mecanismos de regulación y control necesarios para que tales artefactos resulten operativos y eficaces, con un alto grado de rendimiento, se basan en la moderna teoría de los mensajes, que es precisamente el principal fundamento de la cibernética" (Wiener N. , 1984, pág. 11) La cibernética desarrollada por Norbert Wiener trata de un campo interdisciplinario, en el cual estudia los problemas de organización, proceso de control y transmisión de información" (Garibay Rivas, 2013, pág. 26)

Así mismo, se conecta el origen de la cibernética con la tendencia de estados probables de organización y diferenciación en los que encuentra estrecha relación entre la comunicación y control, en búsqueda constante de degradar la naturaleza y destrucción de lo que tiene sentido, es así que "Wiener conecta el origen de la cibernética con la preocupación de Gibas por la entropía, la tendencia mostrada por el universo de pasar de estados menos probables a estados más probables, de estados de organización y diferenciación a otros de caos e identidad. No obstante, señala que, a pesar de esta tendencia entrópica global, hay puntos dentro del universo en los cuales la tendencia entrópica parece revertirse de forma temporal," (Garibay Rivas, 2013, pág. 25).

También se considera que algunos planteamientos sistémicos creados en épocas anteriores establecieron nuevos conceptos en los avances científicos que produjeron la generación de ordenadores y la nueva era del desarrollo industrial, en la que aumentaría significativamente la inclusión en la vida cotidiana de los seres humanos y en el comercio, transporte, educación, entre otros.

En efecto "existen diversas historias que señalan el origen de la cibernética; sin embargo, todas

relacionan el campo con la investigación de Wiener y el ingeniero del MIT Julián Bigelow que el Gobierno de Estados Unidos financió durante la Segunda Guerra Mundial. El desafío era crear un servomecanismo antiaéreo capaz de dirigir con precisión armas que derribaran aparatos enemigos. Para Bigelow y Wiener, este desafío era un problema de retroalimentación o de causalidad circular, en el cual participaban la máquina, el operador humano y su proceso de toma de decisiones" (Medina, 2013, pág. 55).

"A pesar de que la cibernética en este siglo ha tenido un gran auge, es algo tan viejo como el arte de gobernar. En efecto, el vocablo griego del que se deriva ("Kibernetes", que significa timonel), lo uso Platón para describir el aspecto prudencial del arte de gobernar" (Deckert, 1975; citado por Galvis, 2004, p.71). En la que alude la creación de sistemas autómatas que produce conocimientos en el desarrollo de problemas complejos como la criminalidad; sin embargo, produjo la reducción de mano de obra por robótica, lo que generó la desigualdad y explotación del hombre, generando aumento en la industrialización y revolución tecnológica que más tarde daría importancia a la computación.

Según S. Beer, Wiener citados por Johansen (1982, p.29), al definir la cibernética como "la ciencia de la comunicación y el control en el animal y en la máquina", apuntaba a las leyes de los sistemas complejos que permanecen invariables cuando se transforma su materia. Considerándola en su sentido más amplio, Beer la define como "la ciencia de la organización efectiva"; allí señala que las leyes de los sistemas complejos son invariables, no frente a las transformaciones de su materia, sino también de su contenido. Nada importa, dice Beer, que el contenido del sistema sea neurofisiológico, automotor, social o económico.

Estos supuestos teóricos posibilitan la simulación del comportamiento humano por medio de máquinas y el nacimiento de la cibernética; así como también, produce hipótesis en algunos mecanismos principales del sistema nervioso central, en la que se crea un componente de realimentación manifestada en un comportamiento definido como intencional.

De acuerdo con los orígenes de la Cibernética, la evolución del concepto a los sistemas a partir de "1948, publicó estos y otros descubrimientos en el libro *Cybernetics,* el cual popularizó la nueva ciencia. Las indagaciones que Wiener y otros miembros del "grupo de la cibernética" desarrollaron en

torno a los procesos de retroalimentación de las máquinas y los organismos atrajeron a investigadores de una amplia gama de disciplinas, como la ingeniería, las matemáticas, la psicología, la fisiología y las ciencias sociales. Quienes practicaban la cibernética intentaban crear una ciencia universal a través de la elaboración de un idioma universal. Conway y Siegel afirman que "la expansión industrial que se produjo después de la guerra, junto con el crecimiento económico y el progreso tecnológico, se debe en gran parte al trabajo de Wiener" y que la cibernética moldeó los procesos de investigación en áreas como la electrónica e impulsó tanto la producción como el consumo de bienes electrónicos". (Medina, 2013, pág. 52)

2.2.2 Ciberespacio. Palabra acuñada en la década de los ochenta por el escritor de ciencia ficción William Gibson en su novela Neuromancer. Ciberespacio ha llegado designar la base de comunicaciones disponible la red informática mundial conocida como Internet (Edwards, 2001, p. 19). Es así como "la estrategia de Ciberseguridad Nacional define el Ciberespacio como "un dominio global y dinámico compuesto por las infraestructuras de tecnología de la información incluida el internet, las redes y los sistemas de información y de telecomunicaciones. Esto es el conjunto de ordenadores, programas y medios de comunicación que permiten intercambiar y procesar información" (De Tomás morales, 2015, pág. 111).

Sin embargo, así como tiene sus ventajas al facilitar la comunicación y comercio enmarcados dentro del desarrollo económico y social, también tiene sus desventajas al ser un mundo accesible oculto al no poseer fronteras en el que no se alcanza a percibir la dimensión y peligrosidad que este contiene, ya que su control está directamente relacionado con el desarrollo tecnológico por permitir el desarrollo de actividades licitas, ilícitas y encubiertas, aunque permanentemente se esté dejando rastro de las actividades que se realicen; es por ello que se debe tomar conciencia de ello y colocar los filtros necesarios para restringir el uso de internet en algunos ambientes. Sin embargo, muchas de estas dependen del grado de actividad laboral que este requiera.

2.2.3 Ciberseguridad. Permite la aplicación de normas, procedimientos, protocolos y técnicas destinadas a ser un sistema seguir y confiable "Se refiere al uso seguro y responsable de los productos de la tecnología de la información y la comunicación (TIC), incluyendo Internet, los dispositivos móviles

y de comunicación y los instrumentos tecnológicos diseñados para guardar, compartir o recibir información, por ejemplo, los teléfonos móviles, las cámaras digitales, etc." (Giant, 2016, pág. 16).

Con forme el mundo avanza, las Tecnologías de la Información y las Comunicaciones progresa rápidamente, es por tal razón que siempre se buscan procesos que ayuden a impulsar la optimización de tiempos y recursos, agilizando eficazmente procesos. En este nuevo esquema, la velocidad, la capacidad y el acceso, se ha visto expuesta a nuevos riesgos, cuyas amenazas son cibernéticas y sus impactos son críticos y reales, requiriendo así que, el Estado en general se replantee sus lineamientos y desarrolle estrategias nacionales que contrarresten las amenazas o incidentes de naturaleza informática a los que los ciudadanos del común estamos expuestos cotidianamente.

Para nuestro sentido común, algunas acciones requieren de un cierto grado de madurez y responsabilidad individual, las cuales, solamente se adquieren cuando adquirimos cierto grado de madurez, pero nuestra sociedad cada vez es más permisiva con nuestros menores, los cuales se están viendo afectados por el uso de dispositivos tecnológicos, pasando conductas inseguras casi desapercibidas. Por esto es importante destacar que: "El problema, como ha señalado el General Gómez López de la Medina, jefe del Mando Conjunto de Ciberdefensa, Internet se concibió para interconectar al mundo, pero sus creadores no pensaron en la maldad que forma parte de él, de esta forma no se pensó en la seguridad". Por este motivo, a medida que han ido evolucionando las TIC, se ha ido haciendo tangible la necesidad de avanzar en estrategias que garanticen la seguridad y permitan el éxito de las oportunidades que ofrece el ciberespacio, poniendo los medios para proteger al usuario frente a las ciberamenazas, que suponen un riesgo, muchas veces invisible, para la normal actividad de un país, afectando directamente a sus ciudadanos e instituciones. (De Tomás morales, 2015, pág. 112)

"La ciberseguridad es la protección de los servicios e infraestructuras críticas frente a cualquier irrupción, así como la protección de la información contra accesos no autorizados. Las medidas de Ciberseguridad no evitarán la recopilación y uso de datos generados por las acciones de cada individuo en Internet; de hecho, algunas medidas sobre Ciberseguridad (como una mejor autenticación de la identidad online) podrían facilitar la recopilación de dichos datos e incrementar los riesgos contra la privacidad. Aunque la Ciberseguridad y la privacidad comparten algunos problemas y soluciones (tales como el uso de la encriptación o la notificación de violaciones de datos), deberíamos tratarlas como dos

cuestiones políticas distintas e independientes, de las que se requieren soluciones para conseguir el beneficio económico completo de las tecnologías digitales" (Jorge Pérez Martínez, 2012, pág. 47). Además, la falta de conciencia y recursos destinados, hacen un escenario demasiado peligroso con consecuencias graves, produciendo así una inadecuada gestión de actualizaciones de seguridad por ordenadores desactualizados, vulnerabilidades localizadas, correos electrónicos maliciosos, todo esto debido a la existencia de atacantes cada vez más especializados, siendo el eslabón más débil de la cadena, el ser humano.

Es importante destacar que las grandes compañías no les gusta admitir que diariamente pierden datos importantes sobre sus cuentas, registros personales, creando un ciberpersonaje, el cual ocasiona desastres de inteligencia monumentales. "Los riesgos de una Ciberseguridad débil han recibido una atención considerable durante los últimos años al ir aumentando la cantidad de incidentes perjudiciales. Pero a pesar de toda la atención, muchas estrategias de Ciberseguridad Nacional no son adecuadas, pues se basan en enfoques desfasados" (Jorge Pérez Martínez, 2012, pág. 48)., utilizando a su favor, brechas se seguridad presente en las tecnologías de la información, aprovechando la vulnerabilidad que presentan la mayoría de las estructuras. "Resulta fácil malinterpretar los riesgos de una Ciberseguridad pobre, y suele subestimarse la magnitud de la amenaza para las redes y los datos. La actividad maliciosa implica el robo de propiedad intelectual, el espionaje y otros delitos penales, más que la creencia popular de los ataques de terroristas contra las infraestructuras críticas. Las principales amenazas contra la seguridad son el espionaje (tanto económico como político), los delitos financieros transnacionales y el potencial de acciones militares. Cada uno de esos problemas requiere políticas y prioridades distintas y conlleva implicaciones diferentes para la privacidad" (Jorge Pérez Martínez, 2012, pág. 48). En la actualidad, se hace necesario plantearse estrategias concretas que mitiguen las dificultades y necesidades en cuanto a este tema, trabajado esquemas de gestión que permitan detectar y tratar dichos riegos, implementando arquitecturas de seguridad que faciliten la medición de los niveles de riegos y de incidentes; y al estar tan conectados al uso de internet " La privacidad siempre estará en peligro sin una Ciberseguridad adecuada, pero una mejor Ciberseguridad en sí misma no protegerá la privacidad" (Jorge Pérez Martínez, 2012, pág. 48).

"La tensión entre la seguridad y la privacidad se sostiene sobre los pilares de Internet, que comenzó como una herramienta de investigación y se convirtió, de manera involuntaria, en una red global. Los creadores de Internet no tuvieron en cuenta muchos aspectos de importancia durante el proceso

de diseño, entre los que se incluyen la seguridad y la privacidad. El diseño original de Internet se centraba en garantizar una conectividad sencilla y fiable" (Jorge Pérez Martínez, 2012, pág. 49), como por ejemplo el sector financiero, las revoluciones agrícolas y el sector salud, que con sus nuevas oportunidades digitales han cambiado constantemente nuestras vidas, sin embargo, el control de nuestra privacidad nos requiere de manera urgente establecer barreras que nos protejan. "Mientras que una Ciberseguridad débil pone en peligro la privacidad, los procesos de defensa pueden exigir a los gobiernos emprender medidas invasivas con el fin de controlar las comunicaciones y detectar el software malicioso y otras acciones ilegales" (Jorge Pérez Martínez, 2012, pág. 49). Pero no debemos dejar de lado, que las amenazas informáticas que viene en el futuro son mucho más profesionales, las cuales manipulan el significado del contenido virtual, haciendo necesario preservar la confidencialidad, integridad y disponibilidad de la información.

Plantear estrategias compartidas se hace necesariamente probable, debido a la inestabilidad de la seguridad de la información emergente, lo cual hace que diariamente, segundo a segundo se convierta en un reto que implica desaprender aquello que conocemos y considerar un aprendizaje desde las especulaciones del presente. Así, los algoritmos, las aplicaciones y la conexiones, serán comprometidas, requiriendo un nuevo escenario en los negocios digitales.

Uno de los eslabones más débiles en cuanto al manejo de la información, es el ser humano, de aquí la idea de generar una cultura organizacional como seres humanos responsables de la información. Como se sabe, la amenaza más difundida en Colombia es el "phishing" (mensajes falsos para robar información), lo cual hace que muchas amenazas conocidas y desconocidas lleguen rápidamente hasta la información confidencial, inclusive a degenerar el servicio, a pesar de herramientas existentes, la cuales son muy avanzadas, muchos de los virus están programados para operar sigilosamente, encontrando la vulnerabilidad, la cual puede permitir accesos o restricciones a datos específicos, superposición de identidad, entre otras.

Colombia fue el primer país latinoamericano en aprobar una Estrategia Nacional de Ciberseguridad, cambiando así el enfoque de gestión de riesgo existente y la protección del ciberespacio para atender amenazas, (hasta el año 2011), incluyendo principios y estrategias que sirven como guía para la prevención de los riesgos más eminentes, contribuyendo al crecimiento de la economía digital nacional, y a su vez la prosperidad económica y social del país.

Las organizaciones y hasta los mismos Estados, han empezado a realizar un cambio en sus estrategias con el fin de lograr retener las amenazas presentadas o por lo menos disminuir su impacto. Entre lo más notorio encontramos la valoración de activos, capacidades, necesidades, amenazas y riesgos en sectores públicos y privados; adaptándose según las diferentes capacidades, presupuestos e infraestructuras.

A pesar de que el mundo avanza velozmente, en cuanto al tema de ciberseguridad, las organizaciones aún no hacen de este tema un punto estratégico para ellas mismas, incluso, algunas todavía operan con niveles muy limitados y algunas muy pocas con medidas básicas. No obstante, la preocupación por la privacidad se volvió un tema de mucha importancia, tanto que, otras partes del mundo analizarán y contemplarán la posibilidad de una ley global en cuanto este tema.

2.2.4 Gestión de la ciberseguridad. "Refiriendo a la gestión de la Ciberseguridad es de anotar que, dentro del entorno tecnológico, la Ciberseguridad debe ser considerada un proceso y no una actividad aislada y diferenciada del resto de los servicios o herramientas informáticas. En el mundo actual, digitalizado y en el que Internet es ya parte esencial de cualquier servicio, organización o entorno, la seguridad es una cualidad, la cual hay que cuidar desde el principio y en cuya gestión participa gran cantidad de funcionarios. La Ciberseguridad es, en este sentido, un proceso que implica prevención, detección y reacción o respuesta, y que debe incluir un elemento de aprendizaje para la mejora continua del propio proceso. (Jorge Pérez Martínez, 2012, pág. 18). Las organizaciones deben contar no solo con soluciones tecnológicas, sino con gestiones que permitan concientizar a quienes representan el eslabón más débil de la cadena y comprender que la amenaza más grande a la que nos enfrentamos en no entender los riesgos que se corren

A menudo se presentan malentendidos, como el de creer que las técnicas y pautas establecidas en la ciberdefensa son las más adecuadas, sin entender que éstas necesitan ser consideradas estratégicamente, como el de identificar eventos que podrían impedir alcanzar objetivos establecidos institucionalmente.

Las organizaciones no cuentan con un incentivo financiero por el cual los lleve a mejorar en este tema, pero, es muy importante que entiendan que la verdadera protección comienza desde la misión de cada una. Es de vital importancia que las mismas, hagan foco en mejorar sus programas de riesgos: prevención, detección y respuesta.

En las fases antes mencionadas, lo más importante es protegerse ante los peligros que implica llevar a cabo estos procesos.

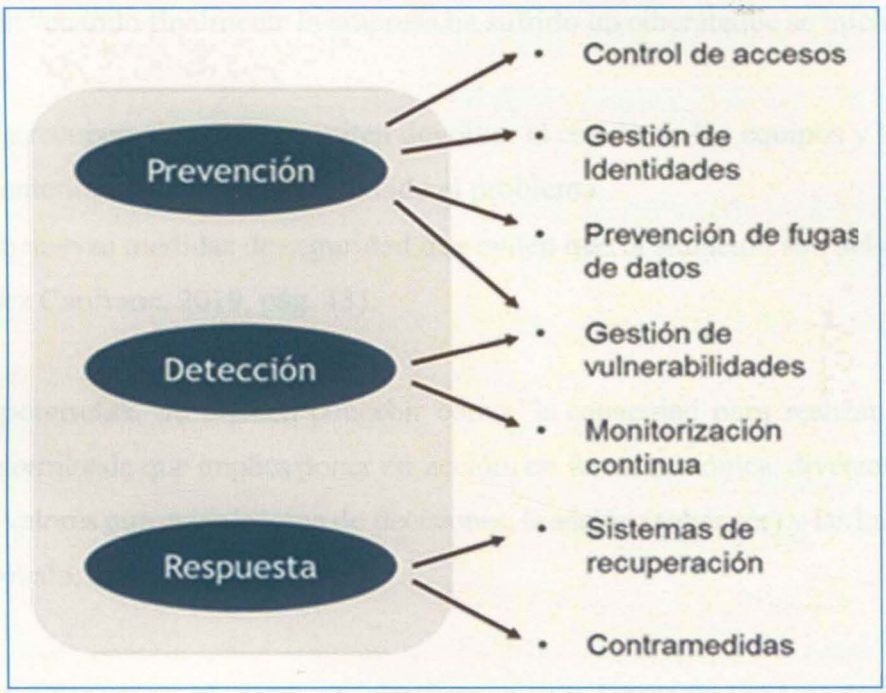


Figura 2. Etapas en la gestión de la ciberseguridad. Recuperado de la Fundación telefónica (2012)

1) *Prevención:* Como primera medida, todas las entidades deben desarrollar controles necesarios para mitigar el riesgo. Algunas de las más importantes son: "El control sobre quién accede a los recursos de la empresa y la asignación de permisos y credenciales al personal en función de los roles desempeñados.

Establecimiento de medidas técnicas, organizativas y legales para evitar fugas de información de la

empresa.

Definición de una política de seguridad de la red, que debe ser implementada a través de herramientas de software y hardware y que debe ser auditada con frecuencia para garantizar su eficacia" (Rodríguez Canfranc, 2019, pág. 13).

2) Detección: En este ciclo, ya se deben introducir tareas que permitan gestionar falencias que presenten los programas a través de un monitoreo continuo.

3) Respuesta: "cuando finalmente la empresa ha sufrido un ciberataque se inicia esta etapa que conlleva:

- Los sistemas de recuperación, que permiten devolver el estado de los equipos y las aplicaciones al punto de partida anterior a que se haya producido el problema.
- la aplicación de nuevas medidas de seguridad que eviten que la situación se vuelva a producir en el futuro" (Rodríguez Canfranc, 2019, pág. 13).

2.2.5 Competencias. Se pueden concebir como "la capacidad para realizar una actividad o tarea profesional determinada que implica poner en acción, en forma armónica, diversos conocimientos (saber), actitudes y valores que guían la toma de decisiones, la acción (saber ser) y las habilidades (saber hacer)" (Monzò Arèvalo, 2006, pág. 11).

Las competencias para el caso se clasifican como ***interpersonales***, ***instrumentales*** y ***sistémicas***, en donde las competencias "***instrumentales*** refieren a aquellas capacidades cognitivas, metodológicas y lingüísticas que se consideran necesarias para la comprensión, la construcción, el manejo, el uso crítico y ajustado a las particularidades de las diferentes prácticas, métodos, procedimientos, técnicas e instrumentos profesionales" (Carlos van-der Hofstadt Roman, 2013, pág. 31); en tanto que las "***sistémicas*** son capacidades y habilidades relativas a todos los sistemas, combinación de entendimiento, sensibilidad y conocimiento" (Carlos van-der Hofstadt Roman, 2013, pág. 31); y finalmente las "***interpersonales*** se relacionan con "las habilidades de relación social e integración en distintos colectivos, así como la capacidad de desarrollar trabajos en equipo específicos y multidisciplinares" (Carlos van-der Hofstadt Roman, 2013, pág. 31).

Capítulo III: Contexto de la situación colombiana en materia de ciberdelincuencia

Con el fin de entender el proceso de gestión en ciberseguridad que desempeñan los funcionarios de Policía Nacional de Colombia, se consideró pertinente realizar un contexto de la situación colombiana en materia de Ciberdelincuencia, para de esta forma poder hacer referencia a las estrategias definidas por la institución con relación a las etapas de prevención, detección y respuestas propias de la gestión de la ciberseguridad.

El 11 de abril de 2011, se presentó en Colombia el ataque a la página web del Ministerio del Interior y de Justicia, y tan solo tres días después fue atacada la página del Senado de la República. Luego el 15 de abril de 2011, fue atacada la página web de la Presidencia de la República.

Entre las tres tendencias principales en inseguridad, el primer puesto lo ocupa la utilización de códigos maliciosos Phishing (Robo de información), el segundo puesto lo determina la fuga y robo de datos con un uso abusivo de los sistemas, y la tercera y más popular en los últimos tiempos se encuentra el cobro masivo ilegal (pirámides cibernéticas, la pornografía infantil). Para el "2009 una serie de ataques afectaron la Casa Blanca, el Departamento de Seguridad Interna (DHS), el Departamento de Defensa, la Administración Federal de Aviación y la Comisión Federal de Comercio. Otro suceso fue el que reportó la Guardia Civil española en marzo de 2010, cuando desmanteló a una de las mayores redes de computadores "zombies", conocida con el nombre de BotNet Mariposa", compuesta por más de 13 millones de direcciones IP infectadas, distribuidas en 190 países alrededor del mundo. Colombia ocupó el quinto puesto entre los países más afectados por esta red. (Departamento Nacional de Planeaciòn, 2011, pág. 6).

"En relación con seguridad cibernética, Colombia también ha sido objeto de ataques. Un caso por resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley "por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet". Este grupo ha atacado indistintamente entidades públicas y privadas, entre las que se

cuentan PayPal, el banco suizo Post Finance, MasterCard, Visa y páginas web del gobierno suizo (Departamento Nacional de Planeaciòn, 2011, pág. 9).

Según el informe de la Policía Nacional y acorde con las amenazas del Cibercrimen presentadas en Colombia durante el 2016 y 2017, se registraron 15.565 incidentes informáticos a través de las diferentes plataformas dispuestas por el Centro Cibernético Policial, es así que el análisis permite describir algunos aspectos como: se recibieron 15.5658 incidentes informáticos. A partir del análisis de información, se identificaron algunos aspectos que permiten caracterizar el delito informático en Colombia", así:

1. De acuerdo con los incidentes atendidos, se observa el cambio que han tenido los cibercriminales en las victimas, interesándose de esta maneta por empresas que generan gran rentabilidad. "En el 2014, del total de incidentes atendidos, el 92% afectaban a los ciudadanos del común, para el 2015 el 63% y en el 2016 el 57%, presentando una disminución del 35%. Mientras tanto, el sector empresarial pasó de un 5% a un incremento del 28% en los reportes atendidos". (Policìa Nacional - Cai virtual, 2017, pág. 2).

2. El phishing y la ingeniería social, son algunas de las técnicas más usadas por los delincuentes para obtener información confidencial o llevar acabo transacciones no autorizadas, es así que esta modalidad facilita la estafa o publicación de falsas ofertas en portales web y cajeros automáticos que le han permitido a los ciberdelincuentes copiar las bandas magnéticas o el chip de las tarjetas débito o crédito.

3. Desde la estrategia de Gobierno en Línea se pretende contribuir a la prestación de servicios transparentes y participativos, de lo que, los ciberdelincuentes aprovecharon para distribuir malware, mediante la utilización de correos institucionales de entidades estatales, es así que "Durante el 2016 hubo un incremento del 114.4% en ataques de malware en el país, en relación al 2015 (153 incidentes reportados en el 2015, 328 incidentes reportados en el 2016). De la misma forma el Ransomware tuvo un incremento de ataques del 500% en comparación del 2016 a 2015, es decir, se pasó de 14 incidentes atendidos en el 2015, a 84 en el 2016, siendo esta modalidad, una de las principales tendencias del Cibercrimen en el 2017. Se estima que el 76% de las infecciones de Ransomware se da

a través del correo electrónico y spam" (Policìa Nacional - Cai virtual, 2017, pág. 3).

4. Buscadores de nivel 4 o Deep Weeb, los cuales permiten la comercialización ilegal de armas, drogas, etc., mediante transacciones realizadas por correos cifrados y pagos en moneda virtual, las cuales no tienen ningún tipo de regulación, lo que los hace más llamativos para los ciberdelincuentes al momento de recolectar el dinero de las víctimas.

Según información reciente suministrada por la Policía Nacional (2018), en un contexto más reciente, en lo corrido del año 2018, las denuncias por delitos informáticos se incrementaron en un 68.5%, la cual corresponde a 6170 denuncias con respecto al año anterior; de las cuales llama la atención el notable aumento en las principales ciudades colombianas a pesar de los 19.907 portales web bloqueados en los últimos 7 años que son utilizados como mercados criminales, a partir de allí se clasifican los principales delitos en los que se encuentran identificados, el hurto a medios informáticos y semejantes, violación de datos personales y acceso abusivo a sistemas informáticos, resaltados en las ciudades como Bogotá con 4805 denuncias, Medellín con 1831 denuncias y Cali con 1490 denuncias, representados en incrementos de 114%, 36,2 y 50% respectivamente.

De acuerdo a lo anterior, los delitos que más registraron denuncias son: hurto por medios informáticos y semejantes con 8817 denuncias, violación de datos personales con 2180 denuncias y acceso abusivo a un sistema informático con 2005 denuncias.

Capitulo IV Conocimientos y competencias de los integrantes de Policía Nacional en temas de Ciberseguridad.

La realización de un análisis objetivo del proceso de gestión de la ciberseguridad en la Policía Nacional de Colombia, en la era digital[1], precisa una indagación base en la cual se enfatice en el nivel de competencias específicas del personal encargado del área de la seguridad en el Ciber- mundo, en otras palabras, es necesario proponer unos fundamentos soportes bajo las cuales los profesionales ejercen sus función, pues estos son claves para el desarrollo de un proceso adecuado en el cual se logre un ejercicio integral de la profesión policial, que propenda efectivamente por la prevención, detección y capacidad de respuesta, en el Ciberespacio. Estos conocimientos cognitivos en términos generales están directamente relacionados al *saber, hacer y ser;* de forma específica, el *saber* está ligado directamente con los conocimientos teóricos necesarios para llevar a cabo sus funciones; en tanto que el *hacer* refiere a la aplicabilidad de los conocimientos, es decir, a poder cristalizar o materializar los saberes teórico en situaciones reales contextualizadas, que den respuestas a las problemáticas de forma efectiva; finalmente está el ser que integra un cúmulo de principios y valores que definen el actuar de las personas dentro de cualquier escenario entre ellos el laboral.

Para el caso refiriendo al proceso de selección de personal competente, obedece al cumplimiento de un manual de funciones consagrado legalmente en la Resolución No. 0937 del 10/03/2016 "Por la cual se establece el Manual de Funciones para el personal uniformado de la Policía Nacional, la metodología de evaluación para el perfil de los cargos y se derogan unas disposiciones" es decir, que a todos los integrantes de la institución se les realiza la evaluación del perfil del cargo, analizando los componentes en forma integral sin descalificar al funcionario para desempeñar un cargo. Eso significa que todos los integrantes de la institución fueron previamente seleccionados bajo criterios rigurosos de elección, en los cuales se establece un perfil, unas

[1] Datos interrelacionados y ordenados según una estructura especifica que puede almacenarse, procesarse y transmitirse electrónicamente, además de transformar su formato para su introducción y comprensión por el ser humano. (Desongles Corrales, 2006, pág. 12)

funciones y una responsabilidad, las cuales deben ser cumplidas a cabalidad por todos los integrantes de la institución; así:

"una vez realizado el cruce del perfil del cargo y los datos del funcionario, se analiza la información para otorgar un puntaje de ajuste al perfil, analizando los tres componentes de las competencias (*saber, saber hacer y saber estar*) en forma integral, es decir que ninguno de los componentes en forma separada, descalifica a un funcionario para desempeñarse en un cargo". (Policía Nacional , 2016, pág. 4)

Figura 3. Modelo de gestión del talento humano- competencia. Fuente: Elaboración propia

Refiriendo *saber, saber hacer y saber estar* que se evidencia en la figura, que fundamentan el manual de funciones por competencias de la Policía nacional al Según Resolución 0937 (2016, art. 6) estas refieren concretamente a:

a) "Competencias del saber: Las competencias del saber representan los conocimientos mínimos requeridos para el desempeño de cada cargo, así: 1) *educación superior*: Compuesta por la familia de estudios técnicos profesionales, tecnológicos, profesionales universitarios y posgrados y *2) formación para el trabajo:* Compuesta por el Grado policial y la actualización de conocimientos evidenciados en seminarios, cursos y diplomados" (Policía Nacional , 2016, pág. 6)

b) "Competencia del saber hacer: Es a la experiencia mínima requerida para ocupar el cargo. Está directamente vinculada con el reconocimiento de los cargos ocupados con anterioridad por parte del funcionario, con el fin de asegurar que su experiencia laboral se ha desarrollado en áreas afines a dicho cargo" (Policía Nacional , 2016, pág. 6).

c) "Competencia del saber estar: El componente del *saber estar* hace referencia a las habilidades que tiene el funcionario policial para desarrollar un cargo con capacidad y destreza aprovechando su experiencia y conocimiento; considerando las demandas del entorno. De esta manera, se definen así: 1) *habilidades comportamentales*: comportamientos que emplea una persona para movilizar su voluntad y la de otros con el fin de alcanzar de manera efectiva los objetivos propuestos. Estos comportamientos están identificados a través de los instrumentos de evaluación con los que cuenta la Dirección de Talento Humano y *habilidades funcionales*: Son aquellas destrezas requeridas para desempeñar las actividades que componen una función laboral, según los estándares y la calidad establecidos por la Institución. Estas habilidades se relacionan además con el "quehacer", es decir, con la especificidad del cargo y las funciones a realizar" (Policía Nacional , 2016, pág. 6).

Figura 4. Modelo de gestión del talento humano- competencia específicas. Fuente: Elaboración propia.

Las competencias del saber, saber hacer y saber estar propuestas para el desarrollo profesional y laboral de la policía nacional refieren a un conjunto de *experiencias, habilidades y conocimientos* las cuales permiten a los funcionarios Policiales desempeñar su profesión de una manera eficiente y eficaz, dentro de un contexto de integridad y ética laboral en la Policía Nacional se realizó a través de 2 categorías relacionadas con el desarrollo profesional no sólo a nivel de investigación sino a nivel de integralidad laboral. Las competencias analizadas son las *instrumentales* y las *sistémicas*, todas ellas enfocadas a determinar las habilidades y capacidades de estos profesionales en materia de ciberseguridad. Teniendo en cuenta que las "competencias instrumentales refieren las habilidades cognitivas, capacidades metodológicas, destrezas tecnológicas y destrezas lingüísticas" (Ministerio de Educaciòn , 2011, pág. 105) que tienen funcionario, en tanto, que "las competencias sistémicas están enfocadas a la capacidad de aplicar los conocimientos, métodos y herramientas qué le son otorgadas para el desarrollo sus funciones, así mismo refiere a la capacidad de aprender y aplicar los nuevos conceptos que se van requiriendo para su cargo, desde un enfoque motivacional y creativo vehemente al cambio" (Ministerio de Educaciòn , 2011, pág. 124).

Relacionando las competencias *instruméntales* y *sistémicas* con la gestión en ciberseguridad que define el protocolo de acción de la Policía Nacional, los cuales refieren directamente a la *prevención*, *detección* y *respuesta*, es evidente que existe una relación directa en la medida en que estas competencias son la base para el desarrollo de una gestión efectiva. En otras palabras, para lograr un tratamiento oportuno a cualquier delito cibernético es necesario que los funcionarios tengan unas habilidades cognitivas, capacidades metodológicas y destrezas tecnológicas y lingüísticas, que les permita tomar decisiones y actuar de forma coherente y oportuna ante los hechos y sucesos delictivos.

Relación entre las competencias instrumentales y los compontes de gestión en ciberseguridad: En el caso particular de las competencias instrumentales esta infieren en el desarrollo de la gestión en la ciberseguridad de forma integral como se observa en la figura, sin embargo es evidente que algunas tienen mayor incidencia que otras; por ejemplo, el manejo adecuado de los sistemas de información, los conocimientos en ciberseguridad e información, así como el dominio en los procesos, procedimientos y protocolos y la aplicación de principios de seguridad, privacidad y control influyen directamente en la ***prevención***, teniendo en cuenta que estás se relaciona con el control de acceso y gestión de entidades, la de fugas de datos y la seguridad en la red.

De otro lado, el trabajo orientado a la consecución de resultados, información oportuna a superiores y el desarrollo de investigaciones favorecen la ***detección*** contribuyendo a la gestión de las vulnerabilidades y la monitorización continua.

Finalmente, la toma de decisiones oportunas, la autonomía en la solución de problemas y el manejo de procedimientos, contribuyen a dar ***respuesta*** pertinente llevando a la recuperación de la información en caso de ataque y la toma de contramedidas adecuadas.

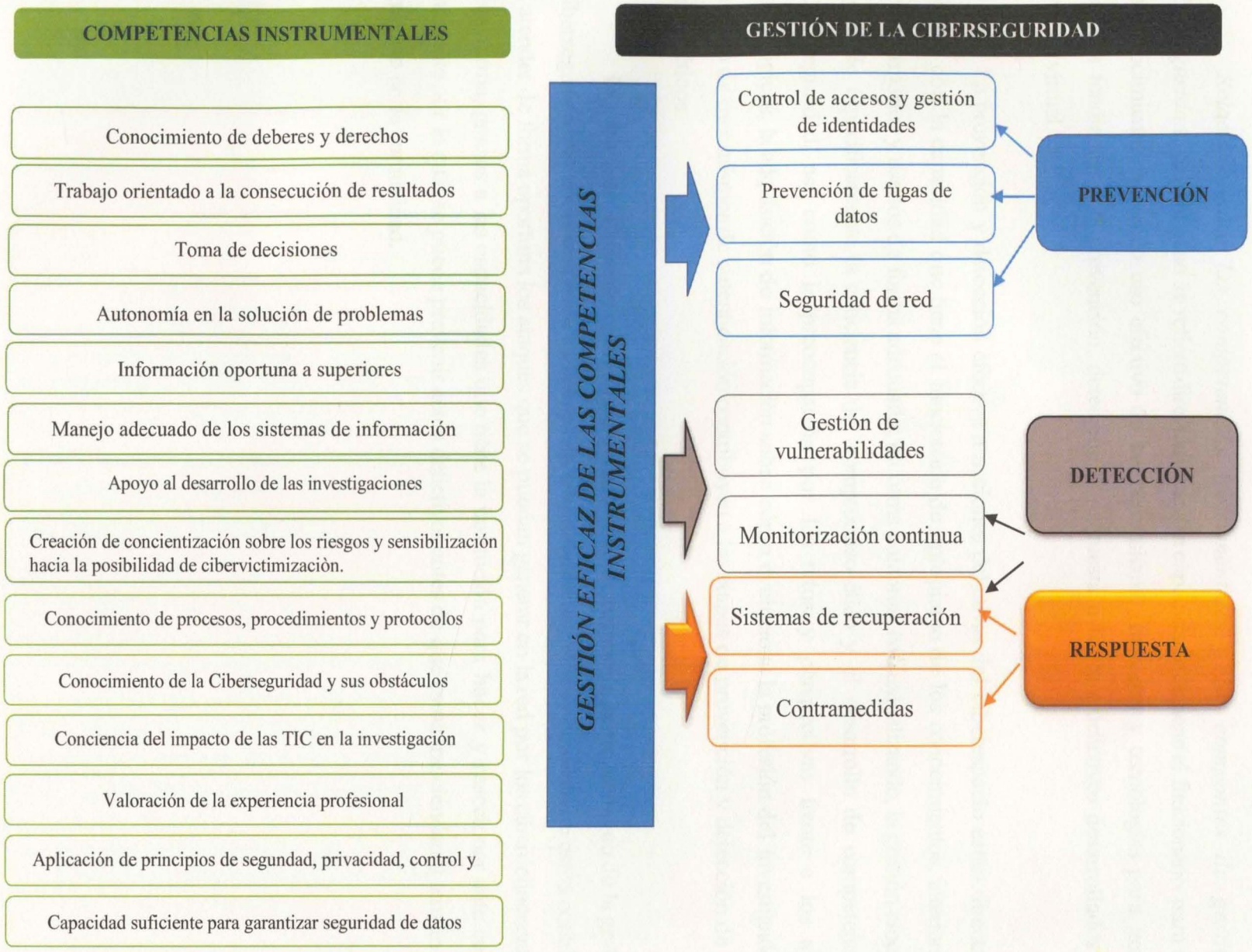


Figura 5. Relación entre las competencias instrumentales y la gestión de la ciberseguridad. Fuente: Elaboración propia.

Relación entre las competencias instrumentales y los compontes de gestión en ciberseguridad: para el caso se refiere directamente a la capacidad que tiene el funcionario para aplicar los conocimientos haciendo uso efectivo de las herramientas, métodos y tecnologías para gestionar acciones tendientes a la prevención, detección y respuesta a hechos delictivos desarrollados en el entorno virtual.

La prevención y detección efectiva a acciones delictivas del ciberespacio están directamente ligadas con la capacidad que tiene el funcionario de apropiarse de los conocimientos, interiorizarlos, transformarlos y usarlos de forma adecuada; en otras palabras, contextualizando, la gestión cibernética depende específicamente la conciencia del compromiso ético y el desarrollo de competencias en Ciberseguridad, así como la preocupación por los retos y perspectivas frente a los avances tecnológicos, la adquisición de información sobre cómo evoluciona la profesión del investigador y el manejo de mecanismos de autenticación contribuyen a las etapas de prevención y detección de delitos cibernéticos.

De otro lado, haciendo referencia a la capacidad de respuesta como elemento de la gestión en ciberseguridad, el afrontamiento a incidentes de ciberseguridad y el conocimiento de estos contribuyen a atender de forma oportuna los ataques que se puedan generar en la red por los ciberdelincuentes. De esta forma, gracias a las capacidades que tiene la institución para hacer y reaccionar ante cualquier incidente por lo cual se puede prevenir actos delictivos antes de que estos trasciendan y tengan mayor impacto en la comunidad.

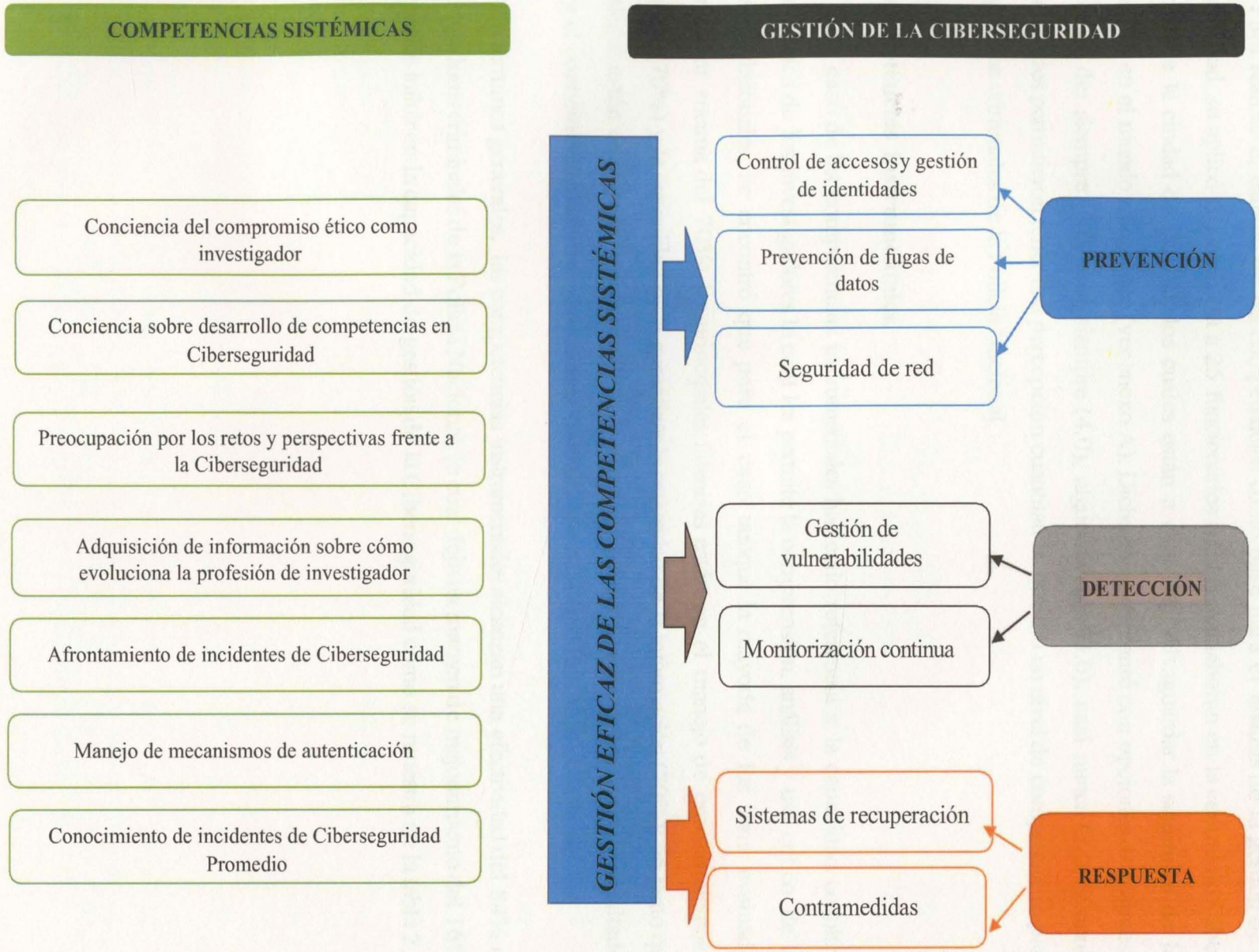


Figura 6. relación entre las competencias sistémicas y la gestión de la Ciberseguridad. Fuente: Elaboración propia

Para realizar el estudio de las competencias como base para el análisis de la gestión de la Ciberseguridad, se aplicó una encuesta a 25 funcionarios activos que laboran en la central de Ciber-inteligencia de la ciudad de Bogotá, los cuales están a cargo de salvaguardar la seguridad de los colombianos en el mundo cibernético (ver anexo A). Dicha encuesta contó con opciones de respuesta y valoración de: siempre (5.0) casi siempre (4.0), algunas veces (3.0), casi nunca (2.0) y nunca (1.0); las cuales permitieron tener una percepción cuantitativa, que dio un nivel de competencias para investigadores criminales de la Policía Nacional.

4.1 Competencias instrumentales.

En el caso de las competencias instrumentales haciendo referencia a la capacidad cognitiva y metodológica de los investigadores la cual les permite la comprensión, análisis y uso crítico de las técnicas profesionales, se encontró que para el caso aunque la mayoría de los ítems evaluados estuvieron por encima del 70%; las principales falencias están en el manejo de procedimientos e información (70%) y la capacidad para garantizar la seguridad de la información (70%); en tanto que las fortalezas están en la toma decisiones (90%), el trabajo orientado a la consecución de resultados (91%) y el conocimiento deberes y derechos (94%).

En términos generales, las competencias instrumentales alcanzan una efectividad del 84% en los investigadores criminales de la Policía Nacional, lo cual deja un margen de mejoramiento del 16%, lo cual puede influir en la capacidad de gestión de la Ciberseguridad como se muestra en la tabla 2.

Tabla 2. Estimación de las competencias instrumentales de los investigadores judiciales de la Policía Nacional.

	S 5		CS 4		AV 3		CN 2		N 1		Cal.	Nivel %
	NR.	%	NR.	%	NR.	%	NR.	%	NR.	%	NR.	%
Conocimiento de deberes y derechos	14	56%	11	44%	0	0%	0	0%	0	0%	4,56	91%
Trabajo orientado a la consecución de resultados	14	56%	10	40%	1	4%	0	0%	0	0%	4,52	90%
Toma de decisiones	17	68%	8	32%	0	0%	0	0%	0	0%	4,68	94%
Autonomía en la solución de problemas	12	48%	12	48%	1	4%	0	0%	0	0%	4,44	89%
Información oportuna a superiores	13	52%	10	40%	2	8%	0	0%	0	0%	4,44	89%
Manejo adecuado de los sistemas de información.	13	52%	7	28%	5	20%	0	0%	0	0%	4,32	86%
Apoyo al desarrollo do las investigaciones en repositorio en la nube	11	44%	11	44%	3	12%	0	0%	0	0%	4,32	86%
Conocimiento de procesos, procedimientos y protocolos	13	52%	10	40%	2	8%	0	0%	0	0%	4,44	89%
Valoración de la experiencia profesional	9	36%	14	56%	1	4%	1	4%	0	0%	4,24	85%
Conocimiento de la ciberseguridad y sus obstáculos	2	8%	11	44%	10	40%	2	8%	0	0%	3,52	70%
Conciencia del impacto de las TIC en la investigación	7	28%	7	28%	8	32%	2	8%	1	4%	3,68	74%
Conocimiento de la información que adelanto dentro de los procesos investigativos	5	20%	8	32%	7	28%	5	20%	0	0%	3,52	70%
Aplicación de principios de segundad, privacidad, control y transparencia	7	28%	8	32%	7	28%	2	8%	1	4%	3,72	74%
Percepción de confidencialidad de la información	15	60%	6	24%	3	12%	1	4%	0	0%	4,40	88%
Capacitación suficiente para garantizar seguridad de datos	5	20%	15	60%	4	16%	1	4%	0	0%	3,96	79%
Manejo de procedimientos para manejo información vulnerable	7	28%	13	52%	4	16%	1	4%	0	0%	4,04	81%
promedio	**10,3**	**41%**	**10**	**0,4**	**3,6**	**15%**	**0,9**	**4%**	**0**	**1%**	**4,18**	**84%**

Fuente: Elaboración propia, información proveniente de la encuesta de diagnóstico. (2017)

El análisis de las competencias instrumentales se fortalece en: la toma decisiones, trabajo orientado a la consecución de los resultados y conocimiento de los deberes y derechos, factores de análisis que superan una efectividad del 90%. De otro lado, se presenta oportunidad de mejora de un 30% a las debilidades que hay en: conocimiento de la información que adelanto dentro de los procesos investigativos y conocimiento de la ciberseguridad y sus obstáculos. Ver figura 7.

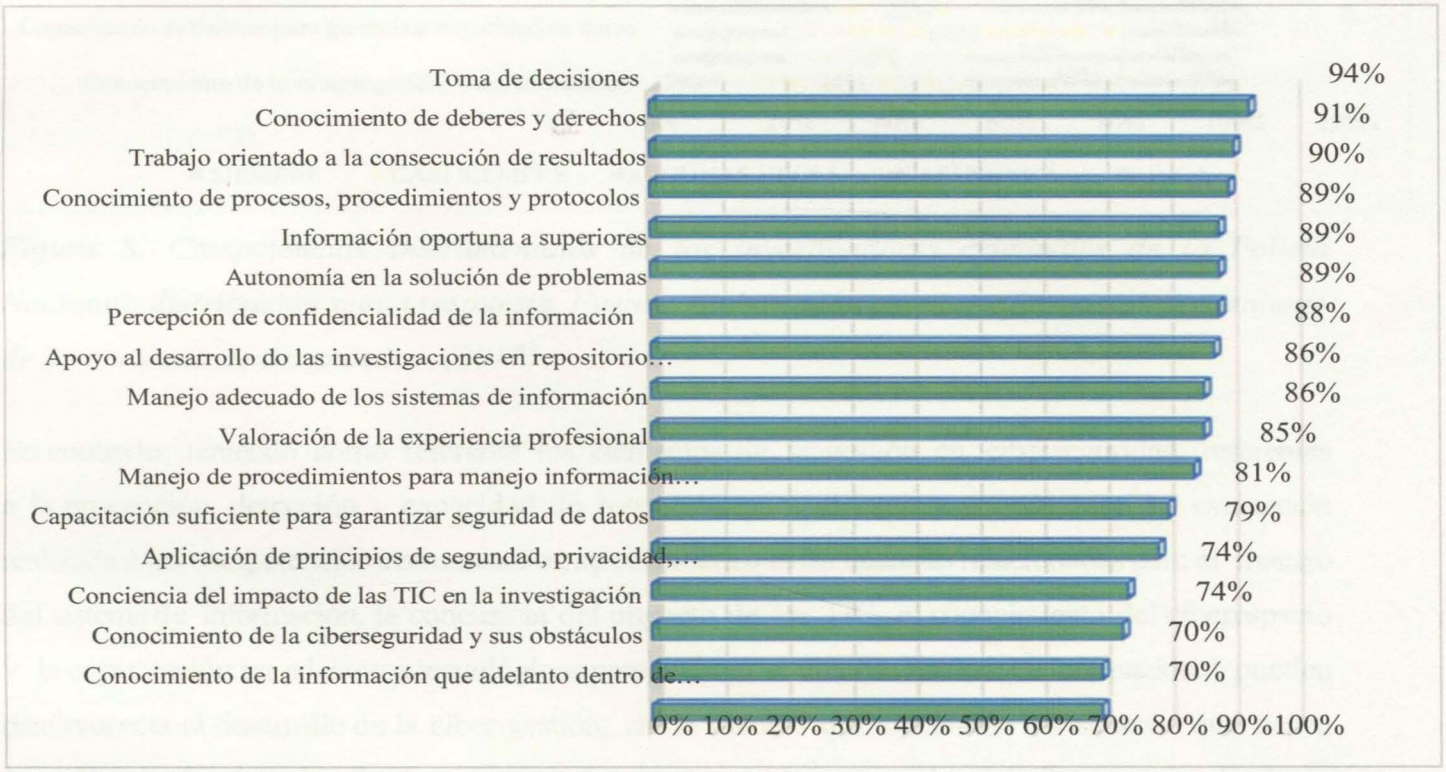


Figura 7. Evaluación de las competencias instrumentales de los investigadores criminales de la Policía Nacional. Fuente: Elaboración propia, información proveniente de la encuesta de diagnóstico. (2017)

Como se muestra en la figura 8, un análisis pormenorizado de la elección de respuesta en donde se tiene opción de siempre, casi siempre, algunas veces, casi nunca y nunca; siendo siempre la opción de mayor nivel (5) es evidente que el 68% de los funcionarios conocen la clasificación en la confidencialidad de la información y el 20% debilidad plena en el conocimiento de la información que adelanto dentro de los procesos investigativos.

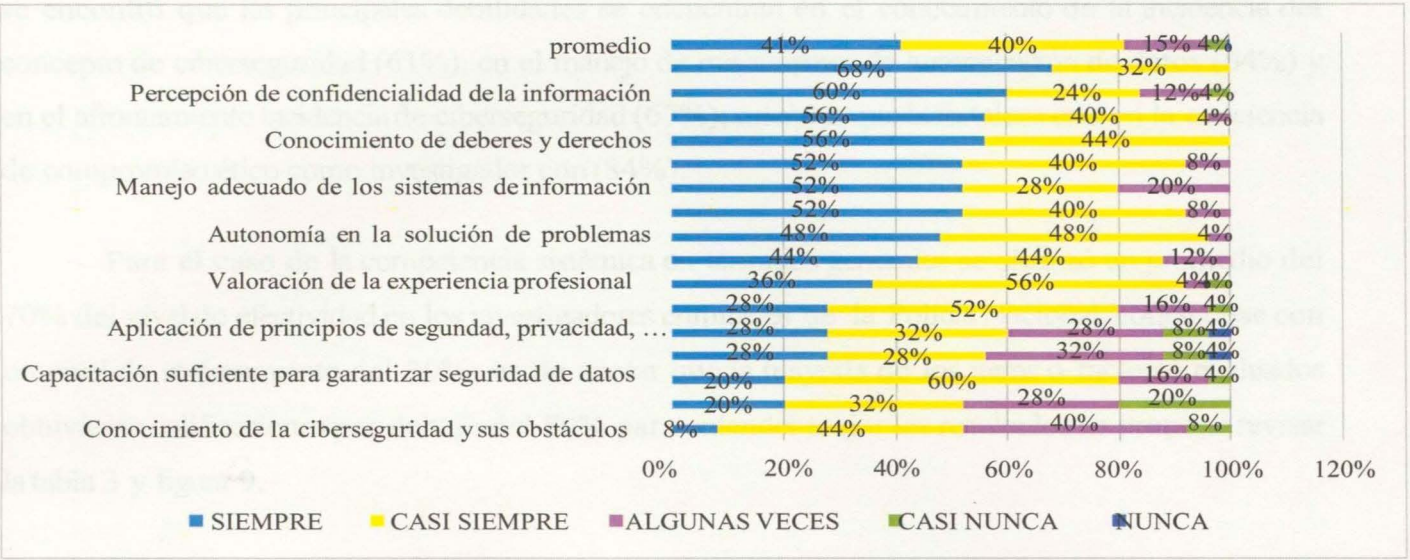


Figura 8. Competencias instrumentales de los investigadores criminales de la Policía Nacional: distribución según respuesta. Fuente: Elaboración propia, información proveniente de la encuesta de diagnóstico. (2017)

En contexto, teniendo como referente los elementos de la gestión en ciberseguridad, referentes a la prevención, detección y capacidad de respuesta, para el caso y acorde con la evaluación realizada a las competencias instrumentales, se considera que las falencias relacionadas con: el manejo del sistema de información, la conciencia del impacto de las TIC, el conocimiento del ciberespacio y la capacitación en adelantos tecnológicos presentes en el entorno nacional e internacional; pueden desfavorecer el desarrollo de la ciber-gestión, en la medida que minimizan los saberes que tienen los policías o funcionarios frente a temas relevantes para la protección del ciberespacio. Es decir, la ausencia de conocimientos principalmente en el área tecnológica dentro del contexto de la gestión de ciberseguridad es una falencia de gran impacto, puesto que le da una ventaja al delincuente al estar más preparado y avanzado a nivel tecnológico, en consecuencia, puede ir más delante del actuar policial, logrando realizar sus acciones delictivas y afectar las empresas, personas y comunidad en general.

4.2 Competencias sistémicas.

En el caso de las competencias sistémicas relacionadas con la capacidad de entendimiento sensibilidad y conocimiento de los deberes propios del cargo de investigadores,

se encontró que las principales debilidades se encuentran en el conocimiento de la incidencia del concepto de ciberseguridad (61%), en el manejo de mecanismos de autenticación de datos (64%) y en el afrontamiento incidencia de ciberseguridad (67%); mientras que la fortaleza está en la conciencia de compromiso ético como investigador con (84%).

Para él caso de la competencia sistémica en términos generales se alcanzó un promedio del 70% del nivel de efectividad en los investigadores criminales de la Policía Nacional, contándose con un nivel de mejoramiento del 30%; es de anotar que la mayoría de los ítems o factores evaluados obtuvieron calificaciones por debajo del 80% para entender mejor los resultados se propone revisar la tabla 3 y figura 9.

Tabla 3. Estimación de las competencias sistémicas de los investigadores criminales de la Policía Nacional.

	S 5		CS 4		AV 3		CN 2		N 1		Cal.	Nivel
	NR.	%	NR.	%	NR.	%	NR.	%	NR.	%	NR.	%
Manejo de mecanismos de autenticación	5	20%	8	32%	4	16%	3	12%	5	20%	3,20	64%
Conocimiento de incidentes de ciberseguridad	4	16%	8	32%	3	12%	5	20%	5	20%	3,04	61%
Afrontamiento de incidentes de ciberseguridad	5	20%	6	24%	7	28%	7	28%	0	0%	3,36	67%
Preocupación por los retos y perspectivas frente a la ciberseguridad	4	16%	9	36%	9	36%	3	12%	0	0%	3,56	71%
Adquisición de información sobre cómo evoluciona la profesión de investigador	6	24%	4	16%	12	48%	3	12%	0	0%	3,52	70%
Conciencia sobre desarrollo de competencias en ciberseguridad	9	36%	6	24%	6	24%	3	12%	1	4%	3,76	75%
Conciencia sobre la labor de investigador.	9	36%	13	52%	2	8%	1	4%	0	0%	4,20	84%
Promedio	6	24%	8	31%	6,1	25%	3,6	14%	2	6%	3,52	70%

Fuente: Elaboración propia, información proveniente de la encuesta de diagnóstico.

Refiriendo a los elementos que conforman las competencias sistémicas se logra el mejor nivel para conciencia sobre la labor de investigador y el menor nivel para conocimiento de incidentes de Ciberseguridad, ver figura 9.

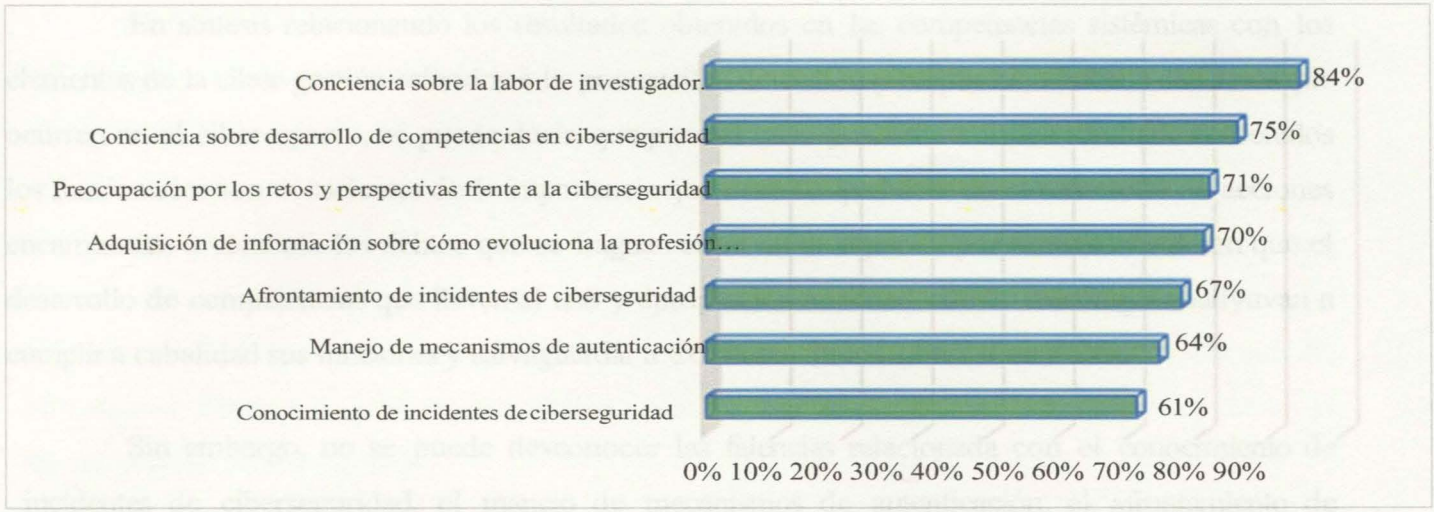


Figura 9. Evaluación de las competencias sistémicas de los investigadores criminales de la Policía Nacional. Fuente: Elaboración propia, información proveniente de la encuesta de diagnóstico.

Un análisis detallado de la elección de respuesta en donde se tiene opción de siempre, casi siempre, algunas veces, casi nunca y nunca; siendo siempre la opción de mayor nivel (5) evidencia que el 36% de los funcionarios tiene plena fortaleza en la conciencia sobre la labor de investigador y debilidad plena para un 20% en manejo de mecanismo de autenticación y conocimiento de incidentes en ciberseguridad. Ver figura 10.

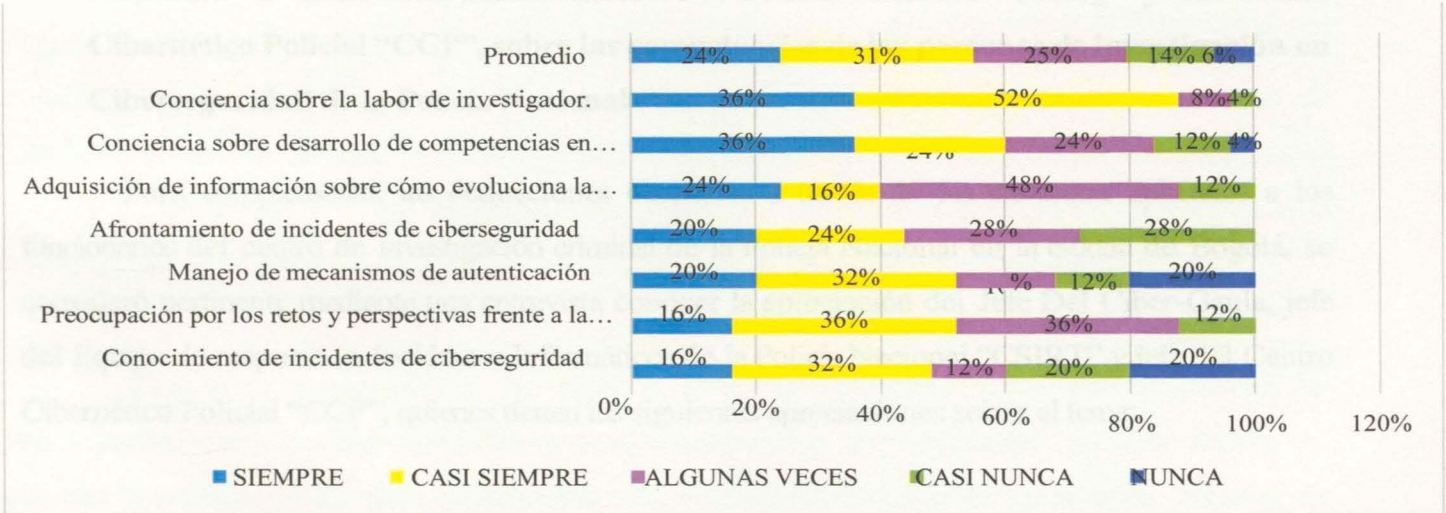


Figura 10. Competencias sistémicas de los investigadores criminales de la Policía Nacional: distribución según respuesta. Fuente: Elaboración propia, información proveniente de la encuesta de diagnóstico. (2017)

En síntesis relacionando los resultados obtenidos en las competencias sistémicas con los elementos de la ciber-gestión referidos a la prevención, detección y respuesta a hechos delictivos que ocurren en el ciberespacio, se puede decir, que para el caso y acorde con los resultados obtenidos los funcionarios son conscientes de la importancia que tiene su quehacer en el desarrollo de acciones encaminadas a combatir los delitos que se fraguan en el ciber espacio, por tanto, consideran que el desarrollo de competencias que lleven al uso y apropiación adecuado de la tecnología coadyuvan a cumplir a cabalidad sus funciones y salvaguardar a Colombia de los ciberdelincuentes.

Sin embargo, no se puede desconocer las falencias relacionada con el conocimiento de incidentes de ciberseguridad, el manejo de mecanismos de autenticación, el afrontamiento de incidentes cibernéticos, la adquisición de información sobre la evolución de los hechos delictivos en el ciberespacio y la falta de preocupación por los retos y perspectivas frente seguridad. Contextualizando, todas estas falencias pueden ser una ventaja para el delincuente, el cual dada su actividad delictiva siempre está a la vanguardia en conocimientos y hechos tecnológicos, además de conocer los modus operandi no sólo de los demás delincuentes, sino también de la policía Nacional y demás entidades competentes encargadas de salvaguardar el ciberespacio y proteger a la comunidad.

4.3 Apreciación de los jefes de la Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales "Ciber-Gaula", el Equipo de respuesta a Incidentes Informáticos de la Policía Nacional "CSIRT" y del Centro Cibernético Policial "CCP", sobre las competencias de las personas de investigación en Ciberseguridad de la Policía Nacional

Para complementar las deducciones obtenidas a través de las encuestas aplicadas a los funcionarios del centro de investigación criminal de la Policía Nacional en la ciudad de Bogotá, se consideró pertinente mediante una entrevista conocer la apreciación del Jefe Del Ciber-Gaula, jefe del Equipo de respuesta a Incidentes Informáticos de la Policía Nacional "CSIRT" y jefe del Centro Cibernético Policial "CCP", quienes tienen las siguientes apreciaciones sobre el tema:

Según el jefe del Centro Cibernético Policial, en el cumplimiento del marco normativo en Ciberseguridad para Colombia y acorde con las políticas establecidas en el CONPES, se ha elegido un personal idóneo y capaz de desarrollar investigaciones de los ciberdelitos, de esta forma se cuenta con funcionarios analistas, peritos informáticos, ingenieros, desarrolladores, abogados e inclusive funcionarios que sin tener titulación, tienen un alto nivel de experiencia fundamentado en la experiencia en temas de ciberdelitos. Sin embargo, dado el crecimiento vertiginoso que ha tenido la actividad en el ciberespacio la policía ha trasformado su área de investigación y generado nuevas formas de investigar en el marco de la afectación del buen nombre, de la honra y acorde con la ley de protección de datos (ley 1581 del 2012).

Entre tanto, para el jefe de la Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales "Ciber-Gaula" el personal a cargo de la Ciberseguridad en la institución es competente, puesto que fueron preparados para el cargo y todos tienes carreras afines con la ingeniería de sistemas y de telecomunicaciones, asiente que realmente la unidades de investigación necesitan que los funcionarios que lleguen tengan un pregrado o una carrera técnica en ingeniería de sistemas, si no es así, queda muy complicado capacitar a un funcionario de cero, se necesita entonces una base que haga más eficiente el proceso de aprendizaje de nuevos conocimientos.

Pero, el personal de las unidades de investigación no solo ha recibido capacitaciones especializadas que fortalecen sus perfiles para desempeñar las funciones de investigación en el ciberespacio, sino también se les ha preparado en temas especiales enfocado al manejo y uso de las herramientas específicas; sin embargo, el jefe del Equipo de respuesta a Incidentes Informáticos "CSIRT", considera que las falencias presentadas en los equipos o unidades enfocadas a la ciberseguridad se genera como consecuencia de la falta de personal en dichos grupos.

Para el funcionamiento de las unidades de inteligencia acorde a las apreciaciones de los entrevistados, estas mantiene una infraestructura tecnológica a la vanguardia, la cual implica un paquete tecnológico que incluye capacitación para el manejo adecuado de los equipos, muchas de estas capacitaciones se realizan en otros países como Corea del Sur y España quienes tienen amplio conocimiento en temas informáticos; en el caso particular del Equipo de Respuesta a Incidentes

Informáticos de la Policía Nacional "CSIRT", las capacitaciones no solo se enfocan en el tema de ciberseguridad como tal, sino que abarca también temas relacionados con ingeniería de datos, análisis de redes sociales, malware, ethical hacking, informática forense, entre otros temas que deben dominar los funcionarios.

Refiriendo directamente al tipo de capacitaciones se debe partir del hecho de que existen diferentes unidades, que si bien manejan delitos informáticos y del ciberespacio tienen funciones diversas, como es el caso de AMERIPOL, INTERPOL, EUROPOL y J-CAT (Joint Cybercrime Action Taskforce), de esta forma las capacitaciones son diversas acorde a los roles y perfiles de los funcionarios, que al igual que las del manejo de equipos , por lo cual se trabaja en articulación a nivel nacional e internacional.

Así mismo, las capacitaciones en redes, ethical hacking, entre otros temas de ciberseguridad que generalmente se brindan cuando se requieren o se adquieren herramientas nuevas, sin embargo, en la Escuela de Investigación Criminal y en la Escuela de Tecnologías de la Información hay una oferta de capacitaciones en herramientas tecnológicas y de evidencia digital enfocados a la formación del personal.

Sin embargo, algunas investigaciones requieren ser desarrolladas por personal con conocimiento técnico en áreas de la informática y de telecomunicaciones, estas carreras implican un pregrado previo al ingreso y una maestría o especialización en seguridad en la información. Se considera importante la carrera profesional porque hay temas relevantes que se deben conocer a profundidad para ejercer una función eficientemente, por tanto, no basta con una capacitación o un curso.

Cabe aclarar que las capacitaciones y algunos cursos brindados a los funcionarios se hacen una única vez, y el hecho de que se hace un registro del personal por cada curso que realiza, de esta forma lo que prosigue es el desarrollo de actualizaciones constantes debido a la velocidad con que los entornos digitales avanzan.

Integrando las apreciaciones de los funcionarios encargados de la ciberseguridad en la Policía Nacional, con los de los jefes de la Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales "Ciber-Gaula", Equipo de Respuesta a Incidentes Informáticos "CSIRT" y Centro Cibernético Policial "CPP", se puede decir, que las competencias identificadas en los policías son el resultado de un proceso de selección objetivo en el cual se identifica y recluta al personal con capacidades y desarrollo profesional relacionado directamente con la tecnología, así como las capacitaciones y la preparación que reciben en el transcurso de su accionar dentro de su puesto de trabajo. Sin embargo, algunas de las falencias encontradas pueden ser el resultado de la falta de formación competitiva y a la vanguardia, la cual manejan las grandes unidades de investigación cibernética a nivel mundial; de esta forma, por cuestiones de presupuesto no es posible que dichas unidades puedan capacitar continuamente a los policías de Colombia, lo cual genera una desventaja ante las grandes organizaciones delictivas que cuentan con los recursos para acceder a la información.

Con base en los recursos humanos, tecnológicos y económicos con los que se dispone para ejercer la función policial de salvaguarda el ciberespacio y con el fin de combatir las falencias que poseen, la Policía Nacional en su Modelo de Gestión del Talento Humano y Cultura Institucional se orienta a:

- Articular los procesos para la gestión del talento humano que permita impactar positivamente el servicio de policía.
- Promover la cultura del trabajo en equipo en las unidades y dependencias policiales.
- Motivar e incentivar al personal de forma transparente, justa y equitativa con fundamento en su adecuado desempeño laboral.
- Fortalecer el sentido de pertenencia, identidad y compromiso con la institución.
- Reconocer el valor de la profesión policial y reflejar confianza ante el ciudadano.

De igual forma, según Policía Nacional (2018) teniendo en cuenta la gestión del conocimiento que se realiza en la Policía Nacional, y aunado esto, a las herramientas con las que dispone el Direccionamiento del Talento Humano para la identificación de las necesidades de capacitación, la institución prevé cada año el presupuesto para otorgar dicha capacitación en dos modalidades:

- Capacitaciones específicas: con el fin de generar conocimiento y experiencia en temas relacionados con la formación para el trabajo, de acuerdo con las necesidades determinadas por el cargo.
- Capacitaciones transversales: considerando el desarrollo de la cultura y los temas de interés general e institucional.

Para la Policía Nacional, el conocimiento enmarcado dentro de las competencias instrumentales y sistémicas, es:

Un activo intangible fundamental asociado con la capacitación del personal, estructuración y transmisión del conocimiento; de esta forma, debe gestionarse desde la adquisición, localización, retención y administración de la información, así como desde los datos crean en la institución a partir de las experiencias individuales y colectivas. Su objetivo principal es el diseño de estrategias, procesos, estructuras y sistemas que le permitan a la organización hacer uso de lo que conoce con el apoyo de la tecnología, con el propósito de crear valor para el servicio de policía y para la comunidad en general.

4.4 Grupos encargados de la ciberseguridad en la Policía Nacional de Colombia

La Policía Nacional cuenta con grupos específicos encargados directamente de la ciberseguridad de la institución, estos grupos nacieron como respuestas a la nuevas exigencias criminales, es decir, a la trascendencia de los delitos del contexto físico al contexto virtual, así se creó el Centro Cibernético Policial (CCP), el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT PONAL), y la Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales (CiberGAula).

Centro Cibernético Policial (CCP): "Es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada de desarrollar estrategias, programas y proyectos para la ciberseguridad, ciberdefensa y la protección de la información y los datos que circulan por el ciberespacio de los habitantes en el territorio nacional, a través de la investigación criminal." (Ministerio de Defensa Nacional, Policía Nacional - Dirección General, 2015) Esta unidad policial tiene las siguientes funciones:

1) Contar con la capacidad de detección (Ciberpatrullaje 24/7 en la web), prevención, investigación, análisis, correlación, frente a crisis informática y planes de contingencia.
2) Judicialización de las amenazas que afecten la ciberseguridad en el ámbito nacional.
3) Liderar procesos investigativos de carácter nacional e internacional contra organizaciones cibercriminales que afecten ciudadanos, patrimonio, infraestructura digital, etc.
4) Administrar el Observatorio Nacional del Cibercrimen realizando análisis de tendencias, alertas tempranas, georreferenciación y focalización.
5) Generar alianzas que fortalezcan la investigación del cibercrimen cumpliendo con la Estrategia de Ciberseguridad en Colombia (Consejo Nacional de Política Económica y Social, 2016).
6) Atender incidentes cibernéticos que afecten a los ciudadanos que utilizan el ciberespacio en Colombia.

Para la ejecución de estas funciones cuenta con una estructura interna de líneas de investigación, las cuales se dividen en operativas (fraude informático, pornografía infantil, ciberterrorismo, etc.) y actividades que desestabilizan al Estado, renombre nacional y temas relacionados con la prevención ante delitos informáticos en todos sus aspectos.

Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRTPONAL): Está compuesto por tres grupos, Grupo Continuidad de la Información (GUCIN), Grupo Seguridad de la Información (GUSIN), y el Grupo Respuesta a Incidentes de Seguridad (CSIRT), son las dependencias encargadas de supervisar el desarrollo, implementación, mantenimiento, calidad, ciclo de vida, continuidad, disponibilidad, confidencialidad, integridad y la atención a incidentes informáticos que puedan o afecten las tecnologías de la información y la información en sí mismo de la Policía Nacional. Esta unidad tiene las siguientes funciones:

1) Definir metodología y controles para contar con las mejores prácticas de ciclo de vida y clasificación de la información, con el fin de conservar la memoria digital de la institución.
2) Realizar el monitoreo de herramientas de disponibilidad de red, servidores y canales de datos.
3) Realizar pruebas de calidad con el fin de verificar que el software adquirido o desarrollado no cuente con vulnerabilidades.

4) Liderar el análisis del impacto en el negocio, plan de continuidad del negocio y el plan de recuperación ante desastres.
5) Implementar, configurar, aplicar, operar y hacer seguimiento a los controles de seguridad y el Sistema de Gestión de Seguridad en la Policía Nacional.
6) Asesorar, adquirir y administrar los proyectos tecnológicos relacionados con seguridad de la información.
7) Detectar, reportar y solucionar, vulnerabilidades y amenazas a incidentes informáticos que afecten la disponibilidad, confidencialidad e integridad de la plataforma de la Policía Nacional.
8) Realizar la difusión, concientización y prevención de las políticas de seguridad de la información.
9) Apoyar y dar respuesta a los incidentes de seguridad de la información que se presenten en la institución.
10) Realizar acuerdos de colaboración y convenios con diferentes organismos nacionales e internacionales, que permita construir una red mundial de apoyo en ciberseguridad.
11) Implementar y hacer seguimiento a la "Estrategia Nacional para la protección del Ciberespacio" (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016), a fin de contribuir a la sensibilización del ciberciudadano sobre la importancia de la seguridad de la información.

Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales (CIBERGAULA): actualmente hace parte de la estructura orgánica de la Dirección de Antisecuestro y Antiextorsión Este grupo tiene como función apoyar investigaciones de secuestro y extorsión donde se hayan empleado medios tecnológicos o se utilice el ciberespacio como canal de comunicación, además realizar el seguimiento a flagelos de extorsión a través de medios tecnológicos (correos electrónicos, redes sociales, mensajería instantánea etc.).

Capítulo V: etapa de Prevención: herramientas aplicadas por la Policía Nacional para la prevención de fugas de datos, control de acceso y seguridad en la red.

5.1 Control de acceso y gestión de servicios TIC.

Refiriendo al control ejercido por la unidad de investigación dentro y fuera de las instalaciones, acorde con la apreciación del jefe del grupo del Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional, la entidad está certificada con la norma internacional, emitida por la Organización Internacional de Normalización (ISO) 27001, que es el sistema de gestión de seguridad a la información, el cual tiene unos dominios y unos controles. Uno de esos dominios refiere específicamente al control en usuarios y acceso a redes, el cual se aplica con rigurosidad, para el caso se tiene un usuario empresarial, todas las personas desde que ingresan a la Policía tienen un usuario y de acuerdo con su misionalidad se le asignan ciertos roles, entonces, si él funcionario trabaja en el CSIRT tiene unos roles, si trabaja con policía judicial tiene otros roles, y a si a lo largo de toda la entidad. Adicionalmente se tienen controles como antivirus, lectores biométricos, usuarios de dominio, políticas de dominio, etc.; realmente el control es como la columna vertebral del sistema acceso y seguridad de la información y es lo que evita que en la mayoría de los casos se fugue dicha información.

En contexto el jefe del Centro Cibernético Policial asiente que por protocolo de seguridad de la información no se trabaja con civiles, porque de una u otra manera los procesos adelantado en la unidad son procesos judiciales o en su defecto verificaciones u órdenes de trabajo de inteligencia que requieren confidencialidad y cuidado, hasta este año se realiza un primer acercamiento con el sector gobierno, con el CSIRT gobierno, en donde se ha tenido un trabajo conjunto en seguridad de la información para acceso a entidades públicas y manejo de información.

Finalmente, el jefe del Ciber-Gaula considera que el control de acceso a la unidad de dirección antisecuestro y antiextorsión se realiza a través del seguimiento a visitantes, quienes tienen que diligenciar formatos de confidencialidad y de ser necesario realizar una identificación plena a través de lectores biométricos, con videocámaras y con registro del sistema de información como el Sistema de Información para el control de visitantes (sicovi).

5.2 Identificación y prevención de ataques de hackers en las redes.

En lo que concerniente a los ataques realizados a través del ciberespacio jefe del Equipo de Respuesta a Incidentes de Información de la Policía Nacional, asiente que esta se evita inicialmente aplicando todos controles del sistema de gestión y seguridad de la información, pero hay unos controles puntuales que se llama seguridad perimetral. Los ataques pueden ser externos o internos, para lo cual se tienen plataformas de seguridad que son herramientas para contrarrestar denegaciones de servicio, Firewall, balanceadores, antivirus, control de aplicaciones; todo esto buscando evitar que algún ciudadano tome acceso remoto o sin control de alguna máquina y pueda acceder al sistema. Adicionalmente, a nivel interno también se tienen controles, que evita la publicación de cierta información que esta categorizada como confidencial, secreta o que tiene algún nivel de clasificación, toda esa información se correlaciona en el sistema de correlación de eventos, el cual informa ciertos patrones que no están permitidos en la red, como intentos de descifrar contraseñas, escaneos dentro de la red, pantallazos no permitidos, entre otras políticas que encaminadas a prevenir y anticipar cualquier tipo de intento de acceso abusivo a la red.

El jefe del Centro Cibernético Policial, entre tanto ratifica que la entidad utiliza un método científico para prevenir y repeler ataques, iniciando con investigaciones de tipo inductivo con base en la ocurrencia de un delito donde se vea vulnerado el derecho en la red o ciber espacio; este tipo de investigaciones se inician a partir de la gestión y administración de los registros, de los logs que permiten hacer una ingeniería inversa para identificar puntos de compromiso, estos puntos de compromiso llevan a verificar que personas alrededor se mueve a través de las redes y con quienes están vinculados, ya sea mediante un uso de un software maliciosos, filtro de información, ciber engaño o cualquier otro tipo de vector de ataque. Cuando se encuentra las direcciones IP se hace búsqueda en base de datos, posteriormente allanamientos, registros y cruce de información con diferentes bases de datos nacionales e internacionales, a través de protocolos que permitan entender, correlacionar, revelar y conocer la finalidad del ciberataque.

De otro lado, el Jefe de la Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales (Ciber-Gaula) considera que la prevención en la unidad se realiza a través de dos frentes; el primer frente, se relaciona con la adquisición de herramientas tecnológicas, las cuales son manejadas por la unidad de telemática, dichas herramientas permiten hacer un rastreo de virus, hardware, programas maliciosos, entre otros elementos informáticos que pueden atentar contra la seguridad; un segundo frente, refiere al talento humano, frente a la concientización y aplicación de controles, de nada sirve contar con las mejores herramientas, si los controles no son aplicados.

5.3 Preparación de la policía para responder un ataque cibernético en Colombia.

Refiriendo a la capacidad de respuesta de la entidad policial frente a un ataque cibernético el Equipo de Respuestas a Incidentes Cibernéticos, considera que se cuenta con equipos y sistemas avanzados para prevenir que se dañe o se pierda información, sin embargo, no se puede asegurar una preparación en un 100%, pero se pude decir que el nivel de control y prevención es aceptable y está acorde con las organizaciones de América Latina.

Sin embargo, a pesar de contarse con recursos físicos, tecnológicos y humanos importantes que buscan salvaguardar la información de la institución de ataques físicos y cibernéticos, el jefe de Ciber-Gaula de la unidad es consiente que se tienen muchas falencias todavía y debido a la agilidad en el cambio tecnológico no se puede asegurar 100% que la institución esté preparada para un ataque cibernético. Además, la prestación de servicios públicos online por parte de la entidad genera un escenario de vulnerabilidad, por lo cual se ha visto la necesidad de solicitar al CSIRT algunas pruebas de ethical hacking.

5.4 Herramientas dispuestas por la Policía Nacional para prevención de problemas de Ciberseguridad.

Además de la información suministrada por los funcionarios implicados en los procesos se pudo identificar herramientas de prevención en la página oficial o CAI virtual de la policía

(**https://caivirtual.policia.gov.co/**) se relacionan directamente con mecanismos mediante los cuales no solo se busca que los investigadores puedan evitar o precaver situaciones de ataques de ciberdelincuentes, sino también ofrecer a la comunidad un cumulo de información relevante, que le permite identificar amenazas y tener en cuenta recomendaciones que pueden minimizar el riesgo en el uso de la internet. Dentro de estas herramientas se tienen:

Mural del Cibercrimen: en este mural virtual se encuentra las publicaciones sobre las diferentes modalidades empleadas por los ciber-delincuentes. Específicamente se tiene las diferentes y más comunes modalidades de estafa y engaño en el Ciberespacio como: phishing, skimming, estafa, carta nigeriana, malware, smishing.

Mapa de Ciberincidentes: muestra un mapa, el cual permite hacer una visualización en tiempo real de los delitos que se han desarrollado y los rankings de Ciberdelitos en cada uno de los departamentos.

Recomendaciones en Ciberseguridad: para el caso la Policía Nacional ofrece recomendaciones a través de boletines, guías, informes e infografías sobre ciberseguridad. Las cuales le permiten al ciudadano conocer los cibercrímenes y delitos informáticos más comunes, de tal manera que se esté al tanto de hechos en el ciberespacio y se evite caer en las trampas de los ciberdelincuentes.

La prevención referente al cuidado y acatamiento de recomendaciones que deben tener los ciudadanos al momento de acceder a portales virtuales, sobre todo cuando se trata de entregar información o hacer transacciones financieras; es uno de los elementos de gestión en ciberseguridad que la Policía afianza, profundiza y promociona con frecuencia desde el CAI virtual, el cual pone a disposición de la ciudadanía, con el fin de salvaguardarlos del cibercrimen y los ciberdelincuentes.

Capítulo VI: etapa de detección: gestión de vulnerabilidades y monitoreo continúo utilizadas por la Policía Nacional

La Policía Nacional en el área de investigación y ciberseguridad desarrolla procesos, procedimientos para conseguir los objetivos en materia de Ciberseguridad, dentro de un contexto administrativo que implica una serie de acciones o trámites conjuntos integrados que llevan a minimizar la vulnerabilidad de los sistemas de información y realización de un monitoreo continuo. Estas formas de gestión se evidenciaron en la entrevista realizada al jefe del Equipo de Respuestas a Incidentes Informáticos de la Policía Nacional, jefe de la Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales CiberGaula y jefe del Centro Cibernético Policial.

6.1 Proceso de monitoreo continuo de las redes

Refiriendo, el proceso como se realiza el monitoreo continuo el jefe del Grupo del Equipo de respuesta a Incidentes Informáticos de la Policía Nacional, asiente que hay un proceso de análisis de vulnerabilidades antes que la información sea publicada, al igual que se les realiza pruebas de vulnerabilidad a las plataformas, si las plataformas tienen vulnerabilidades no salen a producción hasta que se hayan subsanado, dichas pruebas pueden ser estáticas, dinámicas, al código fuente o al ambiente web, este monitoreo se hace antes de salir a publicación o producción, pero semestralmente se realizan pruebas de monitoreo a todas las plataformas en búsqueda de servidores sin actualizar, puertas abiertas, malos procedimientos de desarrollo, deficiencias de estilo. Además, se cuenta con el Agente de Windows Update que a través de Windows Server Update Services (WSUS) envía actualizaciones de todos los sistemas Windows de la Policía, lo que garantiza mantener actualizadas las últimas versiones de seguridad y el sistema operativo de cada uno de los equipos.

Así mismo, el parcheo que realiza el Equipo de respuesta a Incidentes informáticos, se realizan manual, debido que, al realizarlo automático, algunos parches dañan el Sistema Operativo, además de volver indisponible el sitio web; de esta forma el proceso consiste en revisar o generar un ambiente de pruebas para verificar el funcionamiento y las actualizaciones, una vez validado se pone

el parche. En los equipos que no cuentan o no se les puede actualizar, se busca protegerlos con los perímetros de seguridad, con el firewall y tratar de tener el mínimo acceso a esos equipos.

Acorde con su función el jefe del Centro Cibernético Policial hace referencia a un monitoreo continuo que recae sobre el tráfico malicioso y la correlación de ips con diferentes plataformas a nivel Internacional, esto permite correlacionar ips maliciosas o malware; cuando se identifican esas ips que están vinculadas con diferentes aplicaciones o servicios, lo que se hace es un bloqueo temporal de esas ips, a través de la Policía Nacional, del CSIRT y de diferentes portales web del gobierno.

6.2 Medidas tomadas para minimizar los problemas de vulnerabilidad que se registran con la aparición de nuevos programas maliciosos.

Al respecto al Equipo de respuestas a incidentes informáticos de la Policía Nacional deja claro que está a la vanguardia en temas de ciberseguridad, utilizando herramientas de gestión para búsqueda de vulnerabilidades y monitoreo continúo que garanticen que ante la salida de una nueva amenaza se cuente con una forma de combatirlo, por eso se mantienen vigentes los contratos de antivirus, de sistemas de prevención de intrusos y de firewall, debido a que esto minimiza la presencia de amenaza; en tanto que las tácticas de gestión de la vulnerabilidades y monitoreo continúo permiten asumir condiciones de seguridad que se tienen físicamente y aplicarlas al mundo virtual y que se fundamentan en la aplicación de protocolos, es decir, así como se coloca seguro a la puerta cuando se sale de la casa y se le dice a los hijos o familiares que no hablen con extraños, de la misma manera se debe tratar el mundo virtual; no hablarle a personas que no se conocen en las redes sociales, no dejar puertas abiertas que puedan servir de entrada para quebrantar la privacidad y seguridad de información y datos que se manejan en la red.

Finalmente, el jefe del Centro Cibernético Policial asiente que para minimizar los problemas de vulnerabilidad se recurre a la prevención y anticipación, cuando se recibe algún tipo de alerta por parte otra dependencia, ya sea de la Organización Internacional de Policía Criminal (INTERPOL), Oficina Europea de Policía (EUROPOL) o cualquier otra agencia a nivel Internacional, inmediatamente se genera un producto (alerta) para lograr la contención de este tipo de ataque y socializar la información en el CAÍ virtual. Así mismo, se cuenta con expertos que

permiten enviar ese tipo de alertas, que implican mensajes de advertencia a las empresas, para que estas a su vez hagan el despliegue y se generen las alertas ante este tipo de amenaza. Es bueno ratificar que el Cibercrimen es un delito global que permite estar en tiempo real, no solamente haciendo actividad de verificación, sino recibiendo información de otras agencias que ya han verificado, así de manera bilateral se generan las acciones preventivas y anticipadas que sean necesarias y no esperar a que ocurra un delito y salir a enfrentar un problema que puede tener múltiples y graves consecuencias.

6.3 Herramienta dispuesta por la Policía Nacional para gestión de vulnerabilidades y monitoreo continuo.

Además de las estrategias tácticas evidenciadas en las entrevistas la página oficial cuenta con una herramienta a saber:

Verificación de archivos y URLs sospechosos: la Policía ofrece el servicio de análisis URL en archivos, con el fin de saber si son maliciosas, así el usuario recibe boletines y noticias de actualidad en ciberseguridad. Es un servicio gratuito que analiza archivos y URLs sospechosas facilitando la rápida detección de virus, gusanos y/o troyanos. Para que pueda analizar archivos y URL sospechosas deberá previamente haber realizado la suscripción en el enlace que se indica a continuación: https://cc-csirt.policia.gov.co/Sandbox

Para la Policía Nacional el enfoque principal en materia de ciberseguridad es la prevención, aunque existen otros mecanismos ofrecidos por la entidad a la comunidad que buscan la detección de amenazas en el ciberespacio, enfocados principalmente al servicio análisis de archivos y los boletines permanentes sobre noticias y acontecimientos, que ocurren no sólo en Colombia, sino a nivel mundial, relacionadas con acciones delincuenciales fraguadas en el ciberespacio; este tipo de medidas o estrategias buscan debilitar el alcance de los delincuentes cuando ya han tenido acceso a sus víctimas, sin embargo, no siempre se obtiene los resultados deseados, por lo cual es importante que los funcionarios tengan conciencia de la importancia que tiene la precaución en el uso de portales virtuales y el manejo de la información que se encuentra en el ciberespacio.

Capítulo VII: etapa de respuesta: Mecanismos de respuesta de la Policía Nacional en casos que impliquen recuperación de información y aplicación de contramedidas.

De acuerdo con la entrevista realizada al jefe del Equipo de Respuestas a Incidentes Informáticos de la Policía Nacional, Jefe de la Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales CiberGAula y jefe del Centro Cibernético Policial, la Policía Nacional de Colombia incluye un conjunto de elementos integrados entre sí con el fin defenderse de las amenazas, o dar respuesta aquellas hechos o circunstancias que afectan la seguridad de la información en el ciberespacio.

7.1 Medidas tomadas ante una fuga de datos.

Al presentarse una fuga de información se debe investigar el origen para establecer la intención, por ejemplo, si una fuga implica funcionarios de Policía Nacional, eso tiene un proceso de atención a incidentes, el incidente es algo que afecta confidencialidad, integridad o disponibilidad de la información. Una vez se fugue la información, el equipo de respuesta a incidente entra a hacer toda una investigación y diligencia todo un proceso haciendo un rastrero de los acontecimientos paso a paso, estableciendo causas y consecuencias; así las repercusiones dependen del incidente y pueden ser legales o disciplinarias, pero dependiendo de la gravedad puede alcanzar un nivel penal.

7.2 Sistemas de recuperación de información.

Refiriendo a los sistemas de recuperación que se utilizan cuando se presenta una aparición de un programa malicioso o se genera una fuga de datos en la red se utiliza el software Forensic Toolkit (FTK) y Encase cuya función principal es la recuperación de la información; además se capacita a los funcionarios para evitar que reincidas de información por descuidos, permitiéndose máximo tres reincidencias en el año.

En tanto si la fuga se debe a un descuido de la entidad o por un acceso remoto que puede ser la apertura de puertos a través de un troyano, se identifica cual fue el vector infección o ataque, identificando el código y el servidor a que se está apuntando, así los colombianos pueden subir los archivos para que

esta información sea desencriptada. Afortunadamente la Policía Nacional, tiene la capacidad para hacer backup y mantener controlando el tráfico de la información, por eso es importante los buenos hábitos y las buenas prácticas de seguridad en el manejo de la información ya que es un derrotero para los ciberdelincuentes.

Frente a la aparición de programas maliciosos o fuga de datos en la red, se acude a las herramientas forenses de recuperación de información, sin embargo, se tienen limitaciones en relación a software malicioso o secuestro de información a nivel mundial; la Policía Nacional de Colombia no ha sido afectada por software malicioso de gran alcance a nivel mundial, pero si se tiene conocimiento de que es muy difícil poder recuperar la información en caso de que se cifre. La Oficina Europea de Policía (Europol) ha creado herramientas como la página "no más ransomware", con el fin de, identificar o poder descifrar ese tipo de archivos, pero lastimosamente los ciberdelincuentes evolucionan y es muy complejo poder estar a la vanguardia y así lograr la recuperación de la información hurtada o secuestrada.

7.3 Herramientas de ataque.

Concerniente a las herramientas que se usan para afrontar los ataques cibernéticos que se puedan presentar en la red WAN, se cuenta con firewall que se dedican a verificar que consultan las personas en cada sitio web, además el sistema de gestión de la información cuenta con sistemas de control individualizados para cada unidad. De la misma manera se puede recurrir a sistemas de hardware, con enfoque en los colaboradores con cultura de responsabilidad y prácticas de seguridad; esto se debe a que acorde con los casos conocidos la principal vulnerabilidad se presenta en los mismos funcionarios; si el funcionario tiene la autonomía y no maneja responsabilidad y ética profesional es factible perder una descarga o una actualización y a partir de ahí se pierde el control de la información, es por ello que el enfoque principal es la cultura y la prevención.

7.4 Papel de la Policía Nacional en la prevención, detección y respuesta a los problemas de ciberseguridad.

La Policía Nacional como entidad encargada de la seguridad de los colombianos debe velar no solo en su seguridad física sino también en la virtual, de esta forma la Policía Nacional tiene un papel relevante en la prevención, detección y respuesta a los problemas de ciberseguridad que afectan la comunidad y entidades colombianas. Es así, como el jefe del Equipo de Respuestas a Incidentes Informáticos, es consiente que la Policía Nacional tiene la obligación de prevenir, atender e investigar los incidentes que afecten la ciberseguridad de los colombianos, estos deberes están expresos en el documento CONPES 3701 de ciberseguridad y ciberdefensa y CONPES 3854 de seguridad digital, en los cuales se definen responsabilidades puntuales a la Policía, buscando fortalecer las capacidades del Estado y minimizar el impacto de los ataques, ya que los delitos han migrado del mundo físico al mundo digital. Entre tanto se debe fomentar una cultura ciudadana enfocada al buen uso de las tecnologías, convertidas en un agente moderador, que permita combatir los delitos cibernéticos y preservar la integridad de las personas.

7.5 Herramientas dispuestas por la Policía Nacional para prevención, detección y respuesta a los problemas de Ciberseguridad.

La Policía Nacional dispone de servicios enfocados a la comunidad para que puedan denunciar cualquier tipo de ciberdelitos. Adicionalmente se cuenta con la cámara colombiana del CSIRT que es una herramienta o sitio web que permite a las personas analizar en tiempo real archivos sospechosos, estas herramientas se difunden a través de redes sociales Twitter, Facebook, YouTube, y demás medios que tiene la Policía para alertar y mantener informada a la comunidad.

Reporte de delitos informáticos CAI virtual: Para el caso de los delitos informáticos la Policía Nacional cuenta con una línea virtual o un CAI virtual, en el cual los ciudadanos pueden llevar a cabo la denuncia de situaciones o hechos relacionados con la vulneración del ciberespacio y la ciberseguridad.

Para la Policía Nacional la reacción o respuesta a casos delictivos fraguados en el ciberespacio es el último de los recursos, se tiene conciencia de que las medidas de prevención y detección no siempre logran los objetivos propuestos, debido al desconocimiento, falta de información y poca formación de la comunidad en el uso responsable de las TIC, que se suma a la falta de personal en los grupos de inteligencia, las deficiencias en la capacitación de los uniformados en materia de ciberseguridad y el crecimiento vertiginoso y exponencial de la tecnología que cada día permite nuevas formas o mecanismos que son usados por los delincuentes para acceder a información de los colombianos, con miras al desarrollo de actividades delictivas.

Bajo este contexto, el componente de *respuesta* de la gestión en ciberseguridad de la Policía Nacional, se enfoca principalmente salvaguardar los derechos de los colombianos. La identificación es un proceso requerido para estar al tanto de las amenazas cibernéticas presentes en ese espacio, por lo cual se usa un observatorio del cibercrimen que mediante boletines, guías y cartillas publican casos de ciber-operativos, que son la base para identificar acciones o amenazas latentes de acuerdo a los modus operandi de los ciberdelincuentes.

Capitulo VIII: análisis de resultados y propuesta

8.1 Análisis de resultados

Según la información obtenida a través de las encuestas, las entrevistas y el análisis de documentos y paginas oficiales de la Policía Nacional, el proceso de gestión de la ciberseguridad se realiza de forma integrada a través de tres unidades básica que son el Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional, el CiberGaula y el Centro Cibernético Policial, a pesar que estas unidades tienen funciones especiales las acciones y procesos que se realizan apuntan a proteger a la entidad y los ciudadanos en el ciberespacio.

La etapa de prevención en materia de Ciberseguridad en todas las dependencias de la Policía Nacional implicadas en el tema consiste básicamente en la adopción de la ISO 27001, la aplicación de protocolos de seguridad, la utilización de equipos tecnológicos y software de avanzada para la detección de amenazas, la capacitación del personal y el diseño y socialización de programas de prevención enfocados a la comunidad., como se muestra en la tabla 4.

Tabla 4. Síntesis de resultados de la gestión en ciberseguridad: etapa de Prevención. Fuente: Elaboración propia.

	Gestión del Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional	**Gestión del Centro Cibernético Policial**	**Gestión del CiberGaula**
Control de acceso y gestión de servicios TIC.	Aplicación de ISO 27000 sistema de gestión de seguridad a la información. El cual tiene unos dominios y unos controles. Adicionalmente se tienen controles como antivirus, lectores biométricos, usuarios de dominio, políticas de dominio, etc	Se aplica protocolo de seguridad de la información	Se realiza a través del diligenciamiento formatos de confidencialidad y de ser necesario realizar una identificación plena a través de lectores biométricos, con videocámaras y con registro del sistema de información como el sicovi.

	Gestión del Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional	Gestión del Centro Cibernético Policial	Gestión del Ciber-Gaula
Preparación de la policía para atender un ataque cibernético en Colombia	Se cuenta con equipos y sistemas avanzados para prevenir que se dañe, fugue o se pierda información, sin embargo, no se puede asegurar una preparación en un 100%.	Se cuenta recursos físicos, tecnológicos y humanos importantes que buscan salvaguardar la información de la institución de ataques físicos y cibernéticos	Se cuenta con herramientas tecnológicas avanzadas, software y personal preparados.
Identificación y prevención de ataques en las redes.	Mediante controles del sistema de gestión y seguridad de la información, y controles de seguridad perimetral. Mediante plataformas de seguridad externas que son herramientas para mitigar denegaciones de servicio, Firewall de aplicaciones, Firewall de etapa tres, balanceadores, antivirus, control de aplicaciones.	Aplicación del método científico para prevenir y repeler ataques, iniciando con investigaciones de tipo inductivo; este tipo de investigaciones se inician a partir de la gestión y administración de los registros, de los log que permiten hacer una ingeniería inversa para identificar puntos de compromiso	Se realiza a través de dos frentes; el primer frente, se relaciona con la adquisición de herramientas tecnológicas novedosas, dichas herramientas permiten hacer un rastreo de virus, hardware, programas maliciosos, entre otros elementos informáticos que pueden atentar contra la seguridad; un segundo frente, refiere a la gestión del talento humano.

Fuente: Elaboración propia.

La etapa de detección mediante la cual la Policía Nacional descubre y hace seguimiento a programas maliciosos o ciberdelincuentes que asaltan el ciberespacio dentro de un contexto de la gestión de la ciberseguridad se fundamenta básicamente en el análisis de vulnerabilidades, la revisión, el mantenimiento de sistemas de control, el monitoreo continuo sobre el tráfico malicioso, la aplicación de controles adoptados por la institución enfocados a salvaguardar el ciberespacio. Ver tabla 5.

Tabla 5. Síntesis de resultados de la gestión en ciberseguridad: etapa de detección

	Gestión del Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional	Gestión del Centro Cibernético Policial	Gestión del Ciber-Gaula
Proceso de monitoreo continuo de las redes	Hay un proceso de análisis de vulnerabilidades cada vez que la información sale a producción (alguna unidad hace uso de la información). Semestralmente se le hacen prueba a toda la plataforma en búsqueda de servidores sin parchar, cuartos abiertos que no tienen que estarlo, malos procedimientos de desarrollo, deficiencias de estilo.	Revisión periódica de sistemas de control, programas y softwares usados para proteger la unidad.	Monitoreo continuo que recae sobre el tráfico malicioso y la correlación de esas IPs con diferentes plataformas a nivel Internacional, esto me permite llegar a contener pronto IPs maliciosas que hacen parte de un malware.
Medidas tomadas para minimizar los problemas de vulnerabilidad que se registran con la aparición de nuevos programas maliciosos y hackers.	La Policía Nacional está a la vanguardia en temas de ciberseguridad, utilizando herramientas de gestión de vulnerabilidades y monitoreo continúo que garanticen que ante la salida de una nueva amenaza se cuente con una forma de combatirlo	Se aplican herramientas de gestión de vulnerabilidades y monitoreo continúo para asumir las condiciones de seguridad que se tienen físicamente y aplicarlas al mundo virtual y fundamentan en la aplicación de protocolos	Se recurre a la prevención y anticipación, cuando se recibe algún tipo de alerta por parte otra dependencia, ya sea INTERPOL, EUROPOL o cualquier otra agencia a nivel Internacional, inmediatamente se genera alerta para lograr la contención de este tipo de ataque y socializar la información en el caí virtual.

Fuente: Elaboración propia.

Mencionando la etapa de respuesta que tiene la Policía Nacional realiza en el contexto de la gestión de ciberseguridad, esta se lleva a cabo a través de la investigación del origen de los programas maliciosos y ataques cibernéticos, para posteriormente desplegar acciones de recuperación de la información y hacer un seguimiento a las fuentes maliciosas que consecuentemente lleve a la identificación de los implicados para aplicar las normas civiles y penales a las que haya lugar.

En términos generales se considera que la gestión policial en materia de ciberseguridad es constante y actualizada en la medida que se cuenta con apoyo, conocimientos y herramientas tecnológicas sofisticadas, sin embargo, no se puede decir que la entidad este 100% capacitada para combatir eficientemente un ataque Cibernético.

Tabla 6. Síntesis de resultados de la gestión en ciberseguridad: etapa de respuesta. Fuente: Elaboración propia.

	Gestión del Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional	**Gestión del Centro Cibernético Policial**	**Gestión del Ciber-Gaula**
Medidas tomadas ante una fuga de datos	Se debe investigar el origen para establecer la intención, eso tiene un proceso de atención a incidentes. Una vez se materialice los hechos, el equipo de respuesta a incidente entra a hacer toda una investigación y diligencia todo un proceso haciendo un rastrero de los acontecimientos paso a paso, estableciendo casusas y consecuencias.	Se despliega un protocolo de recuperación de la información, el cual implica todo el centro. El protocolo busca causa y efectos, para el pertinente rastreo.	Se tendría sanciones en relación con la ley de protección de datos, esta sanción recae en el caso de que fuese robada y divulgada la información de funcionarios o de terceros. De igual forma, la misma institución policial puede verse abocado a sanciones por parte de estas entidades afectadas. Refiriendo la Policía Nacional se esto conllevaría tanto a sanciones disciplinarias internas.
Sistemas de recuperación de información	cuando hay pérdidas de documentos y/o información, se utiliza el software FTK y Encase cuya función principal es la recuperación de la información; además del software se tiene capacitaciones para evitar que los funcionarios reincidan en pérdidas por descuidos	Se identifica cual fue el vector infección o ataque, esto permite entender realmente lo ocurrido, identificar el código y el servidor a que se está apuntando, si ante una fuga de información o un secuestro de datos existe un portal que se llama "nomoreransomware.org" así los colombianos pueden subir los archivos para que esta información sea desencriptada.	Cuando se presenta un hackeo, se evidencia la aparición de un programa malicioso o se genera fuga de datos en la red, se acude a las herramientas forenses de recuperación de la información, sin embargo, se tienen limitaciones en relación a software malicioso o secuestro de información a nivel mundial

	Gestión del Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional	Gestión del Centro Cibernético Policial	Gestión del Ciber-Gaula
Contramedidas de ataque	Si hay un ataque o se sustrae información confidencial se cuenta con Web Application Firewall - AWS WAF que es un firewall para aplicaciones web, el cual ayuda a proteger aplicaciones web de ataques web, que podrían afectar la disponibilidad de la aplicación, colocar en riesgo la seguridad o consumir recursos, además el sistema de gestión de la información ISO 27000 cuenta con sistemas de control individualizados para cada unidad.	Una vez recuperada la información se busca la fuente para aplicar los correctivos y recuperar el sistema.	El principal enfoque son los colaboradores, una cultura de responsabilidad y prácticas de seguridad
Papel de la Policía Nacional en la prevención, detección y respuesta a los problemas de ciberseguridad.	La Policía Nacional tiene una obligación y es encargada de la prevención, atención e investigación de incidentes que afecten la Ciberseguridad de los colombianos. , estos deberes están expresos en el CONPES 3701 de Ciberseguridad y Ciberdefensa y CONPES 3854 de seguridad digital, en los cuales se definen responsabilidades puntuales a la Policía	Ya no se puede hablar por separado de un mundo virtual y un mundo físico, pues a la luz de la realidad no existe ninguna diferencia, bajo este contexto la Policía no solo debe fomentar una cultura ciudadana enfocada al buen uso de las tecnologías, sino que se convierte en un agente represor para combatir los delitos Cibernéticos.	El papel de la Policía Nacional en la prevención, detección y respuesta a los problemas de Ciberseguridad que afectan la comunidad y la entidad colombiana es preservar la integridad de las personas, una tarea complicada si se tiene en cuenta que antes los delitos se presentaban en el plano físico y ahora se trasladaron al Ciberespacio

Fuente: Elaboración propia.

Según Todas la acciones, operaciones y quehaceres de los funcionarios enfocados a gestión de la ciberseguridad relacionada con la prevención, detección y capacidad de respuesta a casos delictivos que involucran acciones en el ciberespacio, están integrados a una Estrategia Nacional de Ciberseguridad (ENCS), que es un instrumento para mejorar la seguridad en el uso de las tecnologías y la continuidad de los servicios nacionales de información, persiguiendo los siguientes objetivos.

- Alinear acciones para trabajar de manera armoniosa.
- Coordinar la cooperación de los sectores público y privado.
- Transmitir directivas, responsabilidades y establecer relaciones entre todas las partes involucradas.

De esta forma y de acuerdos con los objetivos propuestos por la Estrategia Nacional de Ciberseguridad, así como las afirmaciones e información recolectada de las Unidades de Gestión del Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional, Gestión del Centro Cibernético Policial y Gestión del CiberGAula, se puede indicar que la institución adelanta un trabajo integro, y continúo, el cual busca todas las entidades qué se benefician y les competen el desarrollo y cuidado del ciberespacio. En otras palabras, tomando como referente el he hecho de que en las últimas décadas las nuevas tecnologías y los servicios electrónicos han aumentado y generado una nueva forma de vida que se fragua en el ciberespacio, donde de las comunicaciones, el comercio electrónico, los servicios financieros, los servicios de emergencia y los servicios públicos fluyen a través de estas infraestructuras, es así como la institución busca de salvaguardar la integridad de los navegantes, realización procesos permanentes y continuos, que además integran organizaciones privadas como entidades bancarias, proveedores de servicios electrónicos, pequeñas y medianas empresas (PYMEs), organizaciones de investigación y desarrollo, universidades, ciudadanos y la población en general.

Es importante resaltar que la Estrategia Nacional de Ciberseguridad que integra a la Policía Nacional infiere un cumulo de estrategias o políticas de ciberseguridad, para afrontar los riesgos presente en el ciberespacio relacionadas con: a) Protección de la infraestructura tecnológica, económica, de seguridad nacional y bienestar social; b) un enfoque de la estrategia/política hacia la concientización, el conocimiento del ciberespacio, la educación en ciberseguridad y las capacidades cibernéticas militares para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética

que afecte la soberanía nacional; c) la participación del sector público en la estrategia/política bajo un enfoque de liderazgo consiente de los desafíos del ciberespacio requieren y conocedor del marco Jurídico en el área de ciberseguridad que trata los diferentes tipos de delitos tanto a nivel nacional como internacional; d) Participación del sector privado en la estrategia/política incluyendo a sectores claves como energía, transportes, entidades financieras, bolsas de valores, proveedores de servicios de internet, entre otros , y e) Cooperación internacional trabajando en concordancia con otros países a través de la elaboración y adopción de estándares globales, la expansión de la capacidad del sistema jurídico internacional y el desarrollo y la promoción de las mejores prácticas para generar sistemas de alerta y de respuesta a los ciberataques. (Policía Nacional, 2018)

Acorde con los resultados de la encuesta aplicada, y las entrevistas realizadas al Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional, Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales y el Centro Cibernético Policial, se evidencian fortalezas y debilidades dentro de la institución, así como oportunidades y amenazas que se encuentran en el entorno los cuales se muestran en el siguiente cuadro:

Tabla 7. DOFA de la gestión de la policía nacional en ciberseguridad

	Fortalezas	**Debilidades**
Ambiente interno de la policía nacional	• Personal profesional y técnico con amplio conocimiento en las TIC y ciberseguridad. • Selección de personal con conocimientos previos en ciberseguridad. • Conocimientos e información sobre actividades delictivas en el ciberespacio. • Capacidad de reacción de los equipos o grupos de investigación en ciberseguridad. • Trabajo orientado a la consecución de resultados. • Conocimiento de procesos, procedimientos y protocolos. • Integración de las distintas unidades policiales que combaten el cibercrimen en las diferentes formas.	• Falta de personal en las unidades especializadas en el cibercrimen • Capacitaciones enfocadas a personal que labora para estos grupos. Algunos cursos brindados a los funcionarios se hacen una única vez debido a la necesidad de contratar personal especializado. • poco conocimiento en ciberseguridad de los Policías en general. • Barreras de conocimiento al momento de afrontar incidentes de ciberseguridad.

	• Infraestructura tecnológica a la vanguardia. • Constantes capacitaciones en redes, ethical hacking, entre otros temas de Ciberseguridad. • Trabajo de ciberseguridad sincronizado con entidades gubernamentales (MINTIC), educativas, bancaria, empresas prestadoras de servicios de teleco-municiones, entre toras organizaciones que manejan grandes volúmenes de información de los colombianos. • Existencia de un CAI virtual para atender a la comunidad en el momento requerido. • Vigilancia, control y rastreo. de los de los Ciberdelitos en tiempo	
	Oportunidades	**Amenazas**
Ambiente externo	• Convenios de cooperación con entidades a nivel mundial. • Creación de novedosos programas de rastreo de elementos maliciosos en el ciberespacio.	• Crecimiento tecnológico exponencial que genera nuevos peligros en el ciberespacio. • Crecimiento de la actividad en el ciberespacio que aumenta la probabilidad de hechos delincuenciales. • Aumento de redes de Ciberdelincuencia a nivel mundial. • Falta de conciencia de la comunidad en el uso de la red para acciones sociales, comerciales, financieras, etc. • Incremento en los índices de Ciberdelincuencia en un 68,5% (hurto por medios informáticos y semejantes, violación de datos personales y acceso abusivo a un sistema informático) • Poco presupuesto asignado por las empresas en Colombia para el aseguramiento de la información y seguridad informática.

Fuente: Elaboración propia

Entendiéndose que la gestión de la ciberseguridad comprende un proceso que implica la prevención, detección y respuesta, ante delitos cibernéticos; enfocándose al contexto de la

Policía Nacional y específicamente a los funcionarios que dirigen y ejercen la función de investigadores del ciberespacio y teniendo en cuenta que la ciberseguridad debe ser un proceso que parte del ámbito interno de la institución, para el caso se considera pertinente proponer estrategias de fortalecimiento de competencias que contribuyan a la prevención del ciberdelito, que consecuentemente llevara a contar con una entidad capaz de atender oportunamente las situaciones delictivas que se fraguan en el ciberespacio.

8.2 Propuesta

Acorde con el contexto analizado se propone una estrategia para fortalecer las competencias específicas de los funcionarios de la Policía Nacional, enmarcadas en el modelo de gestión del talento humano y el manual de funciones para el personal uniformado, soportadas desde un componente primario del Equipo de respuestas a incidentes informáticos y centro cibernético policial que alineadas a la normatividad y estrategias institucionales permitirán el despliegue de capacitaciones específicas transversales, generalizadas y desarrolladas desde las escuelas de formación y capacitación para el personal con énfasis en salvaguardar y prevenir incidentes que afectan la seguridad, integridad y disponibilidad de los sistemas de información. De forma concreta, se busca crear competencias específicas y conciencia en los policías, con el fin de proteger la ejecución de acciones relacionadas con la interacción social y el ejercicio de sus actividades en el Ciberespacio. Ver figura 11.

Figura 11. Estrategia de Ciberseguridad. Fuente: Elaboración propia.

8.3 Antecedentes y bases institucionales de la propuesta

Al fortalecer la estrategia alienada desde el manual de funciones dinamizado en el modelo de gestión del Talento Humano facilita la articulación de cada uno de sus componentes y la protección de información desplegada desde el proceso del Direccionamiento del Talento Humano y de impacto para la institución, fortaleciendo así, las competencias de desempeño de los policías y disminuyendo de manera eficiente el impacto de los riesgos que genera la utilización de las herramientas tecnológicas, alineadas a las responsabilidades que estas le generan al recurso humano y que están contempladas en la Resolución 08310 del 28/12/2016 "Por la cual de expide el Manual del Sistema de Gestión de la Seguridad de la Información para la Policía Nacional".

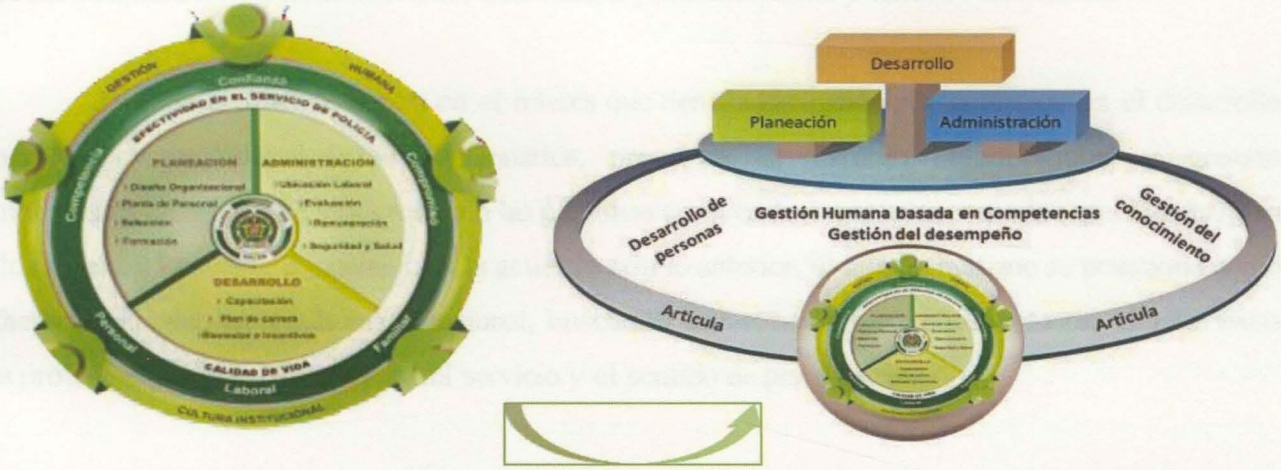


Figura 12. Modelo de Gestión del Talento Humano y Cultura Institucional. Fuente: Manual del Sistema de Gestión Integral – Resolución 03392 del 30 de julio de 2015.

Modelo de Gestión del Talento Humano y Cultura Institucional es la herramienta adoptada por la Policía Nacional para el gerenciamiento del talento humano, a través del cual se integra la capacidad de las direcciones que hacen parte del Direccionamiento del Talento Humano como proceso, en torno al desarrollo de los policías en ambientes de trabajo que favorecen la calidad de vida personal, laboral y familiar; y al mismo tiempo, la efectiva prestación del servicio de policía, reflejada en comportamientos que demuestran competencia, confianza y compromiso, como sello de la cultura institucional. El modelo articula los procesos, procedimientos y actividades a través de tres (3) componentes:

1) Planeación: en el cual se proyectan las necesidades de personal de los diferentes grupos poblacionales que existen en la institución, se realiza y orienta el diseño organizacional para la administración del talento humano, selección y formación para los futuros profesionales de policía, bajo los parámetros de la efectividad y calidad para una efectiva prestación del servicio.

2) Administración: corresponde a los procesos relacionados con el desarrollo de los trámites administrativos necesarios para mantener y formalizar el vínculo legal e institucional de los funcionarios desde su ingreso hasta la salida de la organización, entre lo que se encuentran: ubicación laboral, evaluación del desempeño, seguridad y salud en el trabajo y remuneración. Para apoyar estas actividades se cuenta con herramientas tecnológicas robustas y modernas que alojan la información de los funcionarios y permiten realizar trazabilidad para la consulta y toma de decisiones.

3) Desarrollo: se centra en el interés que tiene la institución por contribuir en el desarrollo personal y profesional de sus funcionarios, promover el cambio organizacional y generar motivación, creatividad e innovación en las personas a través de estrategias como la capacitación, plan de carrera y bienestar e incentivos. De acuerdo con lo anterior, el talento humano se posiciona como factor estratégico en la cultura institucional, buscando favorecer desempeños exitosos, el valor hacia la profesión policial, la vocación del servicio y el sentido de pertenencia.

Este modelo se ha operacionalizado al interior de la institución a través de los Comités de Gestión Humana y Cultura Institucional, con los cuales se ha permitido tener un contacto más cercano entre la Institución y sus funcionarios. Por otra parte, se ha implementado el tablero de gestión para el direccionamiento del talento humano el cual permite medir y evaluar diferentes procedimientos y actividades que impactan tanto en la administración y bienestar del personal, como en la calidad del servicio de policía.

Figura 13. Gestión humana basada en competencias. Fuente: Elaboración propia.

La administración del Talento Humano se encuentra establecida bajo un Modelo de Gestión del Talento Humano y Cultura Institucional que garantiza la trazabilidad de las competencias del personal desde el momento que realizan el proceso de selección hasta que culmina su carrera en la institución. Las competencias genéricas son definidas para dar identidad a la profesión policial por parte de las unidades que conforman el proceso del Direccionamiento del Talento Humano y validadas por la comunidad policial en general, mientras que las competencias específicas son identificadas por cada dueño de proceso en atención a la particularidad de los quehaceres.

Gestión del desempeño: La gestión del desempeño es un proceso continuo, bajo la responsabilidad de los jefes inmediatos, que involucra el acompañamiento a los subalternos en el logro de los resultados mediante la planeación, el seguimiento y la evaluación del cumplimiento de los objetivos concertados. La institución establece un sistema formal de medición que permite la toma de decisiones frente al desempeño de sus funcionarios desde lo personal y profesional, de acuerdo con los estándares establecidos. La evaluación del desempeño es insumo fundamental para ser convocados a cursos de ascenso, otorgamiento de incentivos y condecoraciones, ubicación laboral y otras asociadas a los procesos de gestión del talento humano.

Desarrollo de personas: Teniendo en cuenta la gestión del conocimiento que se realiza en la Policía Nacional, y aunado esto, a las herramientas con las que dispone el Direccionamiento del Talento Humano para la identificación de las necesidades de capacitación, la institución prevé cada año el presupuesto para otorgar dicha capacitación en dos modalidades:

Capacitaciones específicas: con el fin de generar conocimiento y experiencia en temas relacionados con la formación para el trabajo, de acuerdo con las necesidades determinadas por el cargo.

Capacitaciones transversales: considerando el desarrollo de la cultura y los temas de interés general e institucional.

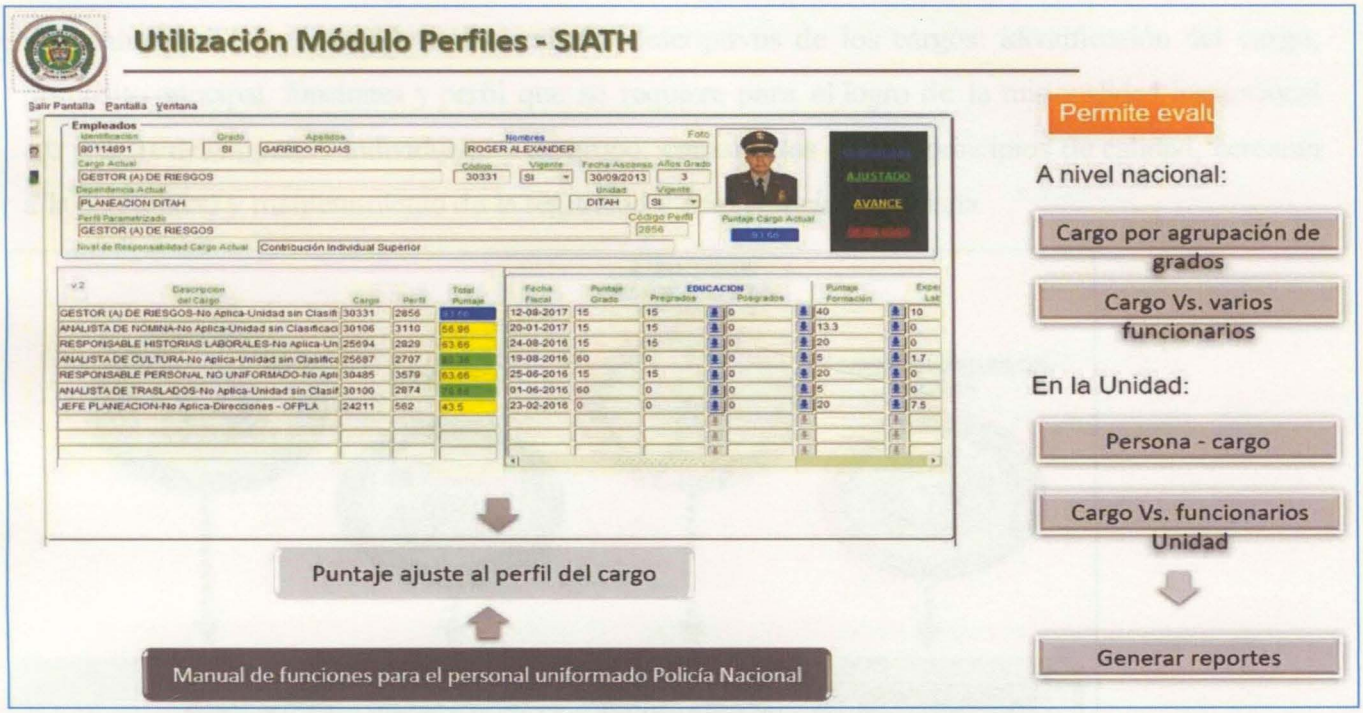
La asistencia a dichas capacitaciones debe ser prioridad de la institución y de sus miembros. De igual forma se promueve el autoaprendizaje como un mecanismo de desarrollo personal y profesional.

Los planes de carrera y de sucesión, así como la identificación de potenciales para ocupar cargos estratégicos, hacen parte de las herramientas que permiten el desarrollo de las personas en la institución.

Gestión del conocimiento: Para la Policía Nacional el conocimiento es un activo intangible fundamental asociado con la capacitación del personal, estructuración y transmisión del conocimiento; de esta forma, debe gestionarse desde la adquisición, localización, retención y administración de la información, así como desde los datos creados en la institución a partir de las experiencias individuales y colectivas. Su objetivo principal es el diseño de estrategias, procesos, estructuras y sistemas que le permitan a la organización hacer uso de lo que conoce con el apoyo de la tecnología, con el propósito de crear valor para el servicio de policía y para la comunidad en general.

- Para garantizar la gestión del conocimiento en la Institución se debe propender por:
- Una cultura orientada al conocimiento
- Infraestructura tecnológica y personas con las competencias para utilizarla

- Respaldo del mando institucional
- Reconocimiento del valor que otorga
- Contribución a una institución adaptable y sostenible
- Definir el alcance y objetivos de la gestión
- Prácticas de motivación para su movilización
- Diseño de una estructura que fundamente los depósitos de conocimiento
- Múltiples canales para la transferencia del conocimiento
- Integrar la información y conocimientos que están en la mente de las personas, plasmándolas en herramientas tecnológicas



La gestión del conocimiento es la gestión del capital intelectual en la institución, con el propósito de añadir valor al quehacer del policía, convirtiéndolo en un profesional íntegro y diferencialmente competitivo.

Figura 14. Utilización del módulo perfiles SIATH. Fuente: Sistema de información para la administración del Talento Humano - SIATH

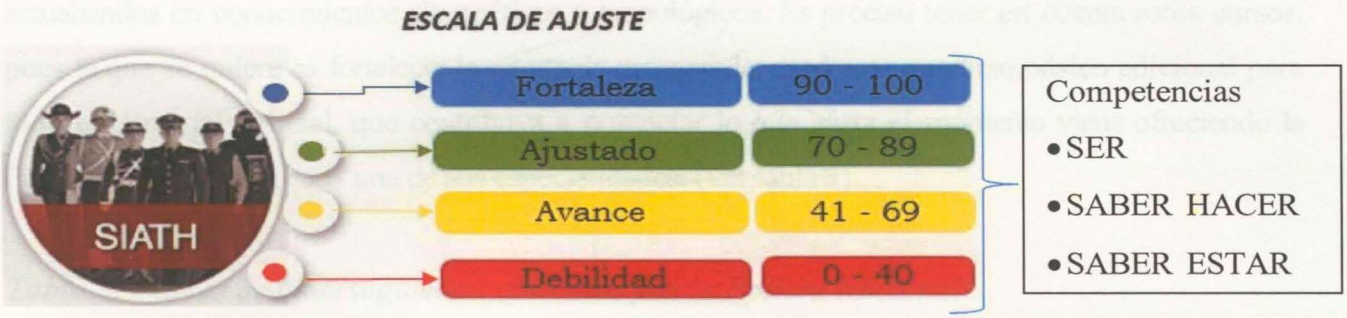


Figura 15. Escala SIATH. Fuente: Sistema de información para la administración del Talento Humano - SIATH

La metodología usada por la Policía Nacional para la evaluación del perfil del cargo a través del Módulo Perfiles de cargos del Sistema de Información para la Administración del Talento Humano (SIATH), el cual brinda elementos descriptivos de los cargos: identificación del cargo, propósito principal, funciones y perfil que se requiere para el logro de la misionalidad institucional a través de desempeños individuales y de grupo, enmarcados en los principios de calidad, cercanía a la comunidad y mantenimiento de la seguridad y convivencia ciudadana.

Figura 16. Herramientas de capacitación. Fuente: Elaboración propia.

Para el caso se consideró pertinente tener en cuenta las herramientas de fortalecimiento que presenta actualmente la Policía Nacional en materia de ciberseguridad, la cual está enfocada a ofrecer a los funcionarios unos cursos, a través de los cuales se busca mejorar sus competencias y mantenerlos

actualizados en conocimientos cibernéticos y tecnológicos. Es preciso tener en cuenta estos cursos, pues lo que se quiere es fortalecer la estrategia presentada, mediante un curso básico adicional para todo el personal policial, que contribuya a potenciar lo que hasta el momento viene ofreciendo la Policía Nacional para cada una de sus especialidades. (ver tabla 8)

Tabla 8. Cursos de ciberseguridad ofrecidos por la Policía Nacional

Cursos	Temas
Curso en Ciberseguridad ***58 horas – presencial*** ***Equipo móvil de capacitación - EMCAP***	Tema 1. Fundamentos de ciberseguridad Tema 2. Fundamentos de redes Tema 3. Técnicas de protección de información Tema 4. Arquitectura de seguridad
Protección de datos (Seminario) 41 horas – virtual ***Escuela de inteligencia y contrainteligencia - ESCIC***	Tema 1. Normatividad Tema 2. Derechos humanos en seguridad de la información – protección de datos Tema 3. Modelo operacional Tema 4. Medios físicos y magnéticos – diagnostico Tema 5. Taller pedagógico e interiorización de conocimientos.
Protección de datos (Curso) ***158 horas – presencial*** ***Escuela de investigación criminal - ESINC***	Tema 1. Informática forense (investigación criminal y evidencia digital) Tema 2. Prevención (cadena de custodia digital y protocolos técnicos y específicos). Tema 3. Sistemas operativos (Dispositivos de almacenamiento periféricos y móviles) Tema 4. Introducción a la informática forense y seguridad informática (técnicas, herramientas y procedimientos para la recolección y análisis de evidencia digital.

Fuente: Dirección nacional de Escuelas

83.1 Información general del curso

Tabla 9. Información general del curso

Nombre del curso:	***CURSO EN CIBERSEGURIDAD***
Duración:	**180 horas**
Responsable:	**Policía Nacional**
Modalidad:	**presencial y/o virtual**
Conocimientos previos:	Conocimientos básicos del software, bases de datos, sistemas operativos y redes de computadores.
Descripción del curso:	Con el fin de que los miembros de la Policía Nacional puedan cumplir a cabalidad con sus funciones de investigadores, el curso ofrece al uniformado el mejoramiento de aspectos o competencias relacionadas con el manejo de procesos investigativos en lo que respecta a la ciberseguridad y el impacto de las TIC en los procesos, la aplicación de principios de privacidad, control y transparencia y la seguridad en datos; así mismo, el conocimiento profundo sobre la incidencia de la ciberseguridad, el manejo adecuado de los mecanismos de autenticación, la adquisición de información sobre cómo evolucionó la profesión del investigador en el entorno virtual y la preocupación por los retos que representa las nuevas formas de vida y desarrollo político, económico y social en la red, entre otras que son claves para aquellos que deseen desarrollar eficientemente sus funciones y puedan generar hábitos que beneficien la vida social y económica.

83.2 Intencionalidades formativas

Propósitos:	Introducir al estudiante en conocimientos sobre "Ciberseguridad" como una estrategia y una alternativa en la adopción de nuevas técnicas para el desarrollo de aplicaciones novedosas, combatiendo delitos a nivel nacional e internacional relacionadas con la reacción proactiva y preventiva de delitos cibernéticos en un contexto de investigación criminal.
Competencias generales del curso:	✓ El estudiante obtiene conocimientos teóricos y adopta nuevas técnicas relacionadas con la reacción proactiva y preventiva de delitos cibernéticos. ✓ El estudiante adquiere la capacidad para relacionar casos nacionales con hechos y estrategias de ciberseguridad internacional a partir de los nuevos delitos cibernéticos presentes a nivel nacional e internacional desarrollando la capacidad para enfrentarlos. ✓ El estudiante a través de los conocimientos y aplicaciones de principios de segundad, privacidad, control y transparencia, en los procesos de investigación, realiza la interpretación de datos y códigos relevantes dentro del área de seguridad informática y de la comunicación con un manejo eficiente de datos, con procedimientos adecuados que garanticen la fiabilidad y aseguramiento de la información operada en cada investigación.

833 Contenidos del curso

Tema 1. Introducción a la ciberseguridad	✓ Normatividad – Conpes 3710 y 3854 ✓ Conceptos fundamentales
Tema 2. Ciber riesgos y seguridad institucional	✓ Pilares de la seguridad ✓ Tipos de amenazas ✓ Malware ✓ Protección con malware ✓ Suplantación de identidad, alteración de información, ausencia de disponibilidad y confidencialidad.
Tema 3. Identidad digital	✓ Ingeniería social ✓ Autenticación y firmas electrónicas
Tema 4. La cultura de la seguridad	✓ Navegadores web ✓ Privacidad en los navegadores ✓ Identificar webs seguras
Tema 5. Redes inalámbricas	✓ Redes wifi ✓ Protocolos de cifrado ✓ Filtrado de direcciones y ocultación
Tema 6. Cifrado y seguridad institucional	✓ Técnicas de cifrado ✓ Cifrado de correo electrónico ✓ Conexión VPN ✓ Manual de seguridad de la información
Tema 7. Proteger a tus ciudadanos	✓ Centro cibernético policial – CCP ✓ Equipo de respuestas a incidentes cibernéticos – CSIRT ✓ Unidad Especializada encargada de investigar los delitos de secuestro y extorsión a través de entornos digitales - CiberGAula
Tema 8. Informática Forense – Rastro digital	✓ Componentes de la seguridad perimetral en las redes ✓ Adquisición, copia forense y cadena de custodia ✓ Leyes vinculadas a la actividad de peritaje ✓ Elaboración y redacción de informes y dictámenes periciales ✓ Herramientas forenses.

Fuente: Elaboración propia.

8.3.3.1 . Procedimientos de retroalimentación y evaluación. Para la evaluación de las actividades propuesta se recurrirá al uso de las siguientes rubricas de evaluación:

Tabla 10. Rubrica para evaluar los talleres

Criterios de evaluación	**Excelente**	**Bueno**	**Regular**	**Malo**
Cantidad de respuestas	Respondió el 100% del taller	Respondió el 75% del taller	Respondió el 50% del taller	Respondió el menos del 25% del taller
Calidad y coherencia de las respuestas	Hay calidad y coherencia en el 100% de las respuestas	Hay calidad y coherencia en el 75% delas respuestas	Hay calidad y coherencia en el 50% de las respuestas	Hay calidad y coherencia en menos del 250% de las respuestas
Responsabilidad	Cumplió de manera impecable con los tiempos de entrega	Cumplió a destiempo con la entrega de manera incompleta en un 20%	Cumplió a des tiempo y de forma incompleta en un 50%	Cumplió a destiempo e incompleto en un 80%

Fuente: Elaboración propia

8.3.3.2 Actividades de enseñanza/aprendizaje. En el caso de este curso, que como ya se ha venido mencionando busca fortalecer las competencias de los funcionarios de la Policía Nacional en materia de ciberseguridad, las actividades de enseñanza/aprendizaje apropiadas son:

-*Clases teóricas*: Las clases teóricas las realiza un docente o tutor que cuenta con los conocimientos teóricos y prácticos relacionados en cada uno de los temas que se piensan abordar, de tal manera que los policías tengan una idea clara que sea la base para desarrollar otros procesos o actividades de enseñanza aprendizaje como: talleres, exposiciones e investigaciones temáticas.

-*Talleres:* Estos talleres buscan fortalecer las clases teóricas a través de la respuesta a preguntas y situaciones que podrían enfrentar los policías en un momento determinado, de esta forma toda la estructura del taller va enfocado al conocimiento y solución de hechos que circundan la criminalidad en el ciberespacio.

-*Investigaciones temáticas:* Las investigaciones temáticas buscan fortalecer la indagación profundización y uso de herramientas TIC, con el fin de obtener resultados efectivos en procesos relacionados con la ciberseguridad. Asimismo, permite conocer los antecedentes de hechos y acontecimientos que se presentan el ciberespacio, además de identificar soluciones que se han dado a problemas por otras entidades u organizaciones enfocadas a combatir la criminalidad en el mundo virtual.

Tabla 11. Rubrica para evaluación de participación en clase

Criterios de evaluación	**Excelente**	**Bueno**	**Regular**	**Malo**
Participación en clase	Intervino activa y periódicamente en las clases aportando coherentemente al tema expuesto.	Intervino activa mente en algunas clases aportando al tema expuesto de forma coherente	Hizo algunas intervenciones mostraron alguna relación con el tema expuesto, pero superficiales	Intervino solo algunas veces y no con relación al tema precisado en clase.
Actitud y comportamiento en clase	La actitud con los compañeros y profesor fue positiva y respetuosa	El comportamiento con los compañeros y con el profesor, fue con respeto, pero con momentos de negativismo	Su actitud fue de poco interés a las actividades en clase, irrespetando así algunas veces a sus compañeros	Presentó falta de respeto a sus compañeros y/o al profesor, actuando de forma negativa.
Responsabilidad	Cumplió de manera impecable con los compromisos de entrega de tareas en tiempo y forma.	Cumplió a tiempo con los compromisos, pero no de manera completa.	Cumplió de manera impuntual, incompleta con sus compromisos.	Cumplió con los compromisos sólo algunas ocasiones.

Fuente: Elaboración propia.

Tabla 12. Rubrica para evaluación investigaciones

Criterios de evaluación	Excelente	Bueno	Regular	Malo
Organización y secuencia del contenido	La investigación se presenta de forma consecuente y organizada acorde a los objetivos	La investigación se presenta de forma consecuente pero no está organizada en objetivos	Aunque se da respuesta a los objetivos no es muy consecuente	No hay secuencia y los objetivos son desarrollados parcialmente.
Coherencia del contenido con el tema	Todas las ideas expuestas hacen parte integral del tema	Las ideas expuestas hacen parte del tema, aunque algunas partes no concuerdan.	No siempre el contenido tratado corresponde al tema	Las ideas expuestas no están relacionadas con el tema sugerido
Aporte del agente al tema investigado	Existe un aporte del congruente y coherente en el logro de tos los objetivos	Existe un aporte en el logro de los objetivos, aunque no siempre es congruente y coherente.	Son pocos los aportes en el logro de los objetivos, y no siempre es congruente y coherente.	No hay aportes personales al tema tratado.
Presentación adecuada del tema de investigación	La investigación muestra un completo entendimiento del tema	La investigación muestra un buen entendimiento del tema	La investigación muestra un entendimiento en algunas partes del tema	La investigación no está acorde al tema

Fuente: Elaboración propia.

Conclusiones

Una vez realizado el análisis del proceso de gestión de la ciberseguridad en la Policía Nacional de Colombia, en la era digital en donde se contó con información suministrada por los funcionarios de investigación de la Policía Nacional y jefe del Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional, Jefe del CiberGaula y jefe del Centro Cibernético Policial, se pudo llegar a las siguientes conclusiones:

El diagnóstico de conocimientos de algunos integrantes de Policía Nacional en temas de ciberseguridad, realizado a través de una encuesta a los funcionarios, donde se determinó las competencias instrumentales y las competencias sistémicas, muestra que en términos generales las competencias instrumentales alcanzan un nivel (84%), las principales falencias están en el manejo de algunos procedimientos e información (70%) y la capacidad para garantizar la seguridad de la información (70%); en tanto que las fortalezas están en la toma decisiones (90%), el trabajo orientado a la consecución de resultados (91%) y el conocimiento deberes y derechos (94%). En tanto que las competencias sistémicas llegan a (70%) de efectividad, así las debilidades se encuentran en el conocimiento de la incidencia del concepto de ciberseguridad (61%), en el manejo de mecanismos de autenticación de datos (64%) y en el afrontamiento incidencia de ciberseguridad (67%); mientras que la fortaleza está en la conciencia de compromiso ético como investigador con (84%).

Con relación a los conocimientos y competencias específicas de los integrantes de Policía Nacional en temas de ciberseguridad, se evidencia la necesidad de fortalecer las competencias específicas afianzadas en el marco normativo; aunque la institución cuenta con investigadores, analistas, peritos informáticos, ingenieros, desarrolladores, abogados e inclusive funcionarios capacitados con un alto nivel de experiencia, formados conforme al rol y responsabilidad que tienen dentro de la institución, aunque dada la complejidad del tema las capacitaciones deben ser y requieren actualización constante.

Dentro de las estrategias aplicadas por la Policía Nacional para la prevención de fuga de datos, control de acceso y seguridad en la red, se relacionan directamente con la labor que desempeña, sin embargo, es necesario la implementación de instrumentos dirigidos desde la

administración del talento humano, con el fin de que todos los funcionarios policiales cuenten con conocimientos basados en las nuevas tecnologías que permitan la prevención de la información.

Frente a un ataque cibernético la Policía Nacional cuenta con equipos y sistemas avanzados para prevenir que se dañe, se pierda información; sin embargo, a pesar de contar con recursos físicos, tecnológicos y humanos importantes que buscan salvaguardar la información de la institución de ataques físicos y cibernéticos, se tienen muchas falencias todavía y debido a la agilidad en el cambio tecnológico no se puede asegurar que la institución esté preparada para un ataque cibernético.

Además, la Policía cuenta con herramientas dispuestas para prevención de problemas de ciberseguridad, dispuestas a fortalecer procesos y procedimientos que faciliten la gestión de las vulnerabilidades y monitoreo continúo, así mismo, persigue el tráfico malicioso realizando correlación de las IPs; además de cooperar y colaborar de forma integrada con agencias internacionales como INTERPOL y EUROPOL.

También incluye un conjunto de herramientas para brindar respuesta aquellos hechos o circunstancias que afectan la seguridad de la información en el ciberespacio; facilitando adelantar investigación y diligencia de procesos con rastreo de acontecimientos paso a paso, estableciendo casusas y consecuencias.

Concerniente a las contramedidas que se usan para enfrentar los ataques cibernéticos que se puedan presentar en la red, se cuenta con firewall de aplicación que se dedican a verificar que consultan las personas en cada sitio web, además el sistema de gestión de la seguridad de la información cuenta con sistemas de control individualizados para cada unidad para minimizar la presencia de vulnerabilidades al momento que se registren programas maliciosos, o amenaza, fundamentados en el mantenimiento y uso adecuado de las tecnologías utilizadas, así como el fortalecimiento de la cultura de los funcionarios, en búsqueda de un equilibrio entre hombre, máquina y sistema

Es importante resaltar que este estudio permitió conocer algunas competencias que tienen los investigadores y afianzar la necesidad de fortalecimiento de competencias que los policías deben tener en materia de Ciberseguridad con el fin de garantizar y salvaguardar los derechos y el bienestar de sus funcionarios, no sólo en el plano físico, sino en el ciberespacio; teniendo en cuenta que en la era de la digitalización la mayoría de las transacciones se realizan a través de medios electrónicos, los cuales si bien es cierto contribuyen al desarrollo y facilitan las operaciones de personas naturales y jurídicas, también son el objetivo de ciberdelincuentes los cuales buscan quebrantar la seguridad para acceder a información y recursos, que pueden afectar de forma directa la institución.

Dada la importancia que tiene la ciberseguridad en un mundo digital y teniendo en cuenta que cada vez son más las personas y las organizaciones que acceden a los medios electrónicos para realizar no sólo sus transacciones comerciales y empresariales, sino también acceder a relaciones sociales e interpersonales en búsqueda de nuevos contactos, se propone la implementación de estrategias basadas en los reglamentos institucionales y políticas públicas fundamentadas en el CONPES, con el fin de, contrarrestar la ciberdelincuencia.

Referencias bibliográficas

Álvarez Munárriz, L. (1994). Nacimiento de la inteligencia artificial. En L. Álvarez Munárriz, *Fundamentos de inteligencia artificial.* España : Edit.um.

Calle Guglieri, J. A. (1997). *Reingeniería y seguridad en el ciberespacio.* Madrid: Diaz de santos

Carlos van-der Hofstadt Roman, J. M. (2013). *Competencias y habilidades profesionales para universitarios* . 2006: Ediciones Díaz de Santos.

Cossa, P. (1962). *Cibernética: del cerebro humano a los cerebros artificiales.* Barcelona : Reveertè .

De Tomás morales, S. (2015). *Retos del derecho ante las nuevas amenazas.* Madrid: Dykinson - Libreria jurídica .

Departamento Nacional de Planeaciòn. (2011). *Documento CONPES 3701* . Bogotà.

Desongles Corrales, J. y. (2006). *Conocimientos bàsicos de informàtica* . España: Mad.

Eugenia, G. M. (2004). *Diseño de proyectos en la investigación cualitativa* . Medellín : fondo .

Galvis Panqueva, A. H. (2004). *Fundamentos de la tecnologìa educativa* . Costa Rica : Universidad estatal a distancia .

Garibay Rivas, S. (2013). Desarrollo del modelo sistèmico - capitulo 2. En S. G. Rivas, *Enfoque sistémico: Una introducción a la psicoterapia familiar - segunda ediciòn.* Mèxico: El manual moderno.

Giant, N. (2016). *Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones* . Madrid : Narcea S.A.

Huertas. (2014). *Reto y amenazas de la seguridad nacional.*

Jorge Pérez Martínez, E. B. (2012). *Privacidad y seguridad en la red. La regulación y los mercados.* Barcelona: Ariel S.A.

Mas, o. M. (2012). *Tendencias en investigaciones.* España: vision.

Medina, E. (2013). Capìtulo I - Cibernètica y socialismo . En E. Medina, *Revolucionarios cibernéticos: Tecnología y política en el Chile de Salvador Allende* . Santiago : LOM Ediciones .

Ministerio de Defensa Nacional, Policìa Nacional - Direcciòn General . (31 de 12 de 2015). Resoluciòn 05839 del 31 diciembre de 2015. *Por la cual se define la structura orgànica de la Direcciòn de Investigaciòn Criminal e Interpol.* Bogotà, Bogotà, Colombia:

PONAL .

Ministerio de Educaciòn . (2011). La formación práctica de estudiantes universitarios: repensando el Practic. *Revista de Educaciòn No. 354.* , 833.

Ministerio de Tecnologías de la información y las comunicaciones . (2014). *Agenda estratégica de innovación: Ciberseguridad* . Marzo.

Monzò Arèvalo, R. (2006). *Concepto de competencia en la evaluaciòn educativa* . Mèxico : Publicaciones cruz S.A. .

Planeaciòn, D. N. (14 de julio de 2011). *Documento CONPES 3701.* Obtenido de Ministerio de Tecnologías de la Información y las Comunicaciones: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Planeaciòn, D. N. (11 de Abril de 2016). *Documento CONPES 3854.* Obtenido de Polìtica Nacional de Seguridad Digital : https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf

Policìa Nacional . (10 de Marzo de 2016). Manual de funciones para el personal uniformado de la Policìa Nacional. *Resoluciòn 00937.* Bogotà.

Policìa Nacional - Cai virtual. (Marzo de 2017). Las Empresas - El blanco de los cibercriminales en Colombia . *Revista de Criminalidad*, 2.

Repùblica, P. d. (1991). Constituciòn Polìtica de Colombia . *Constituciòn Polìtica de Colombia* . Bogotà .

Rodríguez Canfranc, P. (2019). *Ciberseguridad - Protegiendo la información vulnerable.* Madrid: Fundación Telefónica, 2019.

Tamayo, M. T. (2004). *El proceso de la investigación científica.* México : Limusa - Noriega editores .

Velandia Mora, C. (2005). Ha surgido un nuevo paradigma . En C. Velandia Mora, *Modelo pedagògico con fundamentos en cibernètica social* . Bogotà : Universidad Cooperativa de Colombia .

Wiener, N. (1947). *El control de la comunicaciòn entre el hombre y la màquina.* Granada, España .

Wiener, N. (1984). Norbert Wiener y el origen de la cibernètica . En N. Wiener, *Los orìgenes del arte cibernètico en España* (pág. 12). Madrid .

10.1 Anexo A. Encuesta aplicada a funcionarios de ciberseguridad de la Policía Nacional

GESTIÓN DE LA CIBERSEGURIDAD EN LA POLICÍA NACIONAL DE COLOMBIA

Objetivo: realizar un diagnóstico de conocimientos y competencias de los integrantes de Policía Nacional en temas de Ciberseguridad.

Enfocada a: funcionarios de ciberseguridad

Competencias instrumentales *son capacidades cognitivas, metodológicas, técnicas y lingüísticas que se consideran necesarias para la comprensión, la construcción, el manejo, el uso crítico y ajustado a las particularidades de las diferentes prácticas profesionales, de los métodos, procedimientos, técnica se instrumentos profesionales. Por tanto, estas competencias constituyen las capacidades y la formación del graduado:*					
	S	CS	AV	CN	N
¿Desarrollo mi trabajo orientado hacia la consecución de resultados?					
¿Tomo decisiones en el momento oportuno?					
¿Conozco mis deberes y derechos como trabajador de esta área policial?					
¿Cuándo tengo problemas con mi trabajo busco soluciones propias antes de acudir a mis superiores?					
¿Informo oportunamente a mis superiores sobre los pormenores de mi labor policía?					
¿Conozco los procesos, procedimientos y protocolos que se deben desarrollar con motivo de mis labores policiales?					
¿Considero que mi experiencia profesional es un valor agregado para la labor que desarrollo en esta unidad?					
¿Manejo adecuadamente los sistemas formales de información que tiene la policía nacional?					
Conozco que es la ciberseguridad y que tipo de obstáculos					

Competencias sistémicas *son capacidades relativas a todos los sistemas (combinación de entendimiento, sensibilidad y conocimiento; necesaria la previa adquisición de competencias instrumentales e interpersonales). En general hacen referencia a las cualidades individuales, así como la motivación a la hora de trabajar:*					
	S	CS	AV	CN	N
¿Cuándo ingreso al sistema de información, cuento con los mecanismos de autenticación?					
¿Conozco la definición sobre incidentes de ciberseguridad?					
¿Se ha presentado algún tipo de incidente y/o fuga de información en las investigaciones que adelanto?					
¿Me preocupo por la privacidad, situación actual, retos y perspectivas frente a la ciberseguridad?					
¿Me preocupo de informarme sobre cómo evoluciona mi profesión con las nuevas tecnologías?					
¿Cree que es importante desarrollar competencias de ciberseguridad en los investigadores criminales?					

10.2 Anexo B. Entrevista al personal de ciberseguridad de la Policía Nacional

GESTIÓN DE LA CIBERSEGURIDAD EN LA POLICÍA NACIONAL DE COLOMBIA

Objetivo: Conocer el proceso de gestión de la Ciberseguridad en la Policía Nacional de Colombia, en la era digital.

Enfocada a: jefe del área de ciberseguridad

Conocimientos y competencias de los integrantes de Policía Nacional en temas de Ciberseguridad.

1) ¿Considera que el personal a cargo de la Ciberseguridad en la institución es competente, por qué?
2) ¿Los uniformados que hacen parte de unidad de inteligencia y Ciberseguridad requieren una capacitación especial, en que área y en qué consiste?
3) ¿Se capacita constantemente al personal que trabaja la Ciberseguridad en la institución, en que temas y con qué entidades?

Estrategias aplicadas por la Policía Nacional para la prevención de fugas de datos, control de acceso y seguridad en la red.

4) ¿Cómo se realiza el control de acceso y gestión de las entidades que prestan sus servicios a través de las TIC?
5) ¿Qué medidas debe tomar la unidad de inteligencia de la Policía si se presentara una fuga de datos en las entidades vigiladas?
6) ¿Qué proceso se usan para identificar y prevenir los ataques de hackers en las redes?
7) ¿Qué programas de prevención de cuidado en la red fomenta la Policía Nacional ¿Qué programas de prevención de cuidado en la red fomenta la Policía Nacional, enfocado a entidades y la misma comunidad?
8) ¿Se encuentra preparada la Policía para atender un ataque Cibernético en Colombia?

Tácticas de gestión de vulnerabilidades y monitoreo continúo utilizadas por la Policía Nacional

9) ¿Se realiza un monitoreo continuo de las redes y como es el proceso?
10) ¿Qué medidas se toman para minimizar los problemas de vulnerabilidad que se registran con la aparición de nuevos programas maliciosos y hackers?

Mecanismos de respuesta de la Policía Nacional en casos que impliquen recuperación de información y contramedidas."

11) ¿Cuándo se presenta un hackeo, se evidencia la aparición de un programa malicioso o se genera fuga de datos en la red, que sistemas de recuperación se utilizan?
12) ¿Cuáles son las contramedidas que se usan para afrontar los ataques cibernéticos que se puedan presentar en la red?
13) ¿Cuál es el papel de la Policía Nacional en la prevención, detección y respuesta a los problemas de Ciberseguridad que afectan la comunidad y las entidades colombianas?