Diseño y estructuración del grupo de ciberseguridad, enfocado a los sistemas de información, gestionados desde la oficina de telemática en la Policía Nacional

Nelson Javier Peñaranda Lizcano

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

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

DISEÑO Y ESTRUCTURACIÓN DEL GRUPO DE CIBERSEGURIDAD, ENFOCADO A LOS SISTEMAS DE INFORMACIÓN, GESTIONADOS DESDE LA OFICINA DE TELEMÁTICA EN LA POLICÍA NACIONAL

ALUMNO: NELSON JAVIER PEÑARANDA LIZCANO

MAESTRÍA DE CIBERSEGURIDAD Y CIBERDEFENSA

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

Bogotá – Colombia

2020

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

DISEÑO Y ESTRUCTURACIÓN DEL GRUPO DE CIBERSEGURIDAD, ENFOCADO A LOS SISTEMAS DE INFORMACIÓN, GESTIONADOS DESDE LA OFICINA DE TELEMÁTICA EN LA POLICÍA NACIONAL

ALUMNO: NELSON JAVIER PEÑARANDA LIZCANO

DIRECTOR: M.Sc Gabriel Alberto Puerta Aponte

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

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

BOGOTA – COLOMBIA

2020

Aceptación del Trabajo

Nota de Aceptación:

_____

_____

_____

_____

Firma del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Agradecimientos

A Dios por permitirme adelantar y culminar mis estudios de posgrado y generar nuevos conocimientos, fortaleciendo mis competencias técnicas, humanas y de gestión en mi vida laboral; así mismo, a mi madre, mi esposa y mi hijo por el apoyo incondicional para lograr mi meta. Finalmente, a MINTIC por la oportunidad de participar en este proyecto y a mi Policía Nacional de Colomobia por darme el espacio y tiempo suficiente requerido por la maestría.

Contenido

Índice de Ilustraciones

Índice de tablas

1. Resumen

Los sistemas de información en la actualidad, representan un valor importante para la Policía Nacional de Colombia, la implementación de nuevas tecnologías permite optimizar los procesos y procedimientos que se llevan a diario en los lugares de trabajo; es así que, el direccionamiento tecnológico se ubica en la parte alta del mapa de procesos de la Institución y está liderado por la Oficina de Telemática.

La ciberseguridad a nivel Institución, está a cargo del Centro Cibernético Policial encargados de desarrollar estrategias que protejan los datos que viajan a través del ciberespacio de los habitantes del territorio nacional, pero a nivel interno y conociendo los millones de datos que son almacenados desde los sistemas de información que tiene la Institución, no existe en la actualidad ninguna dependencia o grupo que tenga asignadas funciones de Ciberseguridad, direccionadas a vigilar, controlar y monitorear la gestión realizada desde el ciberespacio, por los administradores de sistemas de información con altos privilegios que pueda garantizar la calidad e integridad de los datos (Dirección General, 2019).

Este proyecto propone, el diseño y estructuración de un Grupo de Ciberseguridad en la Oficina de Telemática, con sus cargos, perfiles, tablas de ordenamiento policial, tabla de retención documental, funciones y modificando la estructura orgánica vigente, con el fin de minimizar la amenaza actual encontrada en los administradores de sistemas de información de la Institución con altos privilegios.

Esta investigación es de tipo descriptiva, la cual por definición hace referencia a la caracterización de un hecho o fenómeno tratando de establecer su estructura o comportamiento (Gomez Bastar, 2012); se pretende medir de forma independiente las afectaciones a la integridad de la información por parte de los administradores de los sistemas, a través de los indicadores de gestión diseñados para el Grupo de Ciberseguridad; El enfoque de la investigación es cualitativo, debido a la relación de las variables del

problema de investigación, que involucra la recolección de datos utilizando técnicas como entrevistas a profundidad, revisión de documentos y discusiones en grupo. Las entrevistas, van a ser realizadas al personal del Grupo de Seguridad de la Información, C-SIRT, y el personal que administra técnicamente sistemas de información de la Institución; la investigación también cuenta con un componente de tipo concluyente garantizando la entrega de un producto, resultado del análisis diagnóstico de un esquema de control propuesto (Sampieri et al., 2014).

Se da por finalizada la investigación, cumpliendo con todo el procedimiento estandarizado por la Policía Nacional, para formular el rediseño organizacional de sus dependencias internas, diseñando el Grupo de Ciberseguridad con sus capacidades y aplicando indicadores de gestión para medir la efectividad de su implementación.

2. Abstract

Currently, Information Systems represent a significant value for National Police of Colombia, new technologies implementation allows to optimize processes and procedures that carried out on workplaces; thus, technological addressing is located in the upper part process map of the institution and is led by Telematica Office.

Cybersecurity at institutional level is charge of Police Cybernetic Centre responsible to develop strategies to protect data that travel through cyberspace of inhabitants of the national territory, but internally and knowing million data which are stored from information systems that institution has. Cybersecurity at institutional level is charge of Police Cybernetic Centre responsible to develop strategies to protect data that travel through cyberspace of inhabitants of the national territory, but internally and knowing million data which are stored from information systems that institution has. It doesn't exist at present a dependence or group that have that have assigned functions with cybersecurity focused to monitor and controlling management carried out from cyberspace by the information system administrators with high privileges that allows to guarantee the quality and integrity of data.

This investigation proposes the design and structuring for a cybersecurity group at the Telematic Office with their charges, profiles and Police order table, documental withholding table, functions and modifying the current organizational structure, so as to reduce the current threat found in the information system administrators of the institution with high privileges

This Research is descriptive, which, by definition, is refers to the characterization of a fact or phenomenon trying to establish its structure or behavior; it is purport to measure independently the affectations to the integrity of the information by the system administrators through the management indicators designed for the cybersecurity group; the research approach is qualitative due to the relationship of the variables of problem

investigated that involve data collection through the use of techniques such in-depth interviews, document review and group discussion. Interviews will be conducted to the security information group personnel C-SIRT and staff who administer technically the institution information systems; Also, the research take account with a component of conclusive type guaranteeing the delivering a product result of diagnostic analysis from a control scheme proposed.

Finally, the investigation has concluded with whole fulfilling standardized procedures by the National Police to develop the organizational internal redesign of its dependences through the design of cybersecurity group with its capacities applying management indicators to measure the effectiveness of its implementation.

3. Palabras clave

Ciberespacio.

Ciberseguridad.

Calidad del dato.

Grupo de Administración de Recursos Tecnológicos.

Sistemas de información.

4. Keywords

Cyberspace.

Cybersecurity.

Data quality.

Grupo de Administración de Recursos Tecnológicos.

Information systems.

5. Introducción

A nivel mundial las compañías están ubicando la seguridad de la información y la de todos sus sistemas como prioridad en sus agendas, así lo demuestra un estudio elaborado en conjunto entre McAfee y el Centro para Estudios Estratégicos e Internacionales (CSIS), concluye que el cibercrimen cuesta casi 600.000 millones de dólares a la economía mundial, aproximadamente el 0,8% del Producto Interno Bruto (PBI) global, (Inc, IDG Communications, 2018); comprender el impacto del tiempo de inactividad en la productividad, así como las ventas y la confianza del consumidor es esencial para justificar el gasto en la protección de los activos de información de la empresa en el futuro y mantener la competitividad; según la Revista Gestión (2016):

> Un estudio desarrollado por Intel Security mostró que más del 40% de empresas a nivel mundial se sienten vulnerables ante hackers, según el estudio Predicciones Amenazas de McAfee Labs, los ciberdelincuentes están perfeccionando sus técnicas a nivel mundial y las estrategias de ciberseguridad se vuelven más importantes, (Revista, Gestión, 2016).

En Colombia, el Congreso de la República decretó la Ley 1581 de 2012 que constituye el marco general de la protección de los datos personales en el país, con el fin de que todas las empresas públicas y privadas, garanticen la seguridad de la información de sus clientes, teniendo en cuenta los principios de: legalidad, confidencialidad, integridad, transparencia, acceso y circulación restringida, (Colombia, 2012). Según un estudio realizado por la firma de seguridad informática Digiware, la compañía dio a conocer que en Colombia se registraron 198 millones de ataques cibernéticos, participando con el 8,05% del total de los delitos informáticos de América Latina, lo que equivale a pérdidas por más de US$6.179 millones, (Revista Dinero, 2017).

La Policía Nacional de Colombia, cuenta con la Oficina de Telemática, que tiene como misión asesorar y promover el desarrollo tecnológico de la Institución en las áreas de

Nota: https://computerworld.co/el-cibercrimen-cuesta-600-000-millones-de-dolares-la-economia-mundial/?unapproved=1194&moderation-hash=1bb8a4fb27e63a967a3d330406eadd72#comment-1194

informática y telecomunicaciones a través de la investigación, implementación, administración y soporte, con el fin de estandarizar los procedimientos e innovar la infraestructura telemática para apoyar la gestión policial, (Policía Nacional de Colombia, 2018).

La Oficina de Telemática y otras direcciones de la Institución han desarrollado y adquirido sistemas de información, para la mejora del trabajo que realizan sus integrantes en la ejecución de sus procesos y procedimientos, optimizando recursos y la calidad del trabajo, garantizando un mejor servicio tanto para sus clientes internos como externos; asimismo, la Institución, por ser una entidad del Estado, debe cumplir con toda la normatividad vigente y como cualquier empresa privada, debe evitar la pérdida o adulteración de la información existente en sus bases de datos.

La Oficina de Telemática, que es una dependencia asesora del mando institucional, realiza la gestión necesaria para cumplir la normatividad vigente y garantizar la integridad de la información de sus sistemas. Cuenta con tres grupos encargados de garantizar y mantener el proceso de gestión para la continuidad del negocio, la seguridad de la información y un equipo de respuestas a incidentes (Policía Nacional de Colombia, 2013).

La misión es proteger los activos de información que se encuentran bajo su custodia, de cualquier ataque externo , pero en ningún momento se hace desde el perímetro interno; es decir, cualquier usuario con los roles y privilegios autorizados, o un ciberdelincuente que por algún medio fraudulento los consiga, puede ingresar a las bases de datos desde el ciberespacio (lugar de trabajo, hogar, cualquier sitio), desde la misma LAN o a través de VPN y manipular los datos de los sistemas a su gusto, sin que se genere ninguna alerta o pueda ser detectado.

La Dirección de Investigación Criminal e Interpol (DIJIN), es la unidad operativa del nivel estratégico dentro de la estructura orgánica de la Policía Nacional que contribuye a la prevención y control de la criminalidad; cuenta con el Centro Cibernético Policial que

tiene una línea de investigación en ciberseguridad, enfocada hacia el ciudadano, con el fin de dar pautas y recomendaciones al momento de hacer transacciones bancarias, conocer cómo están protegidas las infraestructuras digitales gubernamentales y prevenir las amenazas cibernéticas que tienen como objetivo la industria, entre otros; pero en ninguna de sus funciones tiene la de velar por la ciberseguridad de la Institución, con relación a los sistemas de información que administrativa y operacionalmente mueven la Policía Nacional.

Sin embargo, en los últimos 4 años según el reporte originado por la Inspección General de la Policía Nacional, se ha visto la afectación del artículo 34 numeral 29 de la Ley 1015 de 2006, por medio de la cual se expide el Régimen Disciplinario para la Policía Nacional, que señala como falta disciplinaria "Afectar los sistemas informáticos de la Policía Nacional" y determina como sanción la destitución e inhabilidad general, ya que se considera como una falta gravísima.

Este proyecto propone el diseño y estructuración de un Grupo de Ciberseguridad, enfocado en los sistemas de información gestionados desde la Oficina de Telemática de la Policía Nacional de Colombia, con el fin de disminuir en gran porcentaje los riesgos en la afectación de la integridad de la información y que haya mayor control sobre los procesos y procedimientos realizados por los administradores de sistemas de información de la Policía Nacional de Colombia en la Oficina de Telemática, (República, 2006).

La información a que tienen acceso los administradores de sistemas de información de la Policía Nacional de Colombia es neurálgica y a gran escala, por eso se hace necesario la creación de este nuevo Grupo de Ciberseguridad, con el fin de gestionar todos los movimientos y transacciones que desde el ciberespacio puedan hacer los administradores técnicos de los sistemas. Cabe mencionar que, la Institución tiene 50 sistemas de información, algunos de ellos desarrollados por la Oficina de Telemática y el resto comprados por otras direcciones, pero con la supervisión de la Oficina de Telemática.

En las empresas, los activos de la información representan un gran valor, tanto así que llegado el caso de perder esos activos o que sea vulnerada su integridad, podría ser el fin para la empresa. En la Oficina de Telemática, la creación del Grupo de Ciberseguridad es una decisión que se debe tomar con urgencia, los sistemas que se custodian son realmente importantes, la información que en ellos reposan es neurálgica y vital para proporcionar continuidad al negocio. Sistemas de información del talento humano, de nómina, de inventarios, el jurídico, estos de la rama administrativa y sistemas de la rama operativa como lo es el sistema de antecedentes, registro nacional de medidas correctivas, sistemas de cuadrantes entre otros, almacenan millones de datos, los cuales en manos de un administrador técnico con fines capciosos, sin la vigilancia y controles desde el entorno de la Ciberseguridad, podría desencadenar en una situación delicada para la Institución y sus empleados.

La gestión en la seguridad de la información y las bases de datos que tiene cada sistema, están centralizadas en la Oficina de Telemática y por ende se debe garantizar la integridad de la información. El que no se cuente con un Grupo de Ciberseguridad, pudo haber contribuido o permitido a que se presenten los casos mencionados y sancionados por la Inspección General; adicional a ello, pude persistir el riesgo a que se siga vulnerando la integridad de la información, está latente sin que pueda ser monitoreado y controlado (Comunicaciones, 2017).

La propuesta no pretende llegar al nivel que se materialice la amenaza, sino contribuir al control y vigilancia de los procesos y procedimientos realizados por los administradores de los sistemas, generando alertas a través de una herramienta tecnológica que cuente con inteligencia artificial, reconocimiento de patrones, y detecte comportamientos anómalos por parte de los administradores técnicos de los sistemas. El software, se parametriza de acuerdo con la necesidad de la Institución y la arquitectura de la aplicación, así mismo, las alertas se pueden ver reflejadas al Grupo de Ciberseguridad, en la interfaz de la herramienta o configurando una cuenta de correo (Wireless et al., 2012).

En el sentido de la necesidad y las competencias del personal, es necesario contar con un talento humano profesional idóneo en ciberseguridad, con las competencias y el perfil técnico requerido en el manejo y administración de la herramienta, sus funciones deben estar enmarcadas y alineadas con la normatividad vigente, teniendo en cuenta que de su trabajo puede dar origen a investigaciones a los usuarios administradores, que por razones diferentes a su misionalidad estén infringiendo los lineaminetos institucionales.

Esta monografía se encuentra dividida en tres objetivos, en primer lugar, se seleccionarán de todos los 50 sistemas de información de la Policía Nacional, aquellos identificados como críticos y más críticos, teniendo en cuenta el criterio del Informe de Análisis de Impacto de Negocio – BIA, realizado por el grupo de continuidad de la información de la Oficina de Telemática, cuyo alcance fue verificar el inventario de activos del proceso de Direccionamiento Tecnológico y su análisis de riesgo, así como el criterio experto de los funcionarios de la Institución que gestionan, administran y verifican el flujo de información de los sistemas de información. Al tenerlos seleccionados, se pretende definir los riesgos en ciberseguridad, enfocado a la vulnerabilidad de la integridad de la información, que pueden estar expuestos estos sistemas (Oficina de Telemática Policía Nacional de Colombia, 2019).

Como segundo objetivo, se propone la creación del Grupo de Ciberseguridad, con su respectiva estructura organizacional, cargos y funciones. Lo anterior, siguiendo los parámetros institucionales que tiene la Policía Nacional de Colombia estandarizados, para la modificación de la estructura interna. Este capítulo pretende generar las capacidades del Grupo de Ciberseguridad, capaz de mitigar los riesgos a la integridad y calidad de la información, que es gestionada por los administradores de sistemas de información de la Policía Nacional de Colombia.

En el último capítulo, se pretende estructurar un plan de operación para el Grupo de Ciberseguridad dividido en cuatro fases, las cuales son: de iniciación, análisis, producción ejecución y seguimiento con evaluación; en este último, se realizará un monitoreo constante

a los indicadores propuestos para la mitigación del riesgo por parte del Grupo de Planeación de la Dirección de Talento Humano, con el fin de enlazar y evaluar los objetivos propuestos en el plan de operación (Vargas, 2018). Del contexto anterior, se desglosa el siguiente interrogante: ¿Cómo diseñar y estructurar un Grupo de Ciberseguridad, enfocado a los sistemas de información gestionados desde la Oficina de Telemática en la Policía Nacional de Colombia?

6. Objetivos

6.1. Objetivo General

Diseñar y estructurar el Grupo de Ciberseguridad, enfocado a los sistemas de información gestionados desde la Oficina de Telemática en la Policía Nacional de Colombia.

6.2. Objetivos Específicos

- Seleccionar los sistemas de información críticos custodiados por la Oficina de Telemática y sus riesgos de ciberseguridad más relevantes, enfocados en vulnerabilidad e integridad de los datos.

- Proponer la creación del Grupo de Ciberseguridad, sus capacidades y su estructura organizacional, aplicando el procedimiento que la Policía Nacional de Colombia tiene estandarizado, mitigando los riesgos a la integridad de los datos.

- Estructurar un plan de operación del Grupo de Ciberseguridad propuesto, para la mitigación de riesgos en las aplicaciones seleccionadas.

7. Metodología

Esta investigación es de tipo descriptiva, la cual por definición hace referencia a la caracterización de un hecho o fenómeno tratando de establecer su estructura o comportamiento (Gómez Bastar, 2012); se pretende medir de forma independiente las afectaciones a la integridad de la información por parte de los administradores de los sistemas, a través de los indicadores de gestión diseñados para el Grupo de Ciberseguridad.

La presente monografía tiene un enfoque metodológico cualitativo, debido a la relación entre las variables del problema de investigación que involucra la recolección de datos utilizando técnicas como entrevistas a profundidad, revisión de documentos y discusiones en grupo, (Hernández Sampieri, Fernandez Collado, & Lucio, 2014).

El método a tener en cuenta, son entrevistas formales, estructurada, siguiendo un orden de preguntas muy estricto con el fin de evitar que el entrevistado se desvíe del tema principal a investigar (Gómez Bastar, 2012), tanto a los funcionarios encargados de la seguridad de la información como a los administradores de las aplicaciones. En el caso de las entrevistas, estas serán dirigidas a los administradores y desarrolladores de sistemas de información de la Oficina de Telemática en la Policía Nacional de Colombia y al personal que labora en el Grupo de Seguridad de la Información y el CSIRT de la Institución.

La investigación también cuenta con un componente de tipo concluyente,(Rodríguez & Valldeoriola, 2010), garantizando la entrega de un producto, resultado del análisis diagnóstico de un esquema de control propuesto, los documentos que se elaboraron para conseguir la viabilidad por parte de la Dirección General de la Policía Nacional de Colombia fueron los siguientes:

1. Solicitud mesa de trabajo para validar el proyecto de Grupo de Ciberseguridad de la Oficina de Telemática.

2. Viabilidad para la elaboración del proyecto orientado a la creación del Grupo de Ciberseguridad de la Oficina de Telemática.
3. Solicitud mesa de trabajo Dirección de Talento Humano, Oficina de Planeación y Secretaría General.
4. Solicitud recepción y revisión de documentación para la creación del Grupo de Ciberseguridad en la Oficina de Telemática de la Policía Nacional de Colombia.
5. Estudio de Planeación.
6. Tabla de Retención Documental para la gestión y archivo de los documentos generados por el nuevo grupo.
7. Tabla de Ordenamiento Policial.
8. Cargos, propósito principal, funciones, funciones genéricas, perfil y habilidades comportamentales de los integrantes del Grupo de Ciberseguridad.
9. Funciones del Grupo de Ciberseguridad.
10. Concepto de la Oficina de Planeación.
11. Concepto de la Dirección de Talento Humano.
12. Concepto de la Secretaría General.
13. Borrador de la nueva Resolución "por la cual se modifica parcialmente la estructura orgánica interna de la Oficina de Telemática creando el Grupo de Ciberseguridad, se determinan sus funciones y se dictan otras disposiciones".

La población con la que se contó para la muestra fue el personal idóneo en el tema, con las competencias necesarias para desarrollar sus funciones y para quienes serián válidas las conclusiones que se obtuvieran. La propuesta de creación del Grupo de Ciberseguridad enfocado a los sistemas de información gestionados desde la Oficina de Telemática para la Policía Nacional de Colombia, coadyuvará con la misionalidad de la Institución, aportando al cumplimiento de las políticas del Sistema de Gestión de Seguridad de la Información (SGSI) y contribuyendo acertadamente a la ciberseguridad del Estado (Ministerio de Interior y de Justicia et al., 2011).

Finalmente, con el resultado de las entrevistas hechas y el consolidado de la selección de los sistemas de información más críticos de la Oficina de Telemática, se consolidó el soporte necesario para estimar pertinente la creación de un nuevo grupo y así mismo responder a la pregunta ¿Cómo diseñar y estructurar un Grupo de Ciberseguridad, enfocado a los sistemas de información gestionados desde la Oficina de Telemática en la Policía Nacional de Colombia?

8. Contexto

La productividad en la era de la información es ampliamente percibida como un problema organizacional importante, una estrategia para mejorar la productividad de las empresas en cuanto a procesos y procedimientos ha sido el uso de sistemas de información. Por definición, es un conjunto de elementos que interactúan entre sí en busca de un fin común, permitiendo que la información esté disponible para satisfacer las necesidades en una organización haciendo alusión tanto al cliente interno como externo (Belloch, 2012).

Los elementos que interactúan entre sí son: los equipos de cómputo, el recurso humano, los datos o fuente de información, software ejecutado, las telecomunicaciones y los procedimientos de políticas y reglas del negocio. Las actividades realizadas por un sistema de información son: entrada de información, almacenamiento de información, procesamiento de la información, salida de información (Niño Camazón, 2011).

La arquitectura de la información, es una disciplina encargada de estructurar, organizar y etiquetar los elementos que conforman el entorno sin formato para facilitar la búsqueda y la actualización de la información por parte de sus usuarios. Entre los principales sistemas o estructuras que conforman la anatomía arquitectónica de un sitio web los sistemas de organización, de etiquetado, de navegación, de búsqueda y los vocabularios controlados. Respecto a su práctica, la elaboración de la anatomía arquitectónica de un sitio web se centra en los aspectos relacionados con las necesidades de sus usuarios (Pérez-Montoro, 2010).

La conexión directa entre los sistemas de información y el desempeño de los negocios ofrece un análisis detallado de la forma en que las empresas contemporáneas utilizan las tecnologías y los sistemas de información para alcanzar sus metas corporativas, deben tener presente la infraestructura TI y tecnologías emergentes, telecomunicaciones, tecnologías inalámbricas. Asimismo, de la seguridad implementada depende la disponibilidad, integridad y confidencialidad de la información (García, González, Luis, & Elmer, 2015).

En los últimos años, los sistemas de información (SI) constituyen uno de los principales campos de estudio en la organización empresarial, debido a la necesidad de identificar su valor empresarial, permitiendo deducir que las empresas que prestan más atención a la mejora de la calidad del sistema de la información y de los sistemas de información, favorecen sus resultados organizacionales (Ábrego, Sánchez, & Medina, 2017).

Es necesario ver algunos antecedentes de la historia a nivel mundial, para prepararnos internamente, se pueden mencionar hechos en los que han ocurrido ataques a un país entero, como lo fue el caso de Estonia (Sánchez, 2012). El problema, para los estonios, es que su país fue absorbido por la URSS, considerando invasores al Ejército Rojo. Los objetivos del ataque fueron las instituciones públicas como el Parlamento y varios ministerios, bancos, partidos políticos y medios de comunicación; este ataque por su gran impacto causado, es estudiado hoy por muchos países y estrategas militares. (Ruus y Reiska, 2015).

Posterior a este ataque ocurrió el caso Stuxnet, que fue el primer virus que causó daños a las plantas nucleares Deirán, el 26 de septiembre de 2010. El ataque fue perpetrado por un gusano informático, bautizado como Stuxnet, capaz de penetrar en los sistemas que se utilizan para controlar instalaciones industriales como plantas de energía eléctrica, presas, y otros complejos. La empresa Symantec explicó que esta amenaza estaba diseñada para permitir a los atacantes manipularan los equipos físicos a su antojo, siendo el primer virus informático capaz de hacer daño en el mundo físico (Falliere, Murchu, & Chien, 2011).

Como en estos dos casos, hay otros de más relevancia a nivel mundial: en Colombia, se presentó en el 2017 un ataque a entidades públicas y privadas con ransomware, logrando secuestrar información y cobrando millonarios rescates pagados en Bitcoin. El ransomware es un software malintencionado que permite a un pirata informático restringir el acceso a la información de una persona o compañía y luego exigir alguna forma de pago para eliminar la restricción. La forma más común de restricción hoy en día es el cifrado de datos

importantes en la computadora o la red, lo que esencialmente permite al atacante mantener los datos del usuario o un rehén del sistema (Brewer, 2016).

La Organización de los Estados Americanos (OEA) es el principal foro político de la región, que promueve y apoya la democracia, los derechos humanos, la seguridad multidimensional y el desarrollo integral de las Américas. La OEA busca prevenir conflictos y lograr la estabilidad política, la inclusión social y la prosperidad de la región por medio del diálogo y de la acción colectiva, como la cooperación, la implementación de mecanismos de seguimiento de los compromisos de los Estados miembros y la aplicación de la Ley Interamericana y de la Ley Internacional (Organización de los Estados Americanos OEA, 2015).

Actualmente en las organizaciones ya sean públicas o privadas se han implementado herramientas tecnológicas, las cuales han optimizado la operación de la empresa, los gobiernos también han contribuido para que este cambio sea adoptado no solo por las grandes empresas sino también por aquellos microempresarios que están llegando al mercado. Los directivos basan sus decisiones en la información (datos ya procesados o que procesamos mentalmente), y las empresas basan su gestión en la información, cada vez más informatizada. El diseño de los sistemas de información adecuados y el aprovechamiento de las posibilidades de las tecnologías de la información pueden aportar a nuestras empresas ventajas competitivas; más aún, sobre todo en determinados sectores, la viabilidad de la propia empresa (M. A. Ramos, 1993).

Tipos de sistemas de información:

En las organizaciones actualmente existen varios tipos de sistemas de información, según el nivel operacional, administrativo o estratégico en que se utilicen. Algunos de los sistemas más comunes se encuentran a continuación:

- Para procesamiento de datos (TPS: *Traditional processing system*): nivel operativo, destinado a procesar grandes volúmenes de información alimentando grandes bases de datos (Liu, Lftikhar, & Xie, 2014).
- Sistema de expertos o basado en el conocimiento (KWS: *Knowledge working systems*): nivel operativo, selecciona la mejor solución para el problema presentado (Gutierrez, 2008).
- Para la administración y gerenciales (MIS: *Management information systems*): nivel administrativo, gestiona y elabora informes periódicos (Aguirre, 2015).
- Para la toma de decisiones (DSS: *Decision support systems*): nivel estratégico, se destaca por su diseño e inteligencia que permite una adecuada selección e implementación de proyectos (Karen, 2015).
- Para ejecutivos (EIS: *Executive information systems*): nivel estratégico, sistema personalizado para que cada ejecutivo para que pueda ver y analizar datos críticos (Yu, Chen, Klein, & Jiang, 2015).
- Sistemas funcionales relacionados con los procesos internos de la organización: forman la base de los sistemas de información para ejecutivos (Kyocera, 2018).

Para el caso de Colombia, se puede mencionar cómo el Estado ha invertido recursos para que las instituciones estén alineadas con sus homónimos de otros países; un ejemplo claro se vé en la Policía Nacional de Colombia que, a través del Ministerio de Defensa, recibió en el año 2000 el Sistema para la Administración del Talento Humano "SIATH", con el que se optimizaron todos los procesos y procedimientos que se estaban llevando de forma manual (Valencia, 2015).

Como este caso, existen en casi todas las dependencias del Estado que han avanzado en la creación y administración de bases de datos sensibles relacionadas con sus ámbitos de acción. En este sentido, en julio de 2011 el Departamento Nacional de Planeación generó el Documento CONPES 3701 "Lineamientos de Política de Ciberseguridad y Ciberdefensa", que propone lineamientos de política para Colombia en Ciberseguridad y Ciberdefensa, desarrollando e implementando una estrategia nacional que neutralice el incremento de las amenazas ciberneticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales de incidentes de Ciberseguridad, aplicando la normatividad vigente del país en relación al tema intervenido (Departamento Nacional de Planeación, 2011).

La generación de este importante documento, fue consecuencia de las constantes amenazas que se estaban materializando en el sector público y privado del país, no hay que desconocer que el uso de las tecnologías de la información y las telecomunicaciones son parte de un mundo globalizado y trae cambios relevantes que ayudan a la realización de las tareas cotidianas, pero también incrementan el uso de medios tecnológicos para fines delictivos (Cortés Borrero, 2015).

Ahora bien, conscientes de que los sistemas de información abarcan un punto estratégico para cualquier empresa, desde el Gobierno nacional se han provisto importantes recursos económicos a las Fuerzas Militares y a la Policía Nacional para gerenciar el Direccionamiento Tecnológico.

En la Policía Nacional de Colombia este proceso está a cargo de la Oficina de Telemática que tiene como misión asesorar y promover el desarrollo tecnológico de la Institución en las áreas de informática y telecomunicaciones, a través de la investigación, implementación, administración y soporte, con el fin de estandarizar los procesos y procedimientos e innovar la infraestructura tecnológica para apoyar la gestión policial (Policía Nacional de Colombia, 2018).

La Oficina de Telemática de la Policía Nacional de Colombia, funciona como una oficina asesora de la Dirección General, desarrollando e implementando sistemas de información para darle un entorno gerencial a todos sus procesos y procedimientos, cuenta con varios grupos de trabajo entre ellos el grupo de Administración de Recursos Tecnológicos (GARTE), encargado de la administración, ajustes y soporte de los sistemas de información y correo electrónico, el se creó la Resolución número 08310 del 28 de diciembre de 2016 "Por la cual se expide el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional", con el objetivo de proteger los activos de la información como insumo fundamental para el cumplimiento de la misión y asegurar la supervivencia y continuidad de la Institución, protegiéndola tanto administrativa como penalmente a través de la aplicación efectiva de las mejores prácticas, acceso autorizado a sus sistemas de información, escritorios limpios, conexiones seguras y controles, garantizando la gobernabilidad del país. (Policía Nacional de Colombia, 2016).

Las tecnologías de la información demandan la generación de medidas adecuadas de ciberseguridad y ciberdefensa en la integridad de la información. La gestión sistemática de los datos es una de las iniciativas más importantes para la gestión de tecnologías de la información (Fabiano Couto Corrêa, 2016). Al menos desde que los informes sobre privacidad y violaciones de seguridad, prácticas contables fraudulentas y ataques a sistemas de TI aparecieron en público, las empresas y organizaciones han reconocido su responsabilidad de proteger los activos físicos y de información. Los estándares de seguridad se pueden utilizar como guía o marco para desarrollar y mantener un sistema adecuado de gestión de seguridad de la información (SGSI). Las normas ISO / IEC 27000, 27001 y 27002 son normas internacionales que están recibiendo un reconocimiento y una adopción crecientes. Se les conoce como "lenguaje común de las organizaciones en todo el mundo" para la seguridad de la información (Disterer, 2013).

Teniendo en cuenta las normas anteriores, que contribuyen a la integridad de la información y el Manual de gestión de seguridad de la información de la Policía Nacional de Colombia, la Oficina de Telemática tiene bajo su custodia, todas las bases de datos

donde se almacena la información que es gestionada por los administradores de los sistemas de información desde el nivel central (la misma Oficina de Telemática) y otras direcciones que han adquirido otros sistemas de información (Dirección Nacional de Escuelas, Dirección de Tránsito y Transporte, Dirección de Investigación Criminal e Interpol).

La Oficina de Telemática el 16 de marzo del año 2019 tomó la decisión de realizar el Business Impact Analysis (BIA), con el objetivo de determinar el nivel de criticidad de los 50 sistemas de información con los que cuenta la Policía Naciomal y sus demás implicaciones. Es importante conocer que para la construcción de un plan de continuidad es esencial realizar el Business Impact Analysis, ya que es una guía que permite identificar las operaciones y servicios críticos dentro de la organización (Leopold, 2013).

El Informe de Análisis del Impacto de Negocio (BIA, por sus siglas en inglés), fue elaborado por el Grupo de Continuidad del Negocio de la Oficina de Telemática, dirigido por el capitán Jhon Guevara, a través del documento controlado de la institución 1DT-FR-0055. (Oficina de Telemática Policía Nacional de Colombia, 2019).

El análisis de impacto al negocio (Business Impact Analysis), es otro elemento o informe utilizado que muestra consideraciones importantes para la gestión del riesgo que podría padecer una organización como resultado de la ocurrencia de un incidente o desastre, así como el análisis de los costos que ocasiona la interrupción de algún o algunos procesos críticos en una empresa y la estimación del tiempo tolerable para recuperarse (Oficina de Telemática Policía Nacional de Colombia, 2019).

El informe BIA, considera el análisis de impacto al negocio de los sistemas de información cuyos servidores están en custodia del centro de cómputo principal de la Policía Nacional de Colombia, tomando como metodología en su primera fase la identificación de los sistemas de información o herramientas tecnológicas críticas, la

segunda fase, es la identificación de impacto por interrupción RTO-RPO y por último, la documentación de los resultados del BIA.

En la primera fase se identificaron 26 sistemas, de los cuales 10 fueron catalogados como críticos y 16 muy críticos; análisis originado de las entrevistas realizadas a los líderes funcionales y técnicos de cada sistema, teniendo en cuenta las siguientes consideraciones:

- Puntos críticos: en esta sección se evaluó el impacto de la no disponibilidad de la aplicación en el tiempo, orientada a dos (2) factores: Reputación y operación, para identificar el Tiempo Objetivo de Recuperación (RTO) de la aplicación.

- Variaciones en el trabajo: se evaluó cuáles son los periodos de mayor sensibilidad en la operación, a nivel de días, meses, horas específicas o fechas especiales.

- Dependencias: se identificaron las dependencias de información ya sea a nivel de servidores, bases de datos o entre aplicaciones.

- Procedimientos alternos: se presentaron las actividades que realizan o que se tienen planeadas para operar de forma alterna, en caso de presentarse la no disponibilidad de algún componente o el sistema de información.

- Requerimiento de recursos: se relacionó la información asociada a los recursos que requiere la aplicación, con el fin de continuar la operación en otra localidad.

- Registros vitales: se recolectan los activos de información digitales o físicos que son esenciales para soportar, restablecer y/o recuperar la aplicación y sin los cuales la aplicación no puede operar o se ve impactado de manera significativa.

8.1. Selección de los sistemas de información que soportan los procesos según su criticidad.

8.1.1. Críticos

- Sistema de Información de Liquidación Salarial (LSI), soporta el proceso de nómina del personal activo de la Policía Nacional de Colombia y pensionados, registrando las novedades de embargos y adiciones que cause derecho cada miembro de la Institución. Teniendo en cuenta el informe BIA, existe la vulnerabilidad en el entendido que su administrador funcional puede ingresar al sistema con sus permisos debidamente otorgados y manipular la información almacenada en el sistema, es tan neurálgico el tema porque se puede prestar para cometer actos de corrupción, conociendo que en este sistema se encuentran todas las tablas y procedimientod que la Institución toma para realizar sus procesos de nómina y cancelarle a su personal. Un administrador podría grabarse en el sistema adicionales o primas sin ser detectado, vulnerando así la integridad de los datos.

- Sistema de Información Jurídico (SIJUR), sirve para realizar seguimiento y control a las investigaciones disciplinarias, procesos administrativos, derechos de petición, tutelas, y contencioso administrativo llevadas a los funcionarios de la Policía Nacional de Colombia. El informe BIA, da a conocer que se debe garantizar la integridad de este sistema, ya que se encuentra almacenada información tanto administrativa como penal de los funcionarios, el riesgo es permanente por la gestión de su administrador técnico, quien no tiene el control y monitoreo constante para conocer sus transacciones y fácilmente puede desde el ciberespacio cometer una conducta punible.

- Sistema de Información para la Gestión del Equipo Automotor (SIGEA), se maneja el control del parque automotor que se asigna a los funcionarios de la Policía Nacional de Colombia, su administración técnica y funcional esta a cargo de la Dirección Administrativa y Financiera, es de mencionar que las bases de datos de todos los

sistemas están bajo custodia de la Oficina de Telemática de la Policía Nacional de Colombia. La integridad de este sistema es de gran importancia para el manejo de los recursos institucionales, fácilmente el administrador técnico por no ser monitoreado podría eliminar todo el historial del sistema de un vehiculo institucional y apropiarse del mismo, solo que en paralelo con este sistema, la Institución realiza una serie de cumplimientos los cuales cada mes físicamente a través de actas, quedan por escrito las revistas físicas que se hacen a los automotores; esto ayuda a controlar al personal que tiene asignado estos vehículos.

- Sistema de Información para la Gestión de Elementos del Servicio de Policía (SIGES), controla la entrega del armamento para las unidades de Policía, procedimiento que también se realiza en físico y debe estar alineado sus balances, cuando se hacen las auditorias por parte del personal del área de control interno de la Institución.

- Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo de la Policía Nacional (SIEDCO PLUS). Sistema de información donde se registran todas las conductas delictivas y actividad operacional de la Policía Nacional de Colombia; además contiene 5 módulos entre los que están: el Sistema de Denuncias y Contravenciones (SIDENCO), que registra denuncias recibidas por la Policía Nacional de Colombia a nivel país en las salas de denuncias, las cuales se envían a la Fiscalía General de la Nación a través de un web service. Sistema Estadístico Vial SIEVI), registra actividades propias de tránsito además de hechos conocidos de accidentalidad vial en el país. Sistema de Información Policial Antisecuestro y Extorsión (SIPSE), registra todas las conductas conocidas por la Dirección de Antisecuestro y Antiextorsión de la Policía, referente a los hechos de secuestro en el país, desde el pago, el valor y el estado de los secuestrados. Sistema de Información contra el Tráfico de Especies Silvestres (SITIES), registra la información referente a la identificación de especies a través de sus nombres taxonómicos específicos y delitos relacionados con ellas. Sistema de Información Estadística Delincuencial y Contravencional (SIEDCO), que registra la actividad operacional de cada una de las unidades de policía y la actividad delictiva de cada

departamento del país. Sistema de Integración Policial de la Accidentalidad y Salud en el Trabajo (SIPAST), en el que se registra la información concerniente a los accidentes de los funcionarios de la Institución.

El Grupo de Seguridad de la Información entrego en su informe BIA, el análisis de vulnerabilidad del sistema en mención, donde deja por escrito que al momento de ser viciada la información almacenada, la institución podría enfrentar procesos penales por que de estos sistemas depende la cantidad y calidad de denuncias que llegan a la fiscalía y que viajan a través de un web service, que la Policía Nacional de Colombia tiene con Fiscalia General de la Nación para comenzar el respectivo trámite judicial.

- Correo Electrónico, servicio bajo el cual se envían y reciben mensajes de manera instantánea a través de Internet, con el fin de tener una comunicación más rápida y de mayor cobertura al personal policial. La Institución debe garantizar que los funcionarios no sean víctimas de phishing (Policía Nacional de Colombia, 2013). El administrador tiene dentro de sus funciones garantizar que el servicio se encuentre disponible 24/7, pero también es de conocimiento que tiene los permisos para acceder a cualquier cuenta y vulnerar la integridad de la información sin ser detectado en tiempo real.

- Portal de Servicios Internos (PSI EVA), al que los funcionarios tienen acceso para consultar toda la información personal en la Institución y la de sus beneficiarios, realizando gran cantidad de procedimientos en línea, sin la necesidad de asistir físicamente a la oficina dueña del proceso. Plataforma de evaluación y clasificación, donde está el historial con relación a la evaluación y clasificación de cada empleado (Dirección General Policía Nacional de Colombia, 2013). Al igual que los otros sistemas, el administrador técnico puede vulnerar la calidad de los datos almacenados, con el fin de sacar provecho propio o para un tercero con información de su vida institucional o de sus beneficiarios.

- Sistema de Información para la Gestión de Incidentes en TIC (SIGMA), los requerimientos a nivel nacional generados por cualquier miembro de la Institución, llegan al Grupo de Mesa de Ayuda de la Oficina de Telemática, que revisa el requerimiento y lo escala al funcionario competente para darle solución. Este sistema es netamente administrativo y esta orientado solamente para mejorar y solucionar problemas técnicos que los usuarios presentan con otros sistemas de información.

- Sistema de Información para la Incorporación (SINCO), permite la preinscripción e inscripción a todas las modalidades de estudio, ofrecidas por la Dirección Nacional de Escuelas. Para este sistema de información, el informe BIA dio a conocer que llegado el caso que su administrador técnico quiera manipular la información contenidad de los aspirantes para ingresar a la institución, es vulnerable y delicado ya que no existe control de las transacciones realizadas desde su código fuente, facilitando por ejemplo el ingreso a la institución como miembro activo a una persona que no cumpla con el perfil requerido.

- Suite Visión Empresarial (SVE), es una herramienta gerencial utilizada para definir y hacer seguimiento a la estrategia de la institución, también están descritos todos los procesos y procedimientos estandarizados en la Policía Nacional de Colombia. Por ser netamente administrativa, no es que genere tantos riesgos de vulnerabilidad a la integridad de la información almacenada, por ende con los controles existentes es importante garantizar el acceso autorizado de la herramienta.

8.1.2. Muy críticos:

- Sistema para la Administración del Talento Humano (SIATH), es el principal sistema que tiene la Institución, teniendo en cuenta que sirve de insumo para la ejecución de otras aplicaciones. En este sistema, se encuentra toda la información personal de los empleados de la Institución y sus beneficiarios; también se registran todas las situaciones administrativas (ascensos, vacaciones, traslados, comisiones, cursos,

ausencias laborales), que puede presentar el empleado en su trayectoria institucional (Dirección General de la Policía Nacional de Colombia, 2002).

A nivel país, todas las unidades descentralizadas de talento humano utilizan este sistema para realizar los procedimientos relacionados con la gestión del personal activo, pensionado y beneficiarios de la Institución. Con relación al informe BIA, que es el insumo tomado para definir la vulnerabilidad existente en los sistemas de la Institución, este arroja como resultado el alto grado de vulnerabilidad que tiene el sistema "SIATH", por ser transversal para la ejecución e ingreso a otros sistemas de información, garantizar la integridad de los datos almacenados desde este sistema es neurálgico y está a cargo de la Oficina de Telemática, quienes lo pueden hacer desde el entorno físico pero el riesgo sigue latente desde lo digital; el acceso desde el ciberespacio, no es controlado ni monitoreado, por ende el administrador técnico tienes los roles y permisos necesarios para acceder al sistema.

Es realmente necesario controlar desde el entorno de la ciberseguridad este y el resto de sistemas de información, como ejemplo se mencionará el caso que puede ocurrir si el administrador técnico accede desde el ciberespacio y adultera los datos almacenados en la tabla de vacaciones con relación a los días disfrutados; en este caso, con fines delictivos y para recibir dádivas el administrador técnico sin ser detectado puede afectar la integridad de la información y eliminar la trazabilidad de la misma. Así mismo, otro ejemplo puede ser el tiempo que lleva un funcionario en la Institución y que el sistema lo almacena en la tabla de tiempos empleados, donde al momento de ser vulnerada y afectada la calidad del dato se puede prestar para cometer conductas negativas y sacar provecho propio de la situación.

- Sistema de Información para la Vigilancia Comunitaria por Cuadrantes (SIVICC 2), registra y controla las actividades realizadas por los policías de los cuadrantes a nivel nacional durante el servicio; de igual forma se planean las actividades de policía y permite habilitar el servicio en línea a los equipos móviles de los policías, para la verificación de los antecedentes de personas y vehículos. Es poco probable que se

pretenda vulnerar la información por parte de su administrador, teniendo en cuenta que este sistema sirve para guardar el trabajo realizado por los policiales del cuadrante de vigilancia.

- Sistema de Identificación del Directorio Activo de la Policía Nacional de Colombia (OID), Oracle Identity Manager está diseñado para gestionar los privilegios de acceso del usuario a través de todos los recursos de una empresa, a través de todo el ciclo de vida de gestión de identidad. Básicamente lo que busca la herramienta es que el control del acceso a todas las plataformas de una organización se realice desde un solo punto (Secretaría General - Policía Nacional, 2011).

- Sistema de Información de Inventarios (SINVE), se registra la información de los inventarios tecnológicos de la Policía Nacional de Colombia. Cada vez que se asigna un elemento, automáticamente queda registrado en el sistema, teniendo un control total del inventario y generando las alertas necesarias cuando el funcionario sale de vacaciones, traslado o es retirado de la Institución (Dirección General , 2019). Garantizar la calidad de los datos almacenados es vital, teniendo en cuenta que se trata del registro de todos los elementos que la Institución asigna y están a cargo del mismo personal, si se afecta la integridad de la información, fácilmente se puede presentar la situación que se pierdan elementos los cuales no sea posible conocer quien las tenga asignadas.

- Sistema de Información Operativo de Antecedentes (SIOPER), es administrado desde la Dirección de Investigación Criminal e Interpol. Allí reposan todos los antecedentes de personas y vehículos subidos por la Fiscalía y los juzgados, a nivel nacional. Operativamente es un sistema bastante neurálgico, si es afectada la integridad de sus datos, se podría omitir como por ejemplo una orden de captura con fines de extradición mientras la persona pasa por el control de migración del aeropuerto, posterior a que la persona pase este filtro el administrador actualiza el sistema sin dejar trazabilidad pero si materializando una amenaza desde el ciberespacio.

- Gestor de Contenidos Policiales (GECOP), herramienta de gestión documental que permite dar una trazabilidad y optimizar tiempos de respuesta a los diferentes requerimientos a nivel interno y externo de la Policía Nacional de Colombia (Secretaria General Policía Nacional de Colombia, 2017). La administración técnica esta a cargo de la Oficina de Telemática, quien debe garantizar la integridad de los datos; es de gran importancia que no sea vulnerado este sistema, por cuanto se gestionan documentos confidenciales y neurálgicos, con gran valor institucional y personal de los policías.

- DOMINIO, servidor central de la Institución, comunicado por medio de un conjunto de ordenadores conectados en red, que permite la administración de los privilegios que tienen los usuarios finales, teniendo el control total de sus máquinas y restringiendo algunas funcionalidades del equipo o de accesos. Para el área de seguridad de la información, en el Dominio es imprecindible garantizar solo su acceso autorizado y que el administrador técnico en conjunto con el personal de conectividad implementen las reglas necesarias para restringir su acceso.

- Página web, documento electrónico que contiene información textual, visual y sonora accesible a través de internet por el ciudadano, para consulta de servicios y noticias ofrecidos por la Policía Nacional de Colombia a través de sus diferentes direcciones (Dirección General - Policía Nacional de Colombia, 2006). El contenido que se sube a esta herramienta tecnológica, lo realiza la Oficina de Comunicaciones Estratégicas de la Institución, donde tienen un procedimiento establecido para cargar la información; su vulnerabilidad según el estudio BIA, se puede presentar al momento que dupliquen la pagina y mediante phishing engañen a alguna persona.

- Registro Nacional de Medidas Correctivas (RNMC), herramienta que permite digitalizar y almacenar el registro nacional de los comparendos aplicados por medidas correctivas al ciudadano por comportamientos contrarios a la convivencia, para este sistema se revisó su vulnerabilidad desde el entorno de la ciberseguridad, a través de un conteo aleatorio de la información almacenada en las bases de datos de Policía como en los

archivos planos originados por las casas de justicia; teniendo en cuenta está situación y por ser un sistema compartido no es tan viable que haya afectación de la integridad de los datos almacenados (Dirección General Policía Nacional de Colombia, 2017).

- POLIRED, es un documento electrónico de la Institución que contiene información textual, visual y sonora, accesible a nivel interno por los funcionarios policiales; en ella se publican los servicios, noticias, información general de interés y enlaces a los principales aplicativos usados por la Policía Nacional de Colombia para apoyar la gestión de procesos de las direcciones (Policía Nacional de Colombia, 2018).

- Plataforma de Llave Pública (PKI), gestiona la generación de firmas digitales a los funcionarios de la Policía Nacional de Colombia, sirviendo como insumo al gestor de contenidos policiales en la estructura final de los documentos, la Institución está acreditada por el Organismo Nacional de Acreditación de Colombia – ONAC, quienes realizaron las respectivas pruebas de funcionalidad de este sistema. (Dirección General de la Policía Nacional de Colombia, 2019).

- Sistema de Recepción de Denuncias (¡A Denunciar!), permite a los ciudadanos desde cualquier lugar del país y con acceso a internet, realizar cualquier tipo de denuncia de tipo penal, ahorrando tiempo y haciendo la diligencia judicial más oportuna y eficiente. Es un sistema hibrido con conexión en tiempo real con la Fiscalia General de la Nación, la vulneración a la integridad de sus datos puede ser mínima por parte de los administradores técnicos, teniendo en cuenta que la data almacenada esta compartida con otra entidad del estado y los sistemas están diseñados para que guarden la trazabilidad de las transacciones realizadas. (Dirección General Policía Nacional de Colombia, 2019).

- Autenticación Personal Plena de Origen Lógico (APPOLO), identifica al ciudadano por medio de la huella dactilar con información real que se encuentra en la base de datos de la Registraduría Nacional del Estado Civil, para llevar a cabo este procedimiento el

sistema debe consultar a dos bases de datos, la primera es externa que es la Registraduría Nacional del Estado Civil, para saber la plena identificación de la persona que se esta cotejando; posterior, viajan los datos hasta la Dijin para verificar si existe alguna orden de captura vigente, es poco probable que haya adulteración en la calidad de los datos. (Secretaria General Policía Nacional, 2016).

- Sistema para la Recepción de Peticiones, Quejas, Reclamos o Sugerencias (PQRS), interpuestas por la ciudadanía en general, estas solicitudes son recepcionadas por el sistema y automáticamente llegan a la Inspección General, que las revisan y dan trámite a la Oficina de Atención al Ciudadano donde labora el uniformado (Policía Nacional de Colombia, 2016).

- Sistema para el Reporte de Documentos Extraviados (SIDEX), permite a los ciudadanos hacer el reporte de la pérdida de sus documentos y dejar el precedente en caso de que sean utilizados de manera fraudulenta por la persona que los encuentre (Dirección General Policía Nacional de Colombia, 2019).

- Sistema de Información para el Seguimiento y Control en la Atención de Casos (SECAD PLUS), permite recepcionar y gestionar todas las llamadas que ingresan al número único de emergencias que tiene la Institución a nivel nacional, en este sistema queda almacenado toda la trazabilidad del caso de policía, desde que ingresa la llamada, hasta que la patrulla de vigilancia reporta la culminación del caso y qué acciones realizó (Departamento Nacional de Planeación, 2006).

Del anterior análisis a los sistemas de información de la Institución, y teniendo presente la aplicación del Informe Análisis de Impacto de Negocio – BIA, realizado por la institución el 16 de marzo de 2019, se deja con argumentos más precisos la necesidad de crear el Grupo de Ciberseguridad en la Oficina de Telemática, que se debe encargar de vigilar y monitorear todas las transacciones que realizan sus administradores técnicos;

también podemos abstraer la importancia que tienen estos sistemas de información para la Institución pero a su vez, el gran problema que se puede presentar si es vulnerada la integridad de sus datos.

Las entrevistas realizadas a los administradores de sistemas de información de la Oficina de Telemática y personal del Grupo de Seguridad de la Información, fueron contundentes para continuar con la investigación planteada y desarrollo de los objetivos. A continuación, se muestra el formato de las preguntas planteadas durante la entrevista y el resultado arrojado por parte de los administradores de los sistemas de información, asi:

Bogotá: 15-09-2018

Nombre del entrevistado: _____

Dependencia y grupo: _____

Objetivo:

Conocer los controles realizados a los administradores de sistemas de información de la Policía Nacional cuando acceden a las bases de datos, con el propósito de diseñar la estructuración de un grupo de Ciberseguridad en la Oficina de Telemática.

Preguntas:

1. ¿Qué sistema de información administra?
   _____
2. ¿Qué procedimiento realizó para que le fuese asignado el usuario con altos privilegios?
   _____
   _____
3. ¿Cada cuánto tiempo son renovados esos permisos y qué debe hacer para continuar con los privilegios?
   _____
   _____
4. ¿Informa a su jefe inmediato o en su defecto al grupo de seguridad de la información de la oficina cuando accede al sistema y manipula los datos?
   _____
   _____
5. ¿Cuál cree usted, que sería el impacto negativo que sufriría la institución, si un administrador de sistemas de información afecta la integridad y calidad de los datos almacenados?
   _____
   _____
   _____
6. ¿Según su punto de vista y profesionalismo como ingeniero de sistemas, se debería controlar y monitorear la gestión realizada desde el ciberespacio (cualquier lugar con acceso a los sistemas de información) a los administradores con altos privilegios?, ¿por qué?
   _____
   _____

Muchas gracias por participar en esta entrevista.

Ilustración 1 Entrevista a los administradores de sistemas de información

Fuente. Elaboración propia.

- Los usuarios de altos privilegios se entregan a través de una solicitud que se hace por medio de un sistema de información, siendo validado y aprobado por el jefe inmediato. Este procedimiento se hace una única vez mientras la permanencia en el cargo del funcionario.

- Estos usuarios en general, no informan a sus jefes inmediatos o al Grupo de Seguridad de la Información, los cambios realizados a los datos almacenados. Solo en ocasiones de implementar en producción un nuevo formulario, se solicita Comité de control de cambios, quienes aprueban o no el nuevo desarrollo.

- Para los administradores, el impacto negativo que sufriría la Institución si se afectara la data almacenada, se convertiría en un problema jurídico teniendo en cuenta la ley de protección de datos entre otras; así mismo, se perdería la credibilidad institucional y la integridad en todos los procesos administrativos ejecutados desde los sistemas de información.

- Que se ejerza un control desde el ciberespacio, es considerado necesario para que el cumplimiento de sus funciones sea transparente; evitaría que fuesen susceptibles a actos de corrupción, o que puedan llegar a proceder bajo amenaza.

En conclusión, los administradores de sistemas de información,consideran pertinente que haya una modificación a la estructura interna de la Oficina de Telemática de la Policía Nacional de Colombia, donde se creé el Grupo de Ciberseguridad, con el fin de garantizar la calidad de los datos y la integridad de los mismos; así evitarle o prevenir a la institución de tener situaciones penales, jurídicas o administrativas que puedan generar demandas millonarias y que la Institución repita contra el funcionario que cometió el hecho punible.

Así mismo, se le aplico la siguiente entrevista al personal del Grupo de Seguridad de la Información opinando lo siguiente:

Bogotá: 15-09-2018

Nombre del entrevistado: _____

Dependencia y grupo: _____

Objetivo:

Conocer los controles realizados a los administradores de sistemas de información de la Policía Nacional cuando acceden a las bases de datos, con el propósito de diseñar la estructuración de un grupo de Ciberseguridad en la Oficina de Telemática.

Preguntas:

1. **¿Qué función cumple en la Oficina de Telemática?**
   _____
   _____
2. **¿Qué controles se realizan desde este grupo a los administradores de sistemas de información?**
   _____
   _____
3. **¿hay control, cuando los usuarios con altos privilegios acceden desde el ciberespacio y manipulan la información?**
   _____
   _____
4. **¿Desde el grupo de seguridad de la información, que funciones tiene asignadas, para garantizar la ciberseguridad en la calidad e integridad de los datos almacenados desde los sistemas de información que son custodiados por la Oficina de Telemática?**
   _____
   _____
   _____
5. **¿Cuál cree usted, que sería el impacto negativo que sufriría la institución, si un administrador de sistemas de información afecta la integridad y calidad de los datos almacenados?**
   _____
   _____
   _____
6. **¿Considera necesario la creación de un grupo de Ciberseguridad en la Oficina de Telemática, enfocado a monitorear y controlar los accesos realizados por los usuarios con altos privilegios a las bases de datos?, ¿por qué?**
   _____
   _____
   _____

Muchas gracias por participar en esta entrevista.

Ilustración 2 Entrevista al personal del Grupo de Seguridad de la información

Fuente. Elaboración propia.

- Los controles realizados a los administradores de sistemas de información son muy débiles y reactivos, solo cuando se tiene algún indicio de movimientos incorrectos, se empieza a revisar la trazabilidad de la información, siendo conscientes que el mismo administrador sabe que puede eliminar la trazabilidad generada por la transacción.

- Desde el ciberespacio no son controladas las transacciones realizadas por los usuarios de altos privilegios, quienes a través de VPN pueden ingresar a la red interna de la Institución y manipular todos los datos almacenados desde los sistemas de información en las bases de datos, sin ser auditados ni controlados.

- El impacto negativo que sufriría la Institución, al momento de que sea vulnerada la calidad e integridad de los datos, sería un daño catastrófico en las bases de datos y afectaría directamente a la misión institucional del Estado, como lo es la convivencia y seguridad ciudadana.

- La creación de un Grupo de Ciberseguridad enfocado a controlar los usuarios de altos privilegios, es considerada muy necesaria en la Policía Nacional, teniendo en cuenta la cantidad, complejidad y sensibilidad de la información a la que tienen acceso estos usuarios.

El grupo de Seguridad de la Información de la Oficina de Telemática, señala como imperiosa necesidad la creación del Grupo de Ciberseguridad, dejando claro que, si existe esta amenaza y en el momento que se llegue a materializar, podría ocasionar bastante daño a la institución y sus empleados, tanto así, que se puede considerar un problema de Estado, en el momento que se vulnere la información almacenada desde estos sistemas.

La investigación, para conocer como desarrollan estos controles en otras instituciones, fue diseñada otra encuesta orientada al área de seguridad de la empresa Pública de Medellin

(EPM) para determinar si hay control desde el ciberespacio a los administradores técnicos de sistemas de información y este fue el resultado de la encuesta.

Nombre del entrevistado: _____

Empresa: _____

Área o grupo de trabajo: _____

Objetivo: conocer los controles realizados a los administradores técnicos de sistemas de información de la empresa.

Preguntas:

1. ¿Qué función cumple en la empresa?
   _____
   _____
2. ¿Qué controles se realizan a los administradores técnicos de sistemas de información?
   _____
   _____
   _____
3. ¿Hay controles desde el ciberespacio (casa, trabajo u otros lugares), se puede conocer las transacciones que un administrador técnico realice en las bases de datos de las aplicaciones?
   _____
   _____
   _____
4. ¿Los administradores técnicos de las aplicaciones pueden eliminar registros de las tablas de auditoría, que control se realiza al respecto?
   _____
   _____
   _____
5. ¿Existe algún grupo encargado de la ciberseguridad en su empresa aplicado a controlar la gestión realizada por los administradores técnicos de sistemas de información?
   _____
   _____
   _____
6. Si es afirmativo, ¿Qué controles realizan a los administradores de sistemas de información, para garantizar la ciberseguridad en la integridad y calidad del dato?
   _____
   _____
   _____
   _____
   _____
7. Si es negativo, ¿Considera necesario la creación de un grupo de ciberseguridad que controle y monitoree la gestión realizada por los administradores técnicos de sistemas de información?
   _____

   Muchas gracias por participar en la entrevista.

Ilustración 3 Entrevista al personal del Área de Seguridad de la información del grupo EPM

Fuente. Elaboración propia.

- Los controles que se realizan por parte del Área de seguridad de la información en el grupo EPM es mínimo, teniendo en cuenta que son minimos los privilegios que tienen los administradores de sistemas de información.

- Los controles que se tienen son Logs de auditoria, por lo tanto se puede percibir que son reactivos más no preventivos, solo cuando se genere alguna alerta se verifican estos Logs.

- Se esta implementando el proyecto Centinela, con el cual van a agregar unas funciones de Ciberseguridad.

- Los controles que realizan es la gestión de privilegios.

- Consideran que el monitoreo y control lo debe hacer cada dueño de proceso, teniendo en cuenta las tres líneas de defensa del control.

El Estado colombiano encabeza del Ministerio de Defensa, vió la necesidad de crear el Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional de Colombia CSIRT-PONAL bajo la responsabilidad de la Oficina de Telemática de la Policía Nacional; un grupo encargado de atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones (Chicano Tejada, 2014).

El Gobierno participa como parte interesada en varios papeles, procesa información altamente sensible para el país: de sus ciudadanos y de los sectores de seguridad pública (finanzas, defensa, salud y educación, entre otros). Debido a la importancia de la

información que maneja, el Gobierno necesita mantener sus sistemas seguros y suele ser el principal "cliente" de un CSIRT nacional ya que puede ser víctima de un ataque que tendría consecuencias potencialmente graves (Organización de los Estados Americanos OEA, 2015).

El CSIRT de la Policía Nacional de Colombia está bajo la dirección y control de la Oficina de Telemática según la Resolución número 02536 de 08 de julio de 2013 "Por la cual se define la estructura orgánica interna de la Oficina de Telemática, se determinan sus funciones y se derogan unas disposiciones" (Policía Nacional de Colombia, 2013). A esta fecha el CSIRT cuenta con tres grupos encargados de velar por el cumplimiento de la Resolución número 08310 de 28 dic 2016 "Por la cual se expide el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional de Colombia", así:

Tabla 1 Área de Seguridad

Funciones del Grupo CSIRT, Seguridad de la Información y Continuidad de la Información
1. Grupo Continuidad de la Información: es la dependencia de la Coordinación Enlace de Telemática, encargada de supervisar el desarrollo, implementación, mantenimiento y actualización de la calidad, el ciclo de vida y continuidad de la información en la Policía Nacional de Colombia, cumplirá las siguientes funciones entre otras:
• Garantizar la conservación de la memoria digital de la Institución para que la información cumpla las características de calidad, exactitud, totalidad, oportunidad y continuidad.
• Definir la metodología para adoptar las mejores prácticas del ciclo de vida de la información alineada a los objetivos de tecnología de la información y los de la Policía Nacional de Colombia.

- Realizar monitoreo de la herramienta de disponibilidad, para optimizar los recursos de la red, servidores y canales de datos.

- Clasificar, diseñar e implantar la gestión de datos informáticos de la institución, para facilitar el acceso y búsqueda de la información.

2. Grupo Seguridad de la Información: es la dependencia de la Coordinación Enlace de Telemática, encargada de proteger la disponibilidad, confidencialidad e integridad de las tecnologías de la información, cumplirá las siguientes funciones entre otras:

- Supervisar los lineamientos y políticas de seguridad de la información institucional, de acuerdo a su clasificación, con el fin de cumplir los estándares y buenas prácticas para el cumplimiento con las regulaciones que apliquen a la institución.

- Supervisar el cumplimiento de las políticas de implementación, configuración y operación de los controles de seguridad de la información existentes.
- Realizar administración de identidades y controles de acceso a sistemas de información y aplicaciones, para que se cumplan las políticas de control de acceso.
- Aplicar controles de seguridad de la información, para garantizar su confidencialidad, integridad y disponibilidad, con el fin de minimizar el riesgo de pérdida, fuga o modificación de la información.

3. Grupo de Respuesta a Incidentes de Seguridad: es la dependencia de la Coordinación Enlace de Telemática, encargada de la atención a incidentes informáticos de la Policía Nacional de Colombia, cumplirá las siguientes funciones entre otras:

- Detectar, reportar y solucionar, vulnerabilidades, amenazas e incidentes informáticos que afecten la disponibilidad, integridad y confidencialidad de la información en la Policía Nacional de Colombia a su vez verificar, monitorear y auditar la plataforma de antivirus de la Policía Nacional de Colombia, generando reportes, estadísticas y control sobre su licenciamiento.
- Realizar la difusión, concientización y prevención de las políticas de seguridad de la información.
- Alertar y advertir los incidentes de seguridad de la información, para mantener informado a las unidades de la Policía Nacional de Colombia.

Fuente. Recuperado de "estructura orgánica interna de la Oficina de Telemática en la Policía Nacional de Colombia".

Teniendo en cuenta las funciones de los tres grupos del CSIRT según la Resolución 02536, es deber del Grupo Seguridad de la Información, velar por la integridad de la información de los sistemas de información, función que hasta el momento se está cumpliendo; pero desde el ciberespacio y referente a la ciberseguridad no está dentro de sus funciones ni las de ningún grupo existente en la actualidad vigilar y controlar el riesgo que puede afectar la integridad de la información. En este sentido, la creación del Grupo de Ciberseguridad, mitigaría en un alto porcentaje la probabilidad de ocurrencia de este riesgo y si llegase a materializar, generaría las alertas necesarias para contrarrestar este delito (K Newmeyer, E Cubeiro, 2015).

Es importante mencionar que el Gobierno Nacional también creo El Centro Cibernético Policial (CCP), que está encargado de la ciberseguridad del territorio colombiano, su misión es ofrecer información, apoyo y protección ante los delitos cibernéticos, desarrolla labores de prevención, atención, investigación y la respectiva judicialización de los delitos

informáticos en el país, a través de su página web debe informar con frecuencia sobre vulnerabilidades cibernéticas detectadas. Asimismo, debe recibir y atender los lineamientos nacionales en ciberseguridad, trabajando coordinadamente con El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Asobancaria, 2018).

La Policía Nacional de Colombia designará el equipo que conformará el Centro Cibernético Policial, el cual estará encargado de dar respuesta operativa a los delitos cibernéticos. Para su operación, el CCP incorporará en su estructura el Comando de Atención Inmediata Virtual - CAI Virtual, un grupo de prevención, uno de gestión de incidentes y otro de investigación; tendrá la labor de gestionar todos los reportes de delitos cibernéticos dando una clasificación a las conductas delictivas encontradas, asimismo puede recibir solicitudes de cursos, charlas o visitas para trasmitir temas de seguridad (Departamento Nacional de Planeacion, 2011).

Teniendo en cuenta estos equipos creados para garantizar la seguridad de la información de las empresas públicas, además de otros que tienen las Fuerzas Militares, cabe mencionar también que la empresa privada cuenta con equipos para la protección de sus activos de información sin desconocer que es deber del Estado garantizar que todos los colombianos convivan en paz, las autoridades de la República están constituidas para proteger en su honra y bienes a los habitantes del territorio colombiano (Colombia, 1991); así como las amenazas de los ciberdelincuentes.

Los ataques cibernéticos se pueden presentar de diferentes formas y para llegar a perpetrarlos se pueden valer de ingeniería social, phishing, acceso no autorizado, spear phishing entre otros; asimismo, trabajadores descontentos o mal intencionados también pueden hacer parte de esta cadena de ciberdelincuentes. Tener el control total del trabajo realizado por nuestros empleados y más aún por aquellos que tienen cargos neurálgicos en la empresa, hace parte de las medidas de protección que debemos tener (Organización de los Estados Americanos OEA, 2015).

La Policía Nacional de Colombia es una empresa del Estado que provee seguridad a nivel nacional, también cuenta con bases de datos y sistemas de información que tienen datos de carácter personal y sensible, motivo por el cual debe contar con las herramientas necesarias y personal idóneo que tengan la misión de velar por la integridad de la información, así como evitar la fuga de cualquier dato relevante para la continuidad del negocio (Tejena-Macías, 2018).

9. Marcos de referencia

En esta fase de la investigación, se darán a conocer algunos conceptos que permiten entender mejor el tema abordado. Relativamente pueden parecer nuevos, pero su origen está basado en la dinámica del avance que a diario tienen los sistemas; así mismo, se citarán algunas teorías que apoyan la investigación en mención y que hacen aportes significativos a la evolución e implementación de los sistemas de información para las organizaciones.

Para concluir, y bajo un enfoque metodológico cualitativo, que relaciona las variables del problema de investigación e involucra la recolección de datos a través de entrevistas personales y encuestas aplicadas a los funcionarios administradores de sistemas de información y personal del Grupo de Seguridad de la Información de la Oficina de Telemática de la Dirección General de la Policía Nacional de Colombia, que cuentan con el perfil y las competencias en el área.

La información obtenida permitió conocer un contexto real de la importancia que tienen los sistemas de información para esa Institución y los problemas reales que se puedan generar al momento de que, a través del ciberespacio, se pueda materializar una amenaza a la integridad de los sistemas de información de la Institución (Martínez, Higuera, & Aguilar, 2013).

9.1. Marco conceptual y teórico

Las organizaciones públicas o privadas implementan políticas de seguridad informática con el fin de proteger su información, muchas organizaciones tienen como enfoque principal la política de seguridad de la información reforzando los comportamientos indeseables que afectan la seguridad; se considera que la generación y/o obtención de información tiene como fin aumentar/mejorar el conocimiento del usuario, o dicho de otra manera reducir la incertidumbre existente sobre un conjunto de alternativas lógicamente posibles; además de proporcionar a quien toma decisiones, la materia prima fundamental para el desarrollo de

soluciones y la elección de tener una serie de reglas de evaluación y reglas de decisión para fines de control (Bernal, 2010).

La importancia del sistema de información en las organizaciones radica en el contexto global en el que se desenvuelven y que les permiten obtener ventajas competitivas como: información confiable, verídica, optimizando recursos y permitiendo realizar un análisis correcto de la información, lo cual conlleva a reducir costos y mejorar procesos y procedimientos (Vargas García, 2015).

Asimismo, los sistemas de información apoyan al proceso de innovación de productos y procesos dentro de una empresa, buscando ventajas. Los sistemas de información para obtener ventajas competitivas deben adaptarse rápidamente a los cambios y a las necesidades de las organizaciones teniendo en cuenta la velocidad que la tecnología a diario contempla, sin desconocer los riesgos y amenazas que consigo trae (Tello, Alberto, & Velasco, 2016).

Sin embargo, analizando algunos estudios que han realizado empresas como Google, Amazon, Intel Security; llegan a la misma conclusión, considerando al ser humano (empleados) como el principal factor en la seguridad de la información, no solo desde una perspectiva tecnológica se debe pretender el cumplimiento de los controles de seguridad establecidos por la empresa, ya que quedaría incompleto y no garantizaría la integridad, confiabilidad y disponibilidad de la información. La tecnología y los sistemas de información no pueden garantizar un entorno totalmente seguro de los datos, de su integridad y calidad, desconociendo la manipulación de la información por parte de quienes tienen acceso y privilegios autorizados por la empresa y con los controles exigidos(Neira & Spohr, 2010).

Desarrollar e implementar políticas de seguridad, para garantizar los pilares de la información es vital en una organización, pues de allí depende la continuidad de la misma, sus recursos y ganancias, además de su buena imagen; esas políticas, deben estar enfocadas

a mitigar los riesgos operacionales asociados con el uso exponencial que se les da a los sistemas de información dentro de la empresa (Tejena-Macías, 2018).

Teniendo en cuenta lo anterior, es viable reconocer que existe una considerable participación humana, a parte de los diferentes controles que en el momento se practican a través de los mismos sistemas; este factor humano con relación a los sistemas de información y su seguridad, según los expertos, está directamente relacionado con el conocimiento y comportamiento de cada ser; es así que, se considera a los humanos como el eslabón más débil de la cadena en todo los temas relacionados con la seguridad de la información e incidentes de seguridad (Cortés Borrero, 2015).

Al transcurrir del tiempo, los investigadores se dedicaron a estudiaron el cumplimiento y resultados de las políticas en la seguridad de la información mediante la aplicación de teorías; es así que, el valor científico de la teoría general de sistemas únicamente depende de la generalización de aquellas propiedades comunes que tienen los sistemas. Esta teoría fue fundamentada como un movimiento científico importante en la biología y la física. A esta teoría, aplican también otras teorías las cuales están orientadas a estudiar el comportamiento humano y la forma como las personas toman decisiones, citando por ejemplo: la teoría de la disuasión general, la del comportamiento planificado y la teoría de la elección racional entre otras, las cuales, asocian las falencias de la seguridad de la información en los sistemas, directamente con la conducta de quien los administra y tiene los permisos y roles necesarios para acceder a los datos y cometer acciones no siempre con fines profesinales sin poder ser controlado y monitoreado (Von, 1976).

Asimismo, la teoría del comportamiento planificado planteada por Ajzen (Ajzen, La teoría del Comportamiento Planificado, 2014), hace referencia a que el comportamiento individual es directamente afectado por la actitud, el control cognitivo percibido y las normas subjetivas. Esta clase de teoría está vinculada con los sistemas de información, teniendo en cuenta que dichos sistemas son administrados por personas y muchas veces depende de su comportamiento el cumplimiento de las políticas de seguridad de la entidad.

Existe otra teoría, con énfasis en los procesos cognitivos que median en el cambio del comportamiento, como lo es la teoría de protección de motivación de la Universidad de Puerto Rico (2009), la cual propone que la intención de proteger a uno mismo depende de cuatro factores, así:

1. La percepción de la gravedad en un evento de amenaza, para nuestro caso y a modo de ejemplo una denegación de servicios.

2. La probabilidad percibida de la aparición o vulnerabilidad, como ejemplo cuando el usuario se da cuenta que está siendo atacado.

3. La eficacia de la conducta preventiva recomendada, es la aplicación de todos los protocolos de seguridad ya establecidos por la entidad para garantizar la disponibilidad, integridad y confidencialidad de la información.

4. La percepción de autoeficacia, hace referencia a la confianza generada luego de poner en práctica los protocolos de seguridad establecidos, y tener la capacidad de darle continuidad al negocio aplicando los comportamientos preventivos reglamentados (Universidad de Puerto Rico, 2009).

A nivel de sistemas de información, hay que mencionar la Teoría General de Sistemas, que trata de una concepción estructurada o metodología teniendo como propósito principal estudiar el sistema como un todo, la base son sus componentes, analizando las relaciones e interrelaciones existentes entre éstas, aplicando estrategias científicas, conduciendo al entendimiento globalizante y generalizado de los sistemas. A esta teoría, aplica la Metodología General de Sistemas, la cual reúne los elementos necesarios para difundir y hacer extensiva su aplicación, esta metodología permite la creación de modelos para pronosticar el comportamiento antes de su puesta en marcha mediante la aplicación de procesos de simulación, así permitir la selección de la mejor alternativa o solución a la problemática en estudio (Niemimaa, 2017).

Boulding, concibió dos posibles enfoques para la Teoría General de Sistemas, los cuales son ampliados de la siguiente forma por Oscar J. Bertoglio (1994):

> El primer enfoque es observar el universo empírico y escoger ciertos fenómenos generales que se encuentran en las diferentes disciplinas y tratar de construir un modelo teórico que sea relevante para esos fenómenos. Este método, en vez de estudiar sistema tras sistema, considera un conjunto de todos los sistemas concebibles (en los que se manifiesta el fenómeno general en cuestión) y busca reducirlo a un conjunto de un tamaño más razonable.
>
> Un segundo enfoque posible para la Teoría General de Sistemas es ordenar los campos empíricos en una jerarquía de acuerdo con la complejidad de la organización de sus individuos básicos o unidades de conducta y tratar de desarrollar un nivel de abstracción apropiado a cada uno de ellos. Este es un enfoque más sistemático que el anterior y conduce a lo que se ha denominado Un Sistema de Sistemas" (Bertoglio, 1994).

Teniendo en cuenta lo anterior, debemos tener claro algunos conceptos básicos en el desarrollo de esta investigación como:

Atributo: características y propiedades estructurales y/o funcionales más a detalle de un sistema, como ejemplo en una base de datos, pueden ser los campos de una tabla con sus características (Enciso, 2018).

Elemento: en los sistemas se entiende como todas las partes o componentes que lo constituyen, se puede mencionar los objetos, procesos y procedimientos (Román, 2016).

Estructura: constituido por un gran número de partes, o subsistemas, que interaccionan unos a otros en grado diferente y cuya estructuración tiene una dimensión vertical y

horizontal buscando sinergia entre ellos para garantizar la escalabilidad e interoperabilidad (Sierra, Escobar, Gago, Navarro, & Rocha, 2007).

Información: es un conjunto de datos organizados, que constituye un mensaje sobre un cierto fenómeno o solicitud, este mensaje da significado a las cosas o requerimientos del sistema (González Longatt, 2007).

Modelo: son constructos diseñados por un observador que persigue identificar y medir relaciones sistémicas complejas. Todo sistema real tiene la posibilidad de ser representado en más de un modelo. La decisión, en este punto, depende tanto de los objetivos del modelador como de su capacidad para distinguir las relaciones relevantes con relación a dichos objetivos (Mankiw, 2012).

Seguridad de la información: persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada. Su finalidad es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización (L. Ramos, 2009).

Sinergia: es la cooperación de dos causas distintas que contribuye a generar el mismo resultado o dicho de otra manera es en consecuencia, un fenómeno que surge de las interacciones entre las partes o componentes de un sistema (Kenneth E. Kendall & Julie E. Kendall, 2011).

Sistemas ciberneticos: son aquellos que tienen a su disposición dispositivos internos de auto-comando o autorregulación que reaccionan ante los posibles cambios de información en el ambiente, diseñando respuestas versátiles que contribuyen al cumplimiento de los parámetros del sistema (Hernan, 2014).

Sistemas de información: es el conjunto de recursos de la compañía, que sirven como soporte para el proceso de captación, transformación y comunicación, este sistema debe

garantizar la seguridad de la información y además ser eficiente y efectivo para el cumplimiento de la misionalidad de la empresa (Vegas-Fernández, 2015).

9.2. Marco legal

El proyecto de investigación está enmarcado con un enfoque sistémico, ya que el modo de abordar los objetos y fenómenos no puede ser aislado, sino que tiene que verse como parte de un todo (EcuRed contributors, 2019). El cumplimiento de los lineamientos legales es necesarios y obligatorios, con el fin de no infringir las disposiciones legales en materia de seguridad de la información y protección de datos y fuera del mismo como son los tratados internacionales; a continuación, se mencionarán algunas normas que fueron tomadas para la ejecución de esta investigación:

9.2.1. Normatividad internacional

- Convenio sobre Ciberdelincuencia14 del Consejo de Europa – CCC (conocido como en convenio sobre cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004. El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas (Consejo de Europa, 2001).

- Resolución AG/RES 2004 (XXXIV- O/04) de la Asamblea General de la Organización de los Estados Americanos. Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética.
  Estipula tres vías de acción (Departamento Nacional de Planeacion, 2011):

1. Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores - CSIRT. Este cometido fue asignado al Comité Interamericano Contra el Terrorismo - CICTE.

2. Identificación y adopción de normas técnicas para una arquitectura segura de Internet. Esta labor es desarrollada por la Comisión Interamericana de Telecomunicaciones.

3. Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas – REMJA (Organizacion de los Estados Americanos "OEA", 2004).

9.2.2. Normatividad nacional

- Ley 962 de 2005, "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados."

- 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 se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Por medio de esta ley, el Congreso de la República se enfocó a garantizar la confidencialidad, integridad, disponibilidad de los datos en los sistemas de información, tipificando nueve delitos que no estaban contemplados en el Código Penal según el Congreso de la República de Colombia (2009), así:

- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos (Congreso de la República de Colombia, 2009).

- Ley 1581 de 2012 Protección de Datos Personales: esta ley complementa la normatividad vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar información personal que es almacenada en las bases de datos o archivos; así mismo, el tratamiento para actualizar, modificar o eliminar los datos personales custodiados por alguna entidad de naturaleza pública o privada. Esta ley deja claro el concepto de dato personal, el cual se refiere a toda aquella información relacionada a una persona y que permite su identificación, como lo: es su documento de identificación, estado civil, lugar de nacimiento, estado de salud y demás aspectos de la persona (Congreso de la República de Colombia, 2012).

- Resolución 00937 del 10 de marzo 2016, "Por la cual se establece el Manual de funciones para el personal uniformado de la Policía Nacional de Colombia, la metodología de evaluación para el perfil de los cargos y se derogan unas disposiciones": en esta Resolución, se constituye en un instrumento de gerenciamiento del talento humano, al brindar elementos descriptivos de los cargos como: 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, mantenimiento de la seguridad y convivencia ciudadana (Oficina de Planeacion Policía Nacional de Colombia, 2016).

- Resolución 05309 del 24 de agosto 2016, "Por la cual se establecen las Tablas de Organización Policial (TOP) de la Policía Nacional de Colombia y se derogan unas disposiciones": estas tablas, son una herramienta mediante la cual se estandarizan las cantidades mínimas requeridas de personal en cada cargo asociado a la unidad, identificando la cantidad de vacantes y/o remanentes por dependencias y determinando las necesidades a nivel nacional. De igual forma, sirven para realizar el análisis sobre el crecimiento institucional y ejercer control sobre los movimientos de personal, estas Tablas de Organización Policial, se establecen a través del módulo de perfiles por cargos en el Sistema para la Administración del Talento Humano (Oficina de PLaneación Policía Nacional de Colombia, 2016).

- Resolución 08310 del 28 de diciembre 2016, "Por la cual se expide el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional de Colombia", este acto administrativo, es de cumplimiento para los funcionarios de la Policía Nacional de Colombia y personal externo que le proporcione algún bien o servicio; quienes están obligados a adoptar los parámetros aquí descritos y los controles adicionales que pueden implementar las diferentes unidades de acuerdo a su misionalidad. La política de Seguridad de la Información busca cubrir toda la información impresa o escrita en papel, recopilada electrónicamente en cualquier medio de almacenamiento actual o futuro, transmitida a través de medio electrónico actual o futuro; mostrada en videos o hablados, y todo lo considerado información de carácter institucional que se convierte en activos de información (Policía Nacional de Colombia, 2016).

- CONPES 3701: documento aprobado en 2011, para 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. Se identificó, que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presentas grandes debilidades y existen algunas iniciativas gubernamentales, privadas y civiles que buscan contrarrestar este flagelo, propone mesas de trabajo para coordinar acciones específicas de impacto contra los ciberdelitos (Departamento Nacional de Planeacion, 2011).

- CONPES 3854: aprobado en 2016, hace referencia al posicionamiento que tiene el país, con relación a la lucha contra el cibercrimen, pero deja muy claro que se ha dejado de lado la gestión del riesgo en el entorno digital; destaca que la política nacional de seguridad digital, debe involucrar activamente todas las partes interesadas y asegurar una responsabilidad compartida entre las mismas. Queda en poder del Ministerio de Justicia, definir los lineamientos que faciliten los ajustes requeridos en el marco legal y regulatorio, adecuándolo a las necesidades como análisis, anticipación, prevención, detección, atención e investigación de delitos cibernéticos (Departamento Nacional de Planeacion, 2016).

10. Diseño del Grupo de Ciberseguridad

En la Policía Nacional de Colombia, el rediseño organizacional está articulado a una estructura basada en procesos y tiene en cuenta el relacionamiento institucional, por cuanto se hace necesario que los factores para la creación de un grupo dentro de una unidad policial, cuente con las validaciones y el cumplimiento del protocolo establecido en la Directiva Administrativa Permanente 011 "Parámetros para la elaboración de propuesta de reestructuración orgánica de las dependencias de la Policía Nacional de Colombia".

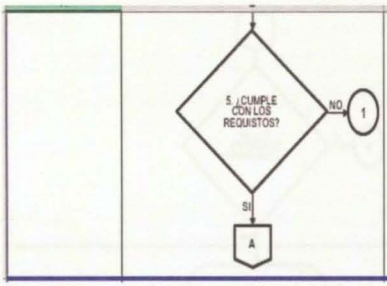
Igualmente está establecido un procedimiento (ver ilustración 1), que fue seguido paso a paso para los fines que la investigación propuso. A continuación se explica cada uno y el requerimiento que se cumplió por parte del investigador.

Código: 105-PR-0022 Fecha: 07-05-2019 Versión: 8	DIRECCIONAMIENTO DEL SISTEMA GESTIÓN INTEGRAL FORMULAR EL REDISEÑO ORGANIZACIONAL DE LAS DEPENDENCIAS INTERNAS DE LA POLICÍA NACIONAL	POLICÍA NACIONAL

OBJETIVO: Formular y mantener la estructura orgánica interna de la Policía Nacional, que permita su funcionalidad y así mismo cumpla con los requerimientos establecidos por el Departamento Administrativo de la Función Pública (DAFP).

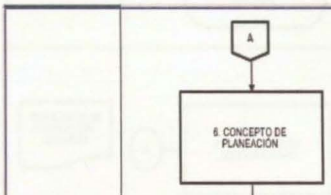
ALCANCE: Valorar y conceptuar la información remitida por las unidades policiales, con el fin de definir o rediseñar la estructura orgánica de las mismas.

DOCUMENTO ENTRADA	TAREA	DOCUMENTO SALIDA	DESCRIPCIÓN	CARGO DEL RESPONSABLE	PUNTO DE CONTROL	DOCUMENTO ASOCIADO	FUNDAMENTO LEGAL
	1. JUSTIFICACIÓN DE LA NECESIDAD	COMUNICACIÓN OFICIAL	La unidad policial justifica la necesidad ante el dueño del proceso, con apoyado por parte de la Región de Policía. Para las Direcciones, Oficina Asesoras, deberá ir dirigido al Jefe de la Oficina de Planeación OFPLA.	Directores. Jefes Oficinas Asesoras. Comandantes de Unidad.		Mapa de Procesos Institucional. Guía de rediseño Institucional de Entidades Públicas del Departamento Administrativo de la Función Pública. Directiva Administrativa Permanente 011 del 28 de abril 2010 "Parámetros para la elaboración de propuestas de reestructuración orgánica de las dependencias de la Policía Nacional" Resolución 03622 del 11 de julio de 2018 "Por medio de la cual se deroga la Resolución 00208 del 25 de enero de 2016 "Por la cual se actualiza el manual unico de gestión documental para la Policía Nacional" Resoluciones de estructura orgánica de las direciones y oficinas asesoras, donde se fijan parámetros para sus unidades desconcentradas y afines a su misionalidad.	Decreto 4222 del 23/11/2006 "Por el cual se modifica parcialmente la Estructura del Ministerio de Defensa Nacional". Acuerdo 004 del 15 de marzo de 2013"Por el cual se reglameta parcialmete los Decretos 2576 y 2609 y se modifica el procedimieto para la elaboracion presentación, evaluación, aprobación, implemetación de las tablas de retecion documetal y las tablas de valoracion documetal". Manual del Sistema de Gestión Integral. Mini-Manual 04 tablas retencion documental y transferencias documentales del Archivo General de la Nacion. Circular externa 003 del 27 de feberode 2015 directrices para la elaboracion de tablas de retencion documental.
COMUNICACIÓN OFICIAL CORREO CONVOCANDO MESA DE TRABAJO	2. MESA DE TRABAJO	ACTA REUNIÓN DE TRABAJO	Se profundiza en la necesidad planteada por la Unidad, al igual se actura y comprenden ideas sobre la propuesta. Debe asistir: Analista de Planeación Institucional con rol de rediseño organizacional, responsable de planeación dueño de proceso, Analista Ocupacional de DITAH y Asesor Jurídico SEGEN.	Jefe Oficina de Planeación. Jefe Gestión Institucional. Analista de Planeación Institucional con el rol de Rediseño Organizacional. Responsable de Planeación Dueño de Proceso.			
	3. ¿APROBACIÓN DE LA NECESIDAD?	COMUNICADO OFICIAL	Teniendo en cuenta los resultados obtenidos en la mesa de trabajo, si no es viable se informa a la unidad a través de comunicado oficial. Al ser viable se continúa con el procedimiento.	Jefe Oficina de Planeación. Jefe Gestión Institucional. Analista de Planeación Institucional con el rol de Rediseño Organizacional.			
REQUERIMIENTO O SOLICITUD	1 → 4. RECEPCIONAR Y VERIFICAR LA DOCUMENTACIÓN		La unidad previo a la presentación del requerimiento debe tener concepto de infraestructura (DIRAF), estudio de vulnerabilidad (DIPOL) y concepto del dueño del proceso, en los casos que sea necesario. Se recepciona la solicitud, verificando que contenga como documentos anexos: el estudio de planeación, el proyecto de resolución, organigrama actual y propuesto de la estructura, listado de cargos y perfiles, tabla de organización policial, proyecto tabla de retención documental. Los cuales deben cumplir con el trámite y lo establecido en la Directiva Administrativa Permanente 011 del 280410 "Parámetros para la elaboración de propuestas de reestructuración orgánica de las dependencias de la Policía Nacional" y normas subsiguientes que la deroguen, modifiquen o adicionen.	Analista de Planeación Institucional con rol de rediseño organizacional.	GUÉ: Aplicar preceptos establecidos en la Guía de Modernización de Entidades Públicas del Departamento Administrativo de la Función Pública. Lineamientos establecidos en la Directiva Administrativa Permanente 011 del 280410 "Parámetros para la elaboración de propuestas de reestructuración orgánica de las dependencias de la Policía Nacional". QUIÉN: Analista Planeación Institucional con rol de rediseño organizacional. CUÁNDO: Cada vez que recepciona una solicitud de rediseño organizacional. EVIDENCIA: Comunicacion Oficial donde se cierre requerimiento o solicitud.	



Si no cumple con todos los requisitos, se emana comunicación oficial solicitando a la unidad respectiva allegar el o los documentos faltantes, hasta tanto no cumpla con el requerimiento, no se continúa con el trámite.

Jefe Oficina de Planeación.
Jefe Grupo Gestión Institucional.
Analista Planeación Institucional.



CONCEPTO OFICINA DE PLANEACIÓN

La Oficina de Planeación emite concepto de favorabilidad o no favorabilidad, teniendo en cuenta los lineamientos institucionales para el rediseño organizacional de las dependencias internas.

Dicho concepto se emitirá a través de un comunicado oficial en un término no mayor a 20 días hábiles, una vez sean recepcionados todos los documentos requeridos.

Jefe Oficina de Planeación.
Jefe Grupo Gestión Institucional.
Analista Planeación Institucional (Rol de Rediseño, Procesos, Riesgos y Gastos de Funcionamiento o quienes hagan sus veces).

QUÉ: Verificar que la propuesta de creación, modificación o deroguación de la estructura orgánica de dicha unidad no afecte los procesos o procedimientos estandarizados.

QUIÉN: Jefe Grupo Gestión Institucional, Analista Planeación Institucional (rol de rediseño, procesos, riesgos y gastos de funcionamiento o quiene haga sus veces).

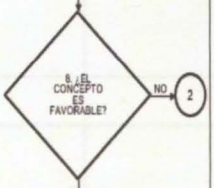
CUÁNDO: cada vez que se solicite emitir concepto sobre rediseño organizacional

EVIDENCIA: concepto de planeación.

Se elabora comunicación oficial suscrita por el Jefe de la Oficina de Planeación, donde se remiten los documentos y el concepto de planeación sobre la estructura propuesta a la Dirección de Talento Humano.

Para que de acuerdo a su misionalidad se realice el análisis y revisión de los cargos, perfiles y tabla de organización policial, actividad desarrollada por el grupo de análisis ocupacional DITAH.

Jefe Oficina de Planeación.
Jefe Grupo Gestión Institucional.
Analista Planeación Institucional con rol de rediseño organizacional o quien haga sus veces.



CONCEPTO DITAH

Si es favorable la Dirección de Talento Humano emite concepto de validación de cargos, perfiles y tabla de organización policial.

De no ser favorable la Dirección de Talento Humano remite a la unidad interesada concepto, informando las inconsistencias encontradas, una vez subsanadas estas novedades se dará continuidad al trámite.

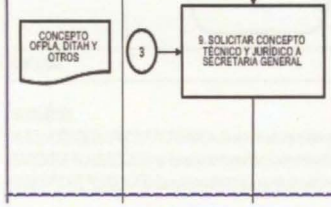
Director de Talento Humano.
Analista Ocupacional DITAH.

QUÉ: realizar la verificación de cargos, perfiles y tabla de organización policial y determinar que se cuente con el talento humano suficiente para dicha modificación.

QUIEN: Analista Ocupacional.

CUANDO: Cada vez que se solicite por parte de la Oficina de Planeación, emitir concepto del talento humano sobre cargos, perfiles y tabla de organización policial.

EVIDENCIA: Concepto



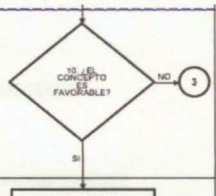
COMUNICACIÓN OFICIAL

CONCEPTO JURIDICO

Una vez DITAH emita concepto favorable y lo envié a OFPLA mediante comunicación oficial, el Jefe de la Oficina de Planeación genera una solicitud a SEGEN, para el análisis tecnico correspondiente a las Tablas de Retención Documental y el análisis jurídico del acto administrativo; remitiendo el estudio de planeación, proyecto de resolución, el concepto de planeación, concepto de talento humano y el proyecto de tablas de retención documental.

La revisión puede generar cambios de forma o de fondo.

Secretario General.
Jefe Área Jurídica de la Secretaría General.



Si la Secretaría General y la Oficina de Planeación sesionan a la unidad interesada, para que realice el ajuste al acto administrativo, de acuerdo con las sugerencias emitidas por la Secretaría General.

Si el concepto no es favorable, mediante comunicación oficial responden dar respuesta a la Unidad.

Responsable de Planeación Institucional delegado por la unidad interesada.

CONCEPTO TÉCNICO Y JURÍDICO SEGEN

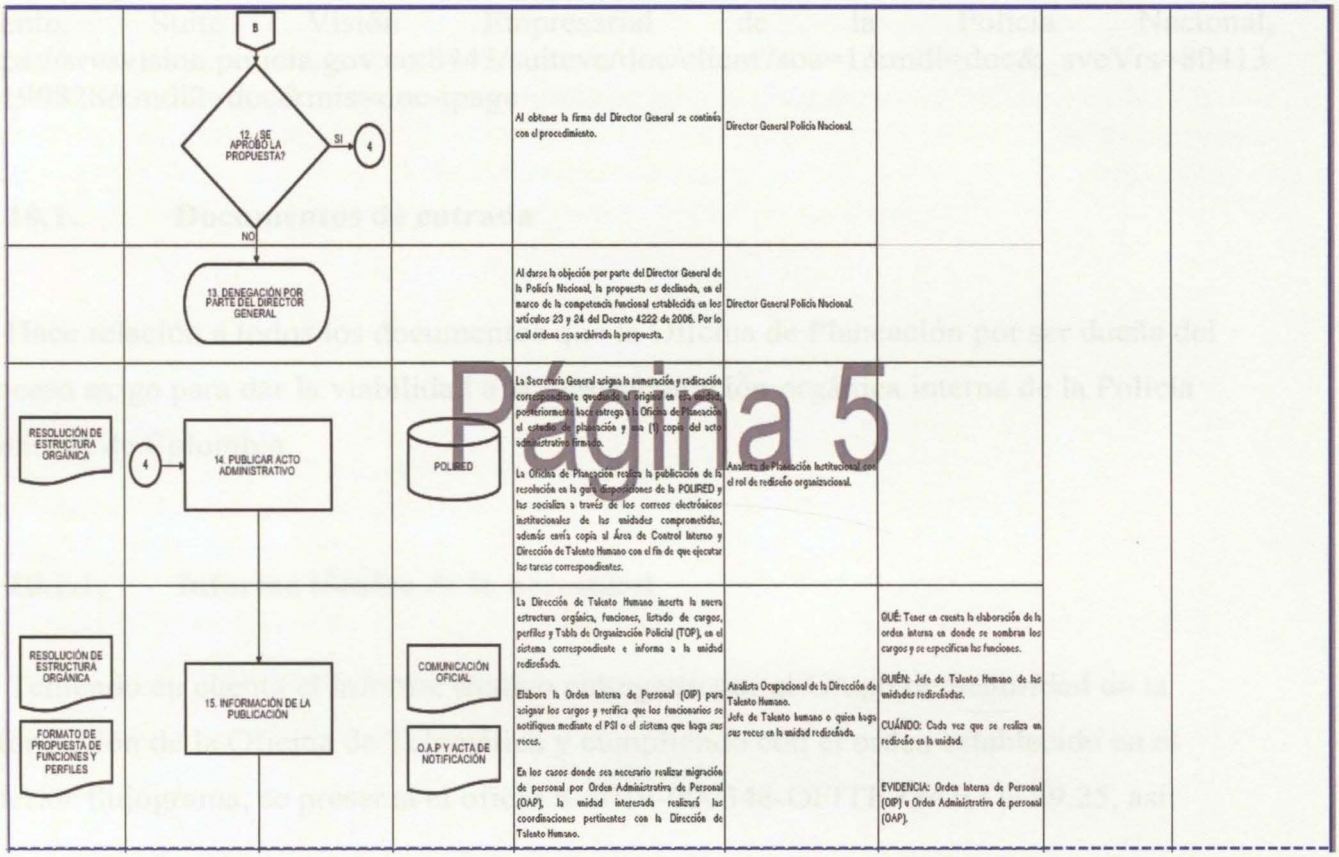
11. PRESENTAR EL PROYECTO FINAL DEL ACTO ADMINISTRATIVO AL DIRECTOR GENERAL PARA APROBACIÓN

B

RESOLUCIÓN DE ESTRUCTURA ORGÁNICA

La Secretaría General gestiona la obtención de la firma del acto administrativo por parte del Director General.

Secretario General.



ANEXOS:

GLOSARIO:

RESOLUCIÓN DE ESTRUCTURA ORGÁNICA: Es el acto administrativo por el cual el Director General, efectúa cambios estructurales a la organización, con fundamento en lo preceptuado en el Decreto 4222 de 2006 o normas subsiguientes que lo deroguen, modifiquen o adicionen.
ESTUDIO DE PLANEACIÓN: Es un documento formal que comprende el análisis conciso de una situación determinada y plantea alternativas de solución, donde se soportan y justifican todos los cambios que generará el rediseño.
CONCEPTO DE PLANEACIÓN: Documento formal que se emplea para emitir percepciones, significaciones o discernimientos basados en hechos, documentos, normas, reglamentos, estudios, entre otros, que permiten la toma de decisiones sobre temas específicos.

MODIFICADO POR:	REVISADO POR:	APROBADO POR:
MARÍA ALEJANDRA LOZANO RODRÍGUEZ Orientador de Defensa Subintendente **VILMER VILMER MOLANO HERNÁNDEZ** Analista Planeación Institucional	Teniente Coronel **ANDRÉS JAVIER PÉREZ FLÓREZ** Jefe Grupo Gestión Institucional	Brigadier General **RAMIRO ALBERTO RIVEROS ARÉVALO** Jefe Oficina de Planeación
FECHA: 17-04-2013	**FECHA: 22-04-2013**	**FECHA: 23-04-2013**

Ilustración 4. Procedimiento para Formular el Rediseño Organizacional de las Dependencias Internas de la Policía Nacional de Colombia.

Fuente. Suite Visión Empresarial de la Policía Nacional, https://srvsvision.policia.gov.co:8443/suiteve/doc/client?soa=1&mdl=doc&_sveVrs=80413 20190828&mdl2=doc&mis=doc-ipage

10.1. Documentos de entrada

Hace relación a todos los documentos que la Oficina de Planeación por ser dueña del proceso exige para dar la viabilidad a la reestructuración orgánica interna de la Policía Nacional de Colombia.

10.1.1. Informe técnico de la necesidad

Teniendo en cuenta el informe técnico entregado por el Grupo de Seguridad de la Información de la Oficina de Telemática y cumpliendo con el orden establecido en el anterior flujograma, se presenta el oficio S-2019-000348-OFITE-GARTE-29.25, así:

Bogotá D.C., 20 de diciembre del 2019

Brigadier General
CEIN CASTRO GUTIÉRREZ
Jefe Oficina de Telemática
Carrera 59 26 - 21
Bogotá D.C.

Asunto: solicitud mesa de trabajo para validar el proyecto de Grupo de Ciberseguridad de la Oficina de Telemática.

Respetuosamente comunico a mi General, que el Grupo de la Seguridad de la Información en cumplimiento de su carácter funcional de supervisión de los lineamientos y políticas de seguridad de la información institucional, identificó un factor de riesgo emanado del Grupo de la Administración Recursos Tecnológicos; debido a que en la actualidad, los administradores de sistemas de información cuentan con roles y usuarios de altos privilegios, los cuales no tienen ningún tipo de control al momento de acceder a los sistemas y poner en riesgo la calidad e integridad de los datos.

Por lo anteriormente expuesto, en el marco del rediseño organizacional se hace perentorio la creación de un grupo al interior de la Oficina de Telemática que se encargue monitorear y controlar la gestión realizada por los administradores de sistemas de información. En este entendido, solicito a mi General la validación de proyecto para iniciar el trámite contenido en la DAP 011 del 28042010 "*Parámetros para la elaboración de propuesta de reestructuración orgánica de las dependencias de la Policía Nacional*"

Atentamente,

Capitán **JOHN ALBEIRO GUEVARA PULIDO**
Jefe Grupo Seguridad de la Información

Se ofició al Director de esta Oficina Asesora, con el fin de poner en conocimiento el riesgo de ciberseguridad existente en el Grupo de Administración de Recursos Tecnológicos, que a futuro podría generar un riesgo en la materialización de una amenaza, que afectaría la calidad e integridad de los datos almacenados en los sistemas de información gestionados desde esta oficina asesora; razón por la cual el Director de la Oficina de Telemática, otorga la viabilidad mediante comunicado oficial S-2019-000350-OFITE-GARTE-29.25 al jefe del Grupo de Seguridad de la Información para que , en coordinación con el Grupo de Planeación, empiece el proyecto de rediseño organizacional de la estructura orgánica en la Oficina, así:

10.1.2. Viabilidad para la elaboración del proyecto

Bogotá D.C., 23 de diciembre del 2019

Capitán
JOHN ALBEIRO GUEVARA PULIDO
Jefe Grupo Seguridad de la Información
Carrera 59 26 - 21
Bogotá D.C.

Asunto: viabilidad para la elaboración del proyecto orientado a la creación del Grupo de Ciberseguridad de la Oficina de Telemática.

En atención al comunicado oficial S-2019-000348-OFITE, de manera atenta informo al señor Capitán, que se da la viabilidad correspondiente para que se hagan las diligencias necesarias en la elaboración y ejecución del proyecto para la creación de un Grupo de Ciberseguridad en la estructura orgánica interna de la Oficina de Telemática ante la Oficina de Planeación.

Atentamente,

Brigadier General **CEIN CASTRO GUTIÉRREZ**
Jefe Oficina de Telemática

Al obtener la viabilidad por parte del jefe de esta oficina asesora, se debe hacer un nuevo oficio de número S-2019-000352-OFITE -GARTE-29.25 dirigido al jefe de la Oficina de Planeación, solicitando una mesa de trabajo e incluyendo otras dependencias de la institución, así:

10.1.3. Solicitud mesa de trabajo

Bogotá D.C., 24 de diciembre del 2019

Brigadier General
RAMIRO ALBERTO RIVEROS ARÉVALO
Jefe Oficina de Planeación
Carrera 59 26 - 21
Bogotá D.C.

Asunto: solicitud mesa de trabajo

En atención a la comunicación oficial No. S-2019-000348-OFITE del 20 de diciembre del 2019, respetuosamente solicito al señor General, disponga la asistencia de los funcionarios de Estructuración Organizacional de la Oficina de Planeación, para que en el marco de lo establecido en el procedimiento 1DS - PR - 0022 " Formular el rediseño organizacional de

las dependencias internas de la Policía Nacional de Colombia", con el propósito de desarrollar la exposición de motivos correspondiente a la creación del Grupo de Ciberseguridad, a la mesa de trabajo conformada por Dirección de Talento Humano, Oficina de Planeación y Secretaría General, de acuerdo con la normatividad del procedimiento y el desarrollo de la propuesta.

Por lo anterior, la mesa de trabajo se llevará a cabo el día miércoles 26 de diciembre de 2019, a las 08:00 horas, en la sala de reuniones de COTEL, segundo piso de la Oficina de Telemática Dirección General.

Atentamente,

Brigadier General **CEÍN CASTRO GUTIÉRREZ**
Jefe Oficina de Telemática

Para asistir a esta mesa de trabajo, con las dependencias que hacen parte del protocolo establecido para proponer la modificación a la estructura interna de una dependencia, la primera tarea fue elaborar una presentación en la que se contextualizó la necesidad del Grupo de Ciberseguridad y el talento humano requerido en conformidad a lo establecido en la Resolución 05309 del 24 de agosto de 2016, "por la cual se establecen las Tablas de Organización Policial (TOP) de la Policía Nacional de Colombia y se derogan unas disposiciones".

Así mismo, la reorganización del espacio físico de la oficina, con el fin de ubicar las herramientas tecnológicas y enseres necesarios para poner en funcionamiento el Grupo de Ciberseguridad. Aunado a lo anterior, se debe ajustar con el responsable de gestión documental, para que se haga una reestructuración a la Tabla de Retención Documental (Dirección Policia Nacional de Colombia, 2016).

Tablas de Organización Policial (TOP), para el Grupo de Ciberseguridad

Tabla 2 Tabla de Ordenamiento Policial (TOP).

Ordenamiento	Sigla Papa	Sigla Fisica	Id Cargo	Id Perfil Cargo	Perfil	Consecutivo	Descripción Dependencia	Id Cargo Jefe
82	OFITE	OFITE	31712	6521	JEFE GRUPO CIBERSEGURIDAD	61999	GRUPO CIBERSEGURIDAD	30977
82	OFITE	OFITE	31713	6522	ANALISTA CIBERSEGURIDAD	61999	GRUPO CIBERSEGURIDAD	31712

Fuente. Elaboración propia

10.1.4. Solicitud recepción y revisión de documentación para la creación del Grupo de Ciberseguridad en la Oficina de Telemática.

Luego de realizar la mesa de trabajo con la Dirección de Talento Humano, Secretaría General y Oficina de Planeación, se debe obtener el concepto favorable de viabilidad al proyecto. Seguido a este procedimiento, se debe oficiar a la Oficina de Planeación, adjuntando los documentos establecidos en el procedimiento para la modificación de estructura dentro de la Policía Nacional de Colombia, así:

No. S-2020-000102-OFITE -GARTE-29.25

Bogotá D.C., 10 de enero del 2020

Brigadier General
RAMIRO ALBERTO RIVEROS ARÉVALO
Jefe Oficina de Planeación
Carrera 59 26 - 21
Bogotá D.C.

Asunto: solicitud recepción y revisión de documentación para la creación del Grupo de Ciberseguridad en OFITE.

En atención al proyecto para la creación del Grupo de Ciberseguridad en la Oficina de Telemática, el procedimiento 1DS - PR - 0022 "Formular el rediseño organizacional de las dependencias internas de la Policía Nacional de Colombia" y los resultados de la mesa de

trabajo llevada a cabo el día miércoles 26 de diciembre de 2019, en donde se emitió concepto de viabilidad al proyecto; de manera atenta me permito solicitar al señor Brigadier General ordenar a quien corresponda, la recepción y revisión formal de los documentos exigidos por el procedimiento con el fin de que se continúe con la ejecución del proyecto, en los términos que señala la normatividad vigente.

Atentamente,

Brigadier General **CEÍN CASTRO GUTIERREZ**
Jefe Oficina de Telemática

10.1.5. Cargos y responsabilidades:

En coordinación con el grupo de Planeación de la Dirección de Talento Humano de la Institución, se deben realizar las gestiones necesarias para la creación de los nuevos cargos y responsabilidades en el Sistema para la Administración del Talento Humano, los cuales deben cumplir con el protocolo establecido por la Institución en cumplimiento a este procedimiento se crearon los siguientes dos cargos así:

Jefe Grupo Ciberseguridad

El propósito principal debe ser supervisar y controlar, la calidad e integridad de los datos, registrados en los sistemas de información de la Policía Nacional de Colombia.

Funciones del cargo:

- Definir la metodología, procedimientos y controles, basados en las buenas prácticas de estándares internacionales para la inserción de datos en los sistemas de información institucional, garantizando la calidad de los datos.

- Establecer procedimientos y controles que garanticen la no alteración de la integridad de los datos institucionales, sin previa autorización y justificación por parte de los dueños de proceso.

- Diseñar, implementar y parametrizar las herramientas o desarrollos tecnológicos necesarios, para garantizar la no alteración a la calidad e integridad de los datos desde el ciberespacio.

- Gestionar convenios y acuerdos con entidades del Estado, empresas públicas, privadas y organismos internacionales, que permitan hacer alianzas estratégicas en ciberseguridad dando escalabilidad al procedimiento de gestión de la información en la Policía Nacional de Colombia.

Habilidades funcionales: (evaluación y desempeño)

Criterios de desempeño:

- Los procedimientos y controles sobre inserción de datos en los sistemas de información son definidos acordes a los protocolos.

- Los procedimientos y controles que garanticen la no alteración de la integridad de los datos institucionales, son establecidos con claridad.

- Las herramientas y desarrollos tecnológicos para garantizar la no alteración a la calidad e integridad de los datos desde el ciberespacio son diseñadas con calidad.

- Los convenios y acuerdos con entidades públicas, privadas y organismos internacionales en ciberseguridad son efectuados según los protocolos establecidos.

Evidencias:

- Desempeño: por observación y/o sustentación durante la gestión en seguridad de la información.
- Conocimiento: producto actas de instrucción. formatos de confidencialidad.

Funciones genéricas:

- Brindar la información que corresponda de acuerdo a la naturaleza del cargo, a quien la requiera, siguiendo los lineamientos de la normativa establecida.
- Implementar el Sistema de Gestión Integral de acuerdo con los lineamientos institucionales, efectuando mejora continua en los procesos que lo requieran.
- Realizar las actividades establecidas en la gestión documental, aplicando la normativa vigente.
- Realizar las actividades establecidas para la implementación del Sistema de Gestión Ambiental en la Policía Nacional de Colombia.
- Guardar la reserva y confidencialidad de los documentos e información que sea de su conocimiento dentro del cumplimiento de sus funciones.
- Dar buen uso a los elementos asignados bajo su responsabilidad, con el fin de mantenerlos disponibles para el servicio.
- Cumplir con las normas, reglamentos e instrucciones del Sistema de Gestión de la Seguridad y Salud en el Trabajo, de acuerdo con lo establecido en la normativa vigente.

- Cumplir con las actividades establecidas a través de los roles asignados, diferentes a las funciones del cargo.
- Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de su cargo.

Perfil:

El grado policial para este cargo debe ser el de un Oficial de la Institución, Capitán o Mayor; con un criterio de profesional universitario, con estudios telemáticos de educación superior y posgrado en ciberseguridad.

Habilidades comportamentales:

Son comportamientos requeridos con mayor frecuencia que se relacionan directamente con el nivel de responsabilidad, propósito y funciones del cargo.

- Elaborar planes para el cumplimiento de metas: idoneidad para proceder con agilidad a la organización de eventos en el tiempo, asegurando una eficiente ejecución que conduzca al cumplimiento sistemático de las metas bajo su responsabilidad, apoyado en su orden mental y en una clara noción de causas y efectos.
- Dar aseguramiento al logro de metas: condición para revisar de manera metódica y sistemática los avances y evaluar la evolución de las tareas y responsabilidades consignadas en los planes, sugiriendo ajustes y cambios de estrategias para asegurar el cumplimiento de los compromisos adquiridos.
- Identificar el potencial del personal: habilidad para revisar y evaluar la capacidad profesional de las personas a su cargo identificando la brecha de crecimiento y el aumento en la asignación de las correspondientes responsabilidades.

- Practicar liderazgo situacional: capacidad para dirigir a las personas de forma acertada y congruente con la realidad, de tal manera que cada persona reciba la guía apropiada y las tareas estén alineadas con el potencial de cada uno.

- Revisar y ajustar informes para uso ejecutivo: habilidad para practicar una revisión permanente y ejecutar los ajustes necesarios a los informes para que aporten hechos y evidencias certeros, orientando así la toma de decisiones.

- Propender por un clima de entusiasmo: habilidad para emplear técnicas motivacionales y de asesoramiento que le permita contar con los mejores aportes por parte de sus subordinados, siendo el compromiso profesional y el entusiasmo un componente importante para la calidad de la contribución del grupo bajo su responsabilidad.

Analista de Ciberseguridad:

Su propósito principal es monitorear permanentemente los sistemas de información con el fin de prevenir la vulnerabilidad y mal uso de los mismos.

Funciones del cargo:

- Crear los formatos y procedimientos necesarios, para documentar los incumplimientos de ciberseguridad, que vulneren el procedimiento de gestión de la información.

- Detectar, reportar y contener los comportamientos anómalos ejercidos desde el ciberespacio, a través del ingreso autorizado por parte de los administradores de sistemas de información y que de esta conducta modifiquen, eliminen, creen o actualicen datos, almacenados en los sistemas de información.

- Aplicar el procedimiento 1DT-PR-0008 cuando se vulnere la integridad de la información, para enviar los respectivos informes a la Inspección General de la Policía Nacional de Colombia, competente de investigar este tipo de conductas.

Habilidades funcionales: (evaluación y desempeño)

Criterios de desempeño:

- Los formatos y procedimientos para documentar los incumplimientos de ciberseguridad son creados y estandarizados según protocolo establecido.
- Los comportamientos anómalos ejercidos desde el ciberespacio son detectados y reportados inmediatamente.
- El procedimiento estandarizado de violación de la política de calidad e integridad de los datos es aplicado cuando se detecta estas conductas.

Evidencias:

- Desempeño: por observación y/o sustentación durante el seguimiento a protocolos de seguridad de la información.
- Conocimiento: producto actas de instrucción. Formatos de confidencialidad.

Funciones genéricas:

- Brindar la información que corresponda de acuerdo a la naturaleza del cargo, a quien la requiera, siguiendo los lineamientos de la normativa establecida.

- Implementar el sistema de gestión integral de acuerdo con los lineamientos institucionales, efectuando mejora continua en los procesos que lo requieran.

- Realizar las actividades establecidas en la gestión documental, aplicando la normativa vigente.

- Realizar las actividades establecidas para la implementación del sistema de gestión ambiental en la Policía Nacional de Colombia.

- Guardar la reserva y confidencialidad de los documentos e información que sea de su conocimiento dentro del cumplimiento de sus funciones.

- Dar buen uso a los elementos asignados bajo su responsabilidad, con el fin de mantenerlos disponibles para el servicio.

- Cumplir con las normas, reglamentos e instrucciones del Sistema de Gestión de la Seguridad y Salud en el Trabajo, de acuerdo a lo establecido en la normativa vigente.

- Cumplir con las actividades establecidas a través de los roles asignados, diferentes a las funciones del cargo.

- Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de su cargo.

Perfil:

El grado policial para este cargo debe ser el de un mando del nivel ejecutivo de la institución, Patrullero, Subintendente, Intendente; con un criterio de técnico o tecnólogo

profesional, con estudios relacionados a la ingeniería de sistemas y conceptos básicos de ciberseguridad.

Habilidades comportamentales:

Son comportamientos requeridos con mayor frecuencia que se relacionan directamente con el nivel de responsabilidad, propósito y funciones del cargo.

- Actualizar su conocimiento constantemente: capacidad para mantenerse enterado de los conocimientos que son útiles para su trabajo, dedicando el tiempo necesario al estudio, a las conversaciones y a las reuniones que le dan riqueza intelectual.

- Integrar información: habilidad para conseguir y ordenar datos que aseguran una adecuada comprobación de la información, prestando atención al detalle.

- Validar procedimientos: capacidad para aportar información confiable de hechos y hallazgos, cuestionando la vigencia de los procedimientos actuales y sugiriendo cambios que conducirán a una mayor certidumbre y sostenibilidad de las acciones.

- Elaborar informes con base científica: pericia del funcionario para realizar informes respaldados por hechos comprobables, profundizando en su indagación cuando esta podría conducirle a una certeza comprobable.

- Comunicarse convincentemente: disposición del funcionario para convencer y desempeñarse con elocuencia al compartir información en su interacción con personas internas y externas.

Con los argumentos y exposición de motivos contenidos en la presentación realizada, se eleva la propuesta en mesa de trabajo ante el encargado del rediseño organizacional de la

Dirección de Talento Humano, la Oficina de Planeación y un asesor jurídico de la Secretaría General, para conocimiento y validación de la propuesta; durante esta mesa de trabajo se determinan los ajustes y la viabilidad del proyecto, lo cual abre paso a que sea presentada toda la documentación a la Oficina de Planeación de la Dirección General.

En la ilustración 2, se representa el esquema de funcionamiento del del Grupo de Ciberseguridad, con las funciones asignadas al jefe del grupo y sus analistas.

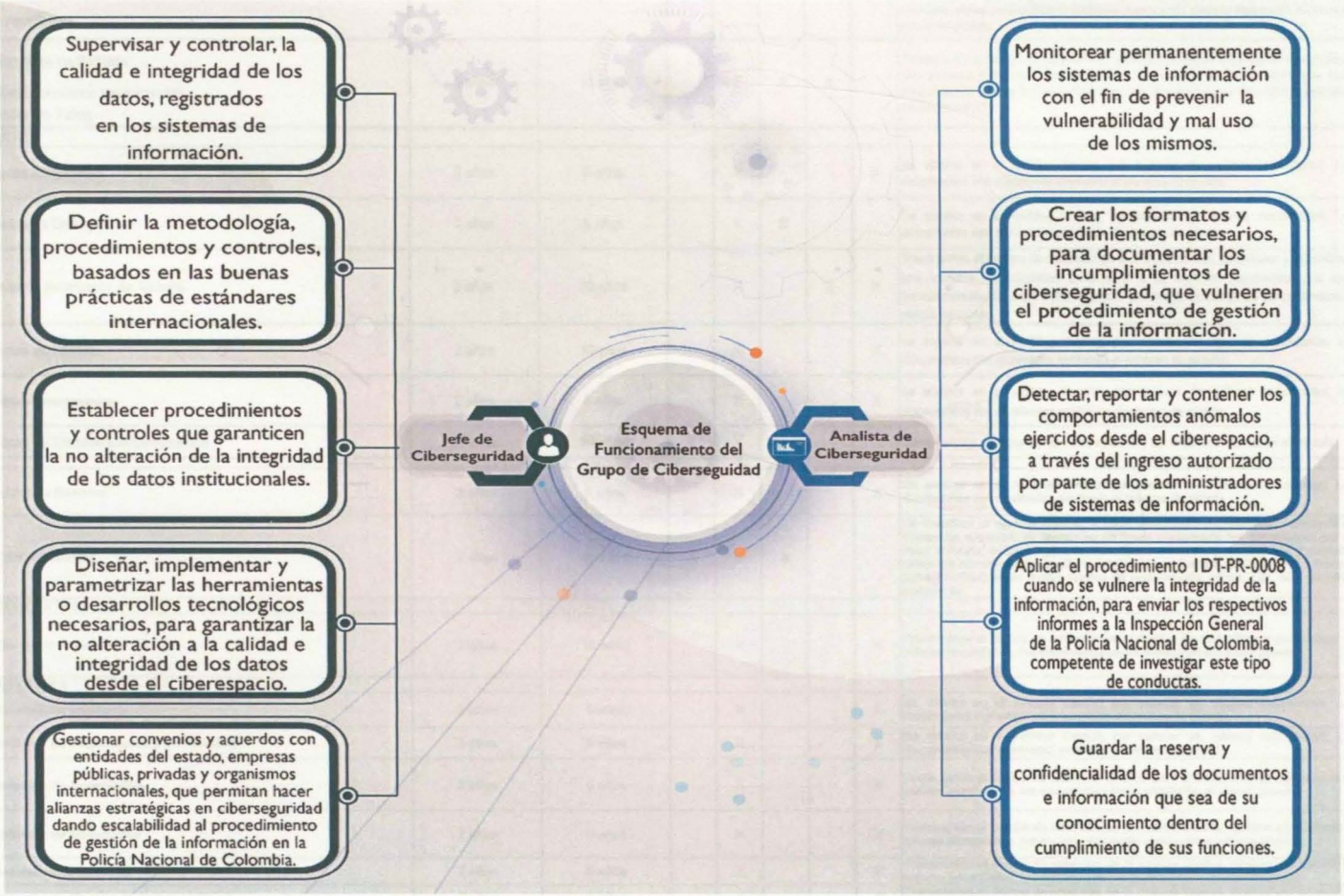


Ilustración 5 Esquema de funcionamiento del Grupo de Ciberseguridad

Fuente. Elaboración propia

10.1.6. Tabla de Retención Documental propuesta para el Grupo de Ciberseguridad

Tabla 3 Tabla de Retención Documental Propuesta para el Grupo de Ciberseguridad

MINISTERIO DE DEFENSA
POLICÍA NACIONAL
TABLA DE RETENCIÓN DOCUMENTAL

UNIDAD PRODUCTORA: POLICÍA NACIONAL	**OFICINA PRODUCTORA : GRUPO DE CIBERSEGURIDAD**	**FECHA DE ACTUALIZACIÓN:**
DIRAN: OFICINA DE TELEMÁTICA	**CÓDIGO DE LA OFICINA PRODUCTORA: 1.10.4.10**	**RESOLUCIÓN Y FECHA: Resolución**

CÓDIGO	SERIES, SUBSERIES Y TIPOS DOCUMENTALES	RETENCIÓN		DISPOSICIÓN FINAL					PROCEDIMIENTO
		ARCHIVO GESTIÓN	ARCHIVO CENTRAL	CT	D	M	S	E	
1	■ ACCIONES CONSTITUCIONALES								
1.1	□ Acción de Cumplimiento ✓ Antecedentes	2 años	5 años		X	X	X	X	Transcurrido el tiempo de retención en el Archivo Central, seleccionar y microfilmar una muestra representativa hasta el 2 % de aquellos documentos que sean trascendentales para la Policía Nacional. Los demás documentos serán eliminados mediante picado.
1.10	□ Derechos de Petición ✓ Quejas, reclamos y sugerencias ✓ Acción de Tutela	2 años	10 años		X	X	X		Transcurrido el tiempo de retención en el Archivo Central, seleccionar y microfilmar una muestra representativa hasta el 1 % de aquellos documentos que sean trascendentales para la Policía Nacional. Los demás documentos serán eliminados mediante picado.
2	■ ACTAS								
2.1	□ Actas Asignación	2 años	5 años		X			X	Se elimina en el Archivo Central, por carecer de valores secundarios. Los documentos son eliminados mediante el proceso de picado.
2.21	□ Actas de Entrega	2 años	5 años		X	X			Se elimina en el Archivo Central, por carecer de valores secundarios. Los documentos son eliminados mediante el proceso de picado.
2.25	□ Acta de Reuniones de Trabajo	2 años	20 años		X		X	X	Transcurrido el tiempo de retención en el Archivo central, seleccionar y microfilmar una muestra representativa hasta el 3 % de aquellos documentos que sean trascendentales para la Policía Nacional. Los demás documentos serán eliminados mediante picado.
2.40	□ Actas de Revista	2 años	10 años		X			X	Se elimina en el Archivo Central, por carecer de valores secundarios. Los documentos son eliminados mediante el proceso de picado.
2.78	□ Actas Compromiso	2 años	5 años		X			X	Se elimina en el Archivo Central, por carecer de valores secundarios. Los documentos son eliminados mediante el proceso de picado.
2.81	□ Actas de Eliminación Documental	20 años	50 años	X	X				Conservación total por ser la única evidencia del soporte documental eliminado.
2.96	□ Actas de Reserva	2 años	5 años		X			X	Se elimina en el Archivo Central, por carecer de valores secundarios. Los documentos son eliminados mediante el proceso de picado.
12	■ CERTIFICADOS	2 años	20 años	X	X	X			Se transfiere al Archivo Central, la serie Certificados Académicos, culminado su tiempo de retención, se conservan en forma permanente los documentos por su valor histórico, cultural y para la investigación, con fines de respaldo y consulta, utilizando microfilmación (según lo establecido en Decreto 2527 de 1950 y Decreto 3354 de 1954) como medio técnico de reproducción según, Ley 594 de 2000, Artículo 19.
15	■ CONCEPTOS								
15.2	□ Concepto Técnico	2 años	10 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
29	■ INFORMES								
29.3	□ Informe de Auditoria	2 años	5 años		X			X	Se elimina en el Archivo Central, por carecer de valores secundarios. Los documentos son eliminados mediante el proceso de picado.
29.10	□ Informe de Seguimiento y Evaluación	2 años	5 años		X			X	Se elimina en el Archivo Central, por carecer de valores secundarios. Los documentos son eliminados mediante el proceso de picado.
29.25	□ Informe de Actividades	2 años	5 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
29.57	□ Informe de Novedades	2 años	5 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
29.61	□ Informe de Procesos	2 años	5 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
29.62	□ Informe de Prueba de Vulnerabilidad	2 años	5 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
30	■ INVENTARIOS	2 años	10 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
30.10	□ Formato Único de Inventario Documental	0 años	0 años	X	X				Conservar totalmente en el Archivo de Gestión y Archivo Central por ser un documento de constante actualización y consulta.
33	■ MANUALES	2 años	5 años		X	X	X	X	Transcurrido el tiempo de retención en el Archivo Central, seleccionar y microfilmar una muestra representativa hasta el 1 % de aquellos documentos que sean trascendentales para la Policía Nacional. Los demás documentos serán eliminados mediante picado.
36	■ NORMAS TÉCNICAS	2 años	5 años	x	x	x			Se microfilma la totalidad de la serie, por cuanto es un documento de carácter histórico.
38	■ ORDENES								
38.6	□ Orden General	2 años	10 años	X	X	X			Se microfilma la totalidad de la serie, por cuanto es un documento de carácter histórico.
38.10	□ Orden de Cumplimiento ✓ memorando ✓ poligramas ✓ Otro	2 años	18 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
38.12	□ Orden de Trabajo	2 años	10 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.

40	■ PLANES								
40.2	□ Plan de Acción ✓ antecedentes	2 años	3 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
40.6	□ Plan de Mantenimiento	2 años	3 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
40.7	□ Planes de mejoramiento ✓ antecedentes	2 años	3 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
40.54	□ Plan de Manejo Ambiental	2 años	3 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
41	■ PROCESOS								
41.1	□ Proceso Administrativo ✓ antecedentes	2 años	20 años		X	X	X		Transcurrido el tiempo de retención en el Archivo Central, seleccionar y microfilmar una muestra representativa hasta el 5% de aquellos documentos que sean trascendentales para la Policía Nacional. Los demás documentos serán eliminados mediante picado.
47	■ SISTEMAS DE INFORMACIÓN	2 años	5 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
60	■ CONVENIOS	2 años	8 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
60.1	□ Convenio de Cooperación	2 años	8 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
60.4	□ Convenio Interinstitucional	2 años	8 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
60.8	□ Convenio Interadministrativo	2 años	8 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
86	■ PROGRAMAS								
86.10	□ Programa de Prevención	2 años	8 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
86.30	□ Programa de Gestión Ambiental	2 años	8 años		X			X	Transcurrido el tiempo de retención en el Archivo Central, eliminar por carecer de valores secundarios, los documentos serán eliminados mediante picado.
95	■ SISTEMAS DE GESTIÓN								
95.6	□ Sistema de la Seguridad Informática ✓ Antecedentes	2 años	8 años		x			x	Transcurrido el tiempo de retención en el Archivo Central eliminnado por carecer de valores secundarios los documentos serán eliminados mediante picado.

■ SERIE DOCUMENTAL
□ SUBSERIE DOCUMENTAL
✓ TIPO DOCUMENTAL
CT CONSERVACIÓN TOTAL
D DIGITALIZAR
E ELIMINACIÓN
M MICROFILMACIÓN U OTRO SOPORTE
S SELECCIÓN

Brigadier General CEIN CASTRO GUTIERREZ
Jefe Oficina de Telemática

Fuente. Elaboración propia

10.1.7. Estudio de planeación

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
OFICINA DE TELEMÁTICA

Bogotá D.C., 28 de diciembre del 2019

ESTUDIO DE PLANEACIÓN

TEMA

CREACIÓN DEL GRUPO DE CIBERSEGURIDAD POLICIAL EN LA OFICINA DE TELEMÁTICA

1. PROBLEMA:

La Oficina de Telemática identificó que existe una amenaza en ciberseguridad por parte de los administradores de sistemas de información, relacionada con la integridad y calidad de los datos almacenados en las bases de datos de la Policía Nacional de Colombia, los cuales desde el ciberespacio pueden acceder y eliminar la trazabilidad de las actividades realizadas.

2. HIPÓTESIS:

Al no contar con un Grupo de Ciberseguridad en la Institución, se podría generar alteración en la integridad de los datos, lo cual podría afectar la calidad y veracidad de la información personal e institucional, para fines contrarios a los lineamientos éticos de la Institución y del correcto comportamiento enmarcado en la función pública.

Con la creación del Grupo de Ciberseguridad Policial, que tenga la función de controlar y monitorear el trabajo realizado por los administradores de sistemas de información de la Oficina de Telemática, se podría garantizar la integridad y calidad de los datos almacenados desde los sistemas custodiados por la Oficina de Telemática.

3. HECHOS QUE TIENEN RELACIÓN CON EL PROBLEMA:

a) Reseña histórica:

Dentro de la Policía Nacional de Colombia las tareas de informática y telemática eran desarrolladas por la unidad de informática, al evidenciar el crecimiento tecnológico, para 1990 se organiza la División de Comunicaciones y Electrónica" y se incluye en la estructura de la División de Comunicaciones y Electrónica, el Grupo de Contabilidad, dependiendo de la Sección Administrativa, la cual continuó con su funcionamiento hasta el año 1998 cuando se definen los procesos de la Oficina de Telemática, que para esta época no tenía la relevancia pertinente; solo hasta el año 2001 se define la estructura orgánica de la Oficina de Planeación que contaba con tres grupos, entre ellos telemática esta composición de mantiene en el tiempo hasta 2007 donde se desarrolla la estructura orgánica y determinan los procesos de las oficinas de Gestión Institucional y Telemática en la cual se crean dos áreas quienes que adquirieron la responsabilidad del desarrollo e implementación de infraestructura de telemática y la administración de los recursos tecnológicos.

En este transcurso la Policía Nacional de Colombia modifica su estructura orgánica bajo el Decreto 4222 de 2006 con el que nace la Oficina de Telemática con un carácter asesor; a causa de esta modificación, en el año 2009 se hace necesario realizar una nueva modificación debido a que las funciones del Decreto y la Resolución eran incompatibles; por tanto, en este año, con la modificación estructural, se da paso a la creación de tres áreas de trabajo focalizadas así: Proyección e implementación tecnológica, Administración de tecnologías de la información y Administración de la información. Durante este tiempo se comienzan a realizar desarrollos tales como el Plan de contingencia y recuperación de la información de bases de datos administrativas y operativas; durante los años venideros se evidencia un

avance en el desarrollo de tecnologías propiamente policiales y la Oficina de Telemática pasó de ser una unidad de soporte y apoyo, a convertirse en un pilar para el desarrollo de las Fuerzas Militares.

Debido a los avances tecnológicos y las necesidades institucionales, en el año 2013 se determinan nuevas funciones de la Oficina de Telemática en la estructura y se rediseñan las dependencias internas, impactando en las direcciones, metropolitanas, departamentos de Policía y unidades especiales.

El acto administrativo que define la estructura vigente se encuentra establecido en la Resolución N° 00090 del 15 de enero de 2015, *"Por la cual se modifica parcialmente la Resolución 02536 del 08 de julio de 2013"* y modifica parcialmente la Resolución N° 02536 del 8 de julio de 2013, "*Por la cual se define la estructura orgánica interna de la Oficina de Telemática, se determinan sus funciones y se derogan unas disposiciones*", en el sentido de agregar el Grupo de Telemática a la Escuela Nacional de Operaciones de la Policía Nacional de Colombia (CENOP) y la Escuela de Policía Providencia de Sumapaz, como unidades desconcentradas; los demás artículos de la resolución continúan vigentes.

Debido a la evolución institucional expuesta y la necesidad perentoria de esta oficina asesora en el manejo de los sistemas de información y tratamiento de la integridad de los datos, se hace obligatorio que la estructura actual sea flexible y se adapte a la necesidad informática de la época, dehí la importancia del rediseño organizacional con el fin de combatir las problemáticas que se pueden presentar frente a la administración de estos recursos.

b) Marco legal:

- Ley 962 de 2005, "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados."

- 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 se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Por medio de esta ley, el Congreso de la República se enfocó a garantizar la confidencialidad, integridad, disponibilidad de los datos en los sistemas de información (Congreso de la República de Colombia, 2009).

- Resolución 00937 del 10 de marzo 2016, "Por la cual se establece el Manual de Funciones para el personal uniformado de la Policía Nacional de Colombia, la metodología de evaluación para el perfil de los cargos y se derogan unas disposiciones": en esta Resolución, se constituye como un instrumento de gerenciamiento del talento humano, brindando elementos descriptivos de los cargos como: 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, mantenimiento de la seguridad y convivencia ciudadana (Oficina de Planeacion Policía Nacional de Colombia, 2016).

- Resolución 05309 del 24 de agosto 2016, "Por la cual se establecen las Tablas de Organización Policial (TOP) de la Policía Nacional de Colombia y se derogan unas disposiciones": estas tablas, son una herramienta mediante la cual se estandarizan las cantidades mínimas requeridas de personal en cada cargo asociado a la unidad, identificando la cantidad de vacantes y/o remanentes por dependencias y determinando las necesidades a nivel nacional. De igual forma, sirven para realizar el análisis sobre el crecimiento institucional y ejercer control sobre los movimientos de personal, estas tablas de organización policial, se establecen a través del módulo de perfiles por cargos en el Sistema para la Administración del Talento Humano (Oficina de PLaneación Policía Nacional de Colombia, 2016).
- Resolución 08310 del 28 de diciembre 2016, "Por la cual se expide el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional de Colombia", este acto administrativo, es de cumplimiento para los funcionarios de la Policía Nacional de Colombia y personal externo que le proporcione algún bien o servicio; quienes están obligados a adoptar los parámetros aquí descritos y los controles adicionales que pueden implementar las diferentes unidades de acuerdo a su misionalidad. La política de Seguridad de la Información busca cubrir toda la información impresa o escrita en papel, recopilada electrónicamente en cualquier medio de almacenamiento actual o futuro, transmitida a través de medio electrónico actual o futuro; mostrada en videos o hablados, y todo lo considerado información de carácter institucional que se convierte en activos de información (Policía Nacional de Colombia, 2016).

c) Análisis externo:

Es importante resaltar que la ciberseguridad es un entorno digital en desarrollo que en Colombia ha sido poco explorada; tanto así que, en las demás Fuerzas Militares del Estado colombiano, no se cuenta con un Grupo de Ciberseguridad enfocado a controlar y monitorear el trabajo realizado por los administradores de sistemas de información. La Policía Nacional de Colombia, con la creación de este grupo servirá de referente ante las demás instituciones del estado presentando un efecto positivo en la calidad e integridad de los datos almacenados en sus sistemas de información.

d) Entorno tecnológico:

La adquisición de las herramientas tecnológicas, es indispensable para cumplir con las funciones asignadas a este grupo, un software como Imperva Data Activity Monitoring, tiene

la capacidad de identificar patrones de comportamiento anómalos en actividades sospechosas, crea automáticamente una lista blanca de los objetos de datos a los que acceden regularmente las cuentas de bases de datos individuales, estableciendo políticas que alerten o bloqueen el acceso cuando una cuenta con perfil intenta acceder a un objeto de datos que no está en la lista blanca. Esta parametrización se realiza directamente por el administrador de la herramienta, quien dependiendo de las necesidades a que haya lugar, determina qué comportamientos considera necesario controlar y cuáles bloquear.

Es necesario integrar las bases de datos que en la actualidad interactúan con los sistemas de información que tiene la Institución, con el fin de implementar este nuevo software, que controle y monitoree los accesos que realizan los usuarios con altos privilegios, como son los administradores de dichos sistemas, y limitando las transacciones de código que puedan afectar la calidad e integridad de los datos.

En esta misma línea, es de precisar que la Policía Nacional de Colombia cuenta con esta herramienta tecnológica, pero a la fecha no ha emprendido las acciones pertinentes para su implementación, esto debido a que los lineamientos institucionales ordenan la creación de un grupo para la ejecución del proceso.

e) Análisis y soporte presupuestal:

La modificación de la estructura interna de la Oficina de Telemática, no requiere inversión presupuestal, por cuanto la oficina tiene a su disposición el software requerido, para ser administrado por el Grupo de Ciberseguridad y el personal profesional idóneo, con las competencias necesarias para parametrizar y ejecutar esta herramienta tecnológica.

Por otra parte, es necesario aclarar que el mantenimiento del software a futuro, se encuentra en el marco del soporte presupuestal que maneja la Oficina de Telemática para cada vigencia, razón por la cual no es necesario el ajuste presupuestal.

f) Análisis interno:

Revisando la información de la Oficina de Telemática, es necesario tener en cuenta aspectos como la estructura jerárquica, las líneas de autoridad, los niveles de responsabilidad, la comunicación interna, los cuales están enmarcados a través de las dependencias, procesos, funciones y cargos que se desprenden así:

Estructura actual de la Oficina de Telemática de la Policía Nacional de Colombia

Ilustración 6 Estructura Actual de la Oficina de Telemática de la Policía Nacional de Colombia

Fuente. Intranet de la Policía Nacional de Colombia, http://polired/default.aspx

La Oficina de Telemática cuenta con una estructura diseñada de tal forma que responde a los procesos definidos actualmente, con un esquema que integra los procesos gerenciales, misionales, de soporte, evaluación y mejora de conformidad con los requisitos del Sistema de Gestión Integral; no obstante, ante las amenazas existente desde el ciberespacio y que pueden afectar la integridad y calidad de los datos almacenados desde los sistemas de información de la Policía Nacional de Colombia, se genera la necesidad de implementar un nuevo Grupo de Ciberseguridad, con el enfoque a controlar y monitorear el trabajo realizado por los usuarios que tienen asignados usuarios de altos privilegios y que desde el ciberespacio

pueden acceder a las bases de datos institucionales. Por lo cual se plantea la siguiente estructura:

Estructura propuesta de la Oficina de Telemática de la Policía Nacional de Colombia

Ilustración 7 Estructura propuesta de la Oficina de Telemática de la Policía Nacional de Colombia

Fuente. Elaboración propia

La implementación del Grupo de Ciberseguridad, le aportará al proceso misional de administración de la información, garantizando la integridad y calidad de los datos almacenados desde los sistemas de información en las bases de datos.

Con la creación de este grupo la Policía Nacional de Colombia, se ve beneficiada en varios factores como lo son: demostrar la efectividad en las tareas realizadas, demostrar un grado de transparencia en su labor, avances institucionales sobre la seguridad de información y

blindar a la institución ante posibles requerimientos judiciales o administrativos por permitir la vulneración de la Ley 1581 de 2012.

Mapa de procesos actual de la Policía Nacional de Colombia

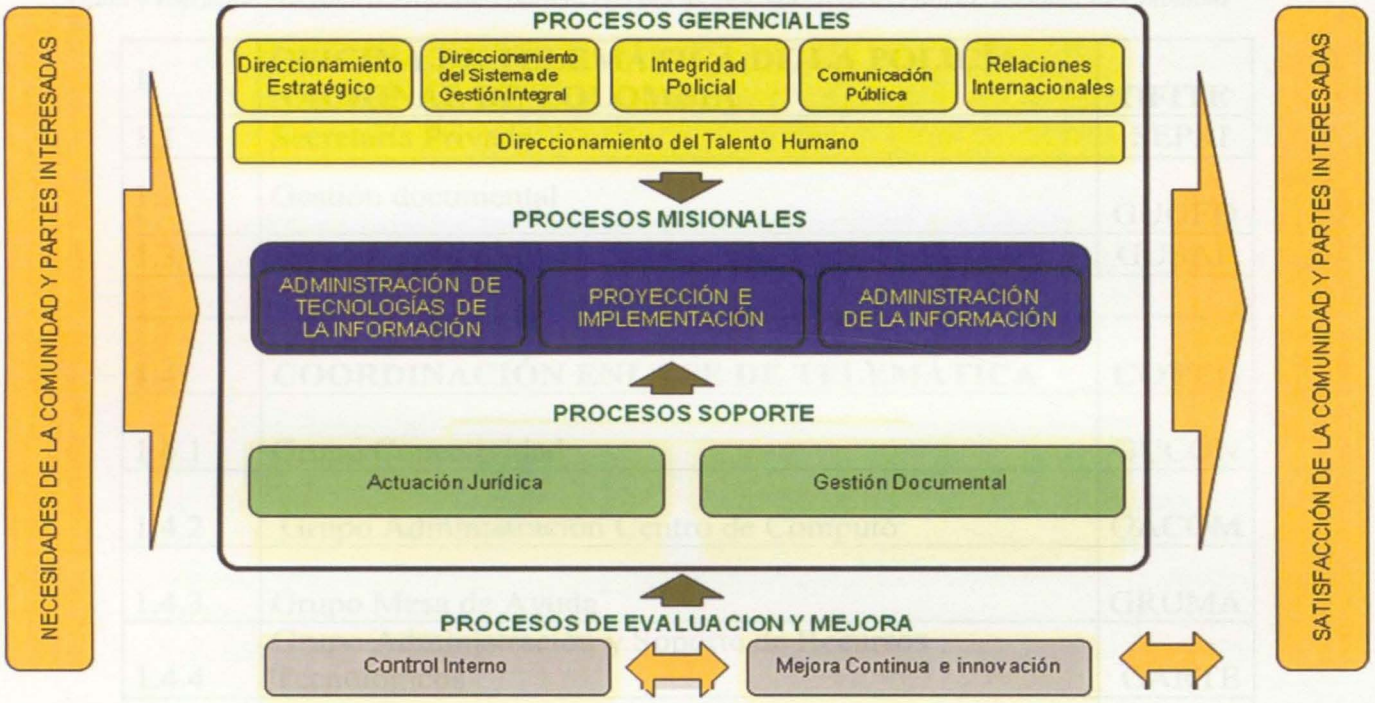


Ilustración 8 Mapa de Procesos - Policía Nacional de Colombia

Fuente. Intranet de la Policía Nacional de Colombia, http://polired/default.aspx

La implementación del Grupo de Ciberseguridad, le aportará al proceso misional de administración de la información, garantizando la integridad y calidad de los datos almacenados desde los sistemas de información en las bases de datos.

Para efectos de planeación que genere infraestructura reflejada en instalaciones policiales, se analizarán adicionalmente las siguientes dimensiones:

Dimensión Física: las instalaciones de la Oficina de Telemática cuenta en su infraestructura con el espacio físico necesario para la adecuación de este grupo, en esta misma línea se propone una distribución espacial, donde se encuentra ubicado el Grupo de Respuestas de Incidentes de Seguridad, se adicionarían tres puestos de trabajo con la logística necesaria como los son: computadores, escritorio, silla y telefonía IP.

La ubicación estratégica del grupo en el entorno de la Oficina Telemática, está dada para la articulación del proceso de integridad de los datos.

A continuación, se presenta la estructura orgánica propuesta para la Oficina de Telemática, con la cual se pretende realizar un monitoreo y control a los administradores de sistemas de información que tienen asignado usuarios con altos privilegios.

Tabla 4 Estructura Orgánica Propuesta para la Oficina de Telemática de la Policía Nacional de Colombia

1.	**OFICINA DE TELEMÁTICA DE LA POLICÍA NACIONAL DE COLOMBIA**	**OFITE**
1.1	Secretaría Privada	SEPRI
1.2	Gestión documental	GUGED
1.3	Soporte y Apoyo	GUSAP
1.4	**COORDINACIÓN ENLACE DE TELEMÁTICA**	**COTEL**
1.4.1	Grupo Conectividad	GUCON
1.4.2	Grupo Administración Centro de Computo	GACOM
1.4.3	Grupo Mesa de Ayuda	GRUMA
1.4.4	Grupo Administración y Soporte de Recursos Tecnológicos	GARTE
1.4.5	Grupo Ensamble y Servicio Técnico	GESET
1.4.6	Grupo Implementación Tecnológica	GRUIM
1.4.7	Grupo Investigación y Proyección Tecnológica	GINTE
1.4.8	Grupo Desarrollo Tecnológico	GRUDE
1.4.9	Grupo Continuidad de la Información	GUCIN
1.4.10	Grupo Seguridad de la Información	GRUSI
1.4.11	Grupo Respuesta a Incidentes de Seguridad	CSIRT
1.4.12	Grupo de Ciberseguridad	GUCIB
1.4.13	**UNIDADES DESCONCENTRADAS DE TELEMÁTICA**	**UNDES**
1.4.13.1	Grupos de Telemática Direcciones	GRUDI
1.4.13.2	Grupos de Telemática Policías Metropolitanas	GRUME
1.4.13.3	Grupos de Telemática Departamentos de Policía	GRUDE
1.4.13.4	Grupos de Telemática Escuelas de Policía	GRUES

Fuente. Elaboración propia

4. ANÁLISIS:

La Policía Nacional de Colombia cuenta con sistemas de información que optimizan el trabajo realizado por las unidades a nivel país, desde la Oficina de Telemática, se soporta tecnológicamente con todas las aplicaciones que están en producción y es deber de la oficina, garantizar la disponibilidad, confidencialidad e integridad de la información.

A nivel de estructuración organizacional, tres grupos de la oficina soportan dentro de sus funciones un pilar fundamental como lo es velar por la seguridad de la información y que el acceso a la misma solo sea por usuarios debidamente autorizados por la oficina, cumpliendo el protocolo establecido.

Teniendo en cuenta lo anterior, se hace necesario la creación del Grupo de Ciberseguridad, enfocado a monitorear y controlar el trabajo realizado por los administradores de sistemas de información; quienes, desde el ciberespacio, con roles asignados y usuarios de altos privilegios, pueden acceder a los sistemas de información y manipular los datos sin que hasta el momento sean detectados este tipo de comportamiento.

La ciberseguridad, debe ir alineada con la seguridad de la información y es ineludible afrontar los retos que trae el mundo actual con la cuarta revolución industrial, donde se hace necesario contemplar nuevos escenarios de posible amenaza a la información como lo es el Ciberespacio. La Policía Nacional de Colombia, con la creación del Grupo de Ciberseguridad, servirá como referente ante las demás entidades del estado, potencializando a esta oficina asesora como un pilar en desarrollo tecnológico en conservación de la integridad de los datos. Además, un referente para todas las policías de américa latina.

A. VENTAJAS

Una modificación en la estructura actual de la Oficina de Telemática, brindaría las siguientes ventajas:

- Mejoramiento en la interacción del Mapa de Procesos con la misma finalidad mediante una estructuración orgánica más flexible, apoyando al mejoramiento contínuo de nuestros procesos.

- Garantizar la calidad e integridad de los datos, almacenados en los sistemas de información de la Policía Nacional de Colombia, para satisfacer las necesidades y expectativas de la institución.

- Alinearse con las políticas de Estado, con relación al tratamiento de datos personales y seguridad de la información, asegurando el cumplimiento de los requisitos normativos en la materia y el marco jurídico actual.

- Desde la perspectiva organizacional de la institución trabajar el concepto de Ciberseguridad institucional, con el fin de detectar y prevenir cualquier tipo de amenaza,

que desde el ciberespacio se quiera materializar y que afecte la calidad e integridad de los datos.

- Se alinea con la política de austeridad del gasto del Gobierno Nacional, en el marco que la propuesta de modificación de la estructura orgánica interna, debido a que no requiere de presupuesto para su realización por cuanto en la actualidad se cuenta el personal, para el desarrollo de las funciones del grupo.

B. DESVENTAJAS

No se tiene contemplada ninguna desventaja dentro del proceso de reestructuración.

5. CONCLUSIONES:

- En consecuencia, a lo propuesto en el presente documento, se considera la necesidad y oportunidad de implementación del Grupo de Ciberseguridad en la estructura orgánica de la Oficina de Telemática, toda vez que los escenarios entrantes de incidentes de ciberseguridad, requieren este grupo como punta de lanza que permite enfrentar sin dilación las ciberamenazas, motivo por el cual su replanteamiento se enfoca directamente en el control sobre los administradores de sistemas de información, los cuales a través de sus roles y privilegios pueden acceder desde el ciberespacio y vulnerar la calidad e integridad de la data almacenada.

- Con la creación del Grupo de Ciberseguridad, se aportará al control desde el ciberespacio de los sistemas de información custodiados y administrados por la Oficina de Telemática.

- La estructura orgánica propuesta, se encuentra ajustada a las necesidades y expectativas de la Policía Nacional de Colombia, permitiendo una interacción con el proceso de administración de la información y articulación con los demás procesos, incluyendo la ciberseguridad como la columna fundamental en la administración de sistemas de información en la institución policial.

6. RECOMENDACIONES:

- Ajustar la estructura orgánica actual conforme a los parámetros establecidos en el presente estudio y las funciones anexas, lo cual contribuye a garantizar la calidad e integridad de los datos almacenados en los sistemas de información, coadyuvando al fortalecimiento del Direccionamiento Tecnológico Policial, a través del ajuste de su estructura orgánica, como uno de los componentes básicos y esenciales del Sistema de Gestión Integral de la Policía Nacional de Colombia y el Sistema de Gestión de Seguridad de la Información.

- Presentar proyecto de resolución que modifica la estructura orgánica interna en la Oficina de Telemática de la Policía Nacional, establecida mediante Resolución No. 02536 del 08 de julio 2013, la cual requiere ser modificada y ajustada a las necesidades actuales y

futuras de nuestra Institución, con el fin de evitar que se materialice cualquier amenaza desde el ciberespacio, por parte de los administradores de sistemas de información y que deben ser monitoreados y controlados por el dueño del Direccionamiento Tecnológico de la Institución.

ANEXOS: Tabla de Organización Policial (TOP) y Tablas de Retención Documental (TRD)

Atentamente,

Brigadier General **CEIN CASTRO GUTIÉRREZ**
Jefe Oficina de Telemática

10.1.8. Concepto de la Dirección de Talento Humano para la modificación estructural de la Oficina de Telemática.

DITAH - PLANE - 15.2

Bogotá D.C., 06 de enero del 2020

Brigadier General
RAMIRO ALBERTO RIVEROS ARÉVALO
Jefe Oficina de Planeación
Carrera 59 26 - 21
Bogotá D.C.

Asunto: concepto modificación estructural de OFITE.

Teniendo en cuenta la comunicación oficial No. S-2019-005381-OFPLA, donde se solicita emitir concepto de viabilidad por parte de esta Dirección para la creación del Grupo de Ciberseguridad en la Oficina de Telemática, respetuosamente me permito informar al señor Brigadier General que, una vez revisada la documentación del proyecto de modificación, se exponen las siguientes consideraciones:

- En cuanto al listado de cargos y funciones que se proyectan, estas se adecuan a los requisitos establecidos y los lineamientos de la Dirección de Talento Humano, teniendo

en cuenta que ya se encuentran contemplados en el manual de funciones del personal uniformado de la Policía Nacional.

- Para la Tabla de Organización Policial, se da viabilidad en atención a que no existe incremento de cantidades numéricas de personal, manteniendo los parámetros establecidos en la administración del talento humano, con relación a no aumentar la TOP general de la unidad.

Dado lo anterior, esta Dirección emite concepto viable en relación al listado de cargos, funciones y cantidades mínimas requeridas en la TOP para la modificación de la estructura orgánica de la Subdirección General; de igual forma, se recuerda que una vez aprobada y firmada la resolución se debe proceder a realizar los ajustes en el Sistema de Información para la Administración del Talento Humano (SIATH), ingresando cargos, funciones, perfiles y TOP, para posteriormente realizar la distribución del personal en la nueva estructura, atendiendo a lo establecido en el procedimiento 1DS-PR-0022 "Formular el rediseño organizacional de las dependencias internas de la Policía Nacional de Colombia".

Atentamente,

Mayor General **ÁLVARO PICO MALAVER**
Director de Talento Humano

10.1.9. Concepto de Planeación para la creación del Grupo de Ciberseguridad

OFPLA - GESIN - 15.15

Bogotá D.C., 30 de enero 2020

CONCEPTO DE PLANEACIÓN

TEMA POR ESTUDIAR: determinar desde el punto de vista del rediseño organizacional la viabilidad de la modificación de la estructura orgánica interna de la Oficina de Telemática con el fin de incluir el Grupo de Ciberseguridad.

HECHOS O ASUNTOS POR ESTUDIAR:

- Analizar el estudio de planeación y proyecto de resolución "por la cual se modifica parcialmente la estructura orgánica interna de la Oficina de Telemática creando el Grupo de Ciberseguridad, se determinan sus funciones y se dictan otras disposiciones".
- Comunicaciones oficiales de referencias: S-2019-000352-OFITE del 24122019 y S-2020-000102-OFITE del 10012020

ANÁLISIS:

- Revisadas las motivaciones que originan la solicitud S-2019-000352-OFITE del 24 de diciembre de 2019, elevada desde la Oficina de Telemática en la que se indica la existencia de la necesidad de crear un Grupo de Ciberseguridad, por la cual se hace ineludible la modificación de su estructura orgánica interna, por cuanto en la actualidad los administradores policiales de sistemas de información con privilegios, roles y permisos, no cuentan con el control y monitoreo en el cumplimiento de sus funciones, teniendo en cuenta lo anterior, se debe crear este grupo de control al interior de la Institución.

- De igual forma, es indispensable que la Oficina de Telemática se articule con los procesos mundiales que afronta las unidades policiales en cuanto a los delitos informáticos, alineado a las políticas de protección de datos de Seguridad Nacional en el marco de Ciberseguridad de los sistemas de información, en procura de fortalecer la interacción de estos lineamientos al interior de la institución, planteamiento que se ajusta a los descrito en la Directiva 011 del 28 de abril de 2010 "Parámetros para la elaboración de propuestas de reestructuración orgánica de las dependencias de la Policía Nacional de Colombia".

- De acuerdo a los criterios expuestos en el estudio de planeación, se argumenta la necesidad que la Oficina de Telemática asuma los cambios generados por la evolución en la seguridad para el tratamiento de datos, lo cual permite a la Policía Nacional de Colombia ser pionera en esta materia.

- De igual manera, es oportuna la creación de las funciones asignada al Grupo de Ciberseguridad, con el fin de establecer parámetros de actuación frente a la posible materialización de amenazas desde el Ciberespacio.

- Así mismo y considerando el análisis presupuestal presentado en el estudio de planeación, correspondiente a la modificación de la estructura interna de la Oficina de Telemática, se encuentra que los mismos no generan un incremento en los recursos asignados a esta oficina asesora, ante este panorama es inminente adoptar los roles de Ciberseguridad, de forma organizada tanto funcional como estructuralmente, para garantizar la calidad e integridad de los datos almacenados; así las cosas es claro que no surgen nuevas

necesidades desde el ámbito presupuestal, alineándose de esta forma a las directrices del Gobierno Nacional en materia de austeridad de gasto y cero impactos económicos en la modificación de estructuras orgánicas de las entidades públicas del Estado.

- La modificación estructural es necesaria y se basa en el hecho que la Oficina de Telemática, en el desarrollo de sus procesos ha emergido como precursora en la implementación de herramientas informáticas, que le permiten a la institución dar pasos agigantados en el control y monitoreo en las bases de datos.

- Adicionalmente el estudio de planeación permite vislumbrar la necesidad de la modificación de la Resolución No. 02536 del 8 de julio de 2013 "Por la cual se define la estructura orgánica interna de la Oficina de Telemática, se determinan las funciones y se derogan funciones", en atención a que este acto administrativo no contempla la necesidad de este grupo.

CONCLUSIÓN:

A partir de la revisión técnica generada desde el Grupo de Gestión Institucional de la Oficina de Planeación, previa revisión y evaluación de la propuesta plasmada en el estudio de planeación para la modificación de la estructura orgánica interna de la Oficina de Telemática, se estableció que los cambios incluidos tanto en el estudio de planeación como en el proyecto de resolución son ajustados y adecuados, desde el punto de vista del rediseño organizacional.

Por lo anterior y desde el punto de vista organizacional y presupuestal, se considera FAVORABLE, efectuar el cambio de la estructura orgánica interna de la Oficina de Telemática y la creación del Grupo de Ciberseguridad.

ES MI CONCEPTO.

Brigadier General **RAMIRO ALBERTO RIVEROS ARÉVALO**
Jefe Oficina de Planeación

10.1.10. Concepto de la Secretaría General para la creación del Grupo de Ciberseguridad

Bogotá D.C., 16 de enero del 2020

Brigadier General
RAMIRO ALBERTO RIVEROS AREVALO
Jefe Oficina de Planeación
Carrera 59 No. 26 - 21 CAN
Bogotá D.C.,

Asunto: respuesta a comunicación oficial No. S-2019-005381-OFPLA

En atención al escrito del asunto mediante el cual mi General, solicita la revisión jurídica de la propuesta presentada por la Oficina de Telemática relacionada con la creación del "Grupo de Ciberseguridad en la Oficina de Telemática", comedidamente me permito precisar lo siguiente:

Resulta imperioso destacar que en desarrollo del artículo 218 del mandato constitucional se expidió el Decreto 4222 del 23 de noviembre de 2006 "Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional", norma que en su artículo 24 facultó al Director General para crear, organizar, con carácter permanente o transitorio, escuelas, unidades, áreas funcionales y grupos de trabajo, determinando en el acto de creación de estas, sus tareas, responsabilidades y demás disposiciones necesarias para su funcionamiento, de ahí que resulta viable desde el marco jurídico adoptar la propuesta, conforme lo establece el procedimiento "Parámetros para la elaboración de propuestas de reestructuración orgánica de las dependencias de la Policía Nacional de Colombia".

En virtud de lo anterior, esta Oficina Asesora concluye que es viable desde el marco jurídico la creación del "Grupo de Ciberseguridad", al interior de la Oficina de Telemática de la Policía Nacional de Colombia, con el apoyo y coordinación de las unidades policiales que considere le aporten a los fines y cumplimientos del Direccionamiento Tecnológico.

Finalmente, en cuanto a la disponibilidad de cargos y personal para la creación de esta dependencia policial, así como las modificaciones organizacionales pertinentes, me permito precisar que la Dirección de Talento Humano en coordinación con la Oficina de Planeación, son las dependencias competentes en esta materia.

Atentamente,

Brigadier General **PABLO ANTONIO CRIOLLO REY**
Secretario General

10.1.11. Borrador de la Resolución por la cual se modifica parcialmente la estructura orgánica interna de la Oficina de Telemática

Tabla 5 Estructura propuesta para la Oficina de Telemática

MINISTERIO DE DEFENSA NACIONAL

POLICÍA NACIONAL

DIRECCIÓN GENERAL

RESOLUCIÓN NÚMERO DE

"Por la cual se modifica parcialmente la estructura orgánica interna de la Oficina de Telemática creando el Grupo de Ciberseguridad, se determinan sus funciones y se dictan otras disposiciones"

EL DIRECTOR GENERAL DE LA POLICÍA NACIONAL DE COLOMBIA

En uso de las facultades legales y,

CONSIDERANDO:

Que el Decreto 4222 del 23 de noviembre de 2006, "Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional", establece en su artículo 2º "Funciones del Director General de la Policía Nacional de Colombia.", numeral 8 Expedir dentro del marco legal de su competencia, las resoluciones, manuales, reglamentos y demás actos administrativos necesarios para administrar la Policía Nacional de Colombia en todo el territorio nacional, pudiendo delegar de conformidad con las normas legales vigentes.

Que la norma ibídem en su artículo 24º- Unidades Funcionales, facultó al Director General de la Policía Nacional de Colombia para crear y organizar, con carácter permanente o

transitorio, escuelas, unidades, áreas funcionales y grupos de trabajo, determinando en el acto de creación de éstas, sus tareas, responsabilidades y las demás disposiciones necesarias para su funcionamiento.

Que la Oficina de Telemática de la Policía Nacional de Colombia rediseña la estructura orgánica interna, eliminando las áreas y se crean los grupos definidos en la presente, asignando funciones, que permitan atender a las necesidades del servicio, y cumplir con eficiencia, eficacia y efectividad los objetivos, políticas, programas y procesos misionales de la Policía Nacional de Colombia.

Que en el Decreto 4485 del 18 de noviembre de 2009, Modelo Estándar de Control Interno de acuerdo a la Ley 87 del 30 de diciembre de 1993 y Decreto 1599 del 20 de mayo de 2005, contribuye al logro de uno de los objetivos del control interno, como es garantizar la eficacia, eficiencia y efectividad en la parte operativa y administrativa de la Policía Nacional de Colombia, promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para el logro de la misión institucional.

Que en la Resolución No. 04055 del 21 de diciembre 2009, que en su artículo 1° modifica y adiciona el artículo 18, se desagregan los grupos de gestión documental de la secretaria privada de las unidades policiales y se modifica y adiciona la Resolución No. 02764 del 26 de junio 2008, "Por medio de la cual se adopta el Programa de Gestión Documental de la Policía Nacional de Colombia y sus políticas".

Que mediante la Resolución No. 02541 del 25 de julio de 2011 "Por la cual adopta el mapa de procesos institucional, los procesos de primer nivel y se derogan unas disposiciones", se dispuso en el artículo 4 "Procesos de Primer Nivel", numerales 3 "procesos de soporte" numeral 3.1 "Direccionamiento Tecnológico" y en el artículo 6 "Dueños de Proceso de Primer Nivel", numeral 11 Direccionamiento Tecnológico – Jefe Oficina de Telemática.

Que mediante Resolución No. 04377 del 28 de noviembre de 2011, se creó la Policía Metropolitana de Villavicencio, se definió la estructura orgánica interna y se determinaron sus funciones.

Que mediante Resolución No. 04378 del 28 de noviembre de 2011, se creó la Policía Metropolitana de Ibagué, se definió la estructura orgánica interna y se determinaron sus funciones.

Que mediante Resolución No. 00215 del 27 de enero de 2012, se modificó parcialmente la resolución 04378 del 28 de noviembre de 2011, "Por la cual se crea la Policía Metropolitana de Ibagué, se define la estructura orgánica interna y se determinan las funciones".

Que mediante Resolución No. 02592 del 25 de julio de 2012, se creó la Policía Metropolitana de Santa Marta, se definió la estructura orgánica interna y se determinaron sus funciones.

Que mediante Resolución No. 04350 del 19 de noviembre de 2012, se creó la Policía Metropolitana de Popayán, se definió la estructura orgánica interna y se determinaron sus funciones.

Que mediante Resolución No. 01935 del 27 de mayo de 2013, se creó la Policía Metropolitana de Neiva, se definió la estructura orgánica interna y se determinaron sus funciones.

Que en atención al estudio de planeación presentado por la Oficina de Telemática, se precisó la necesidad de unificar en un solo acto administrativo la normatividad que define su estructura, el rediseño de sus dependencias internas, sus competencias disciplinarias, con el objeto de mejorar la supervisión, control y el direccionamiento a través de la creación de nuevos grupos internos y unidades desconcentradas, lo que permitirá una adecuada armonía, coherencia, articulación del nivel central con las unidades desconcentradas y facilitará el desarrollo de la política de integridad policial en la Institución, para lo cual,

R E S U E L V E:

CAPÍTULO I
GENERALIDADES

ARTÍCULO 1. MISIÓN. La Oficina de Telemática de la Policía Nacional de Colombia tiene como misión asesorar y promover el desarrollo tecnológico de la Institución en lo correspondiente a las Tecnologías de la Información y las Comunicaciones a través de la investigación, desarrollo, implementación, administración, soporte y seguridad de la información, para apoyar el servicio policial.

CAPÍTULO II
ESTRUCTURA ORGÁNICA INTERNA

ARTÍCULO 2. ESTRUCTURA. Para el cumplimiento de su misión, la Oficina de Telemática contará con la siguiente estructura orgánica interna:

1.	**Oficina de Telemática**	**OFITE**
1.1.	Secretaría Privada.	SEPRI
1.2.	Gestión Documental.	GUGED
1.3.	Soporte y Apoyo.	GUSAP
1.4.	**Coordinación Enlace de Telemática**	**COTEL**
1.4.1.	Grupo Conectividad.	GUCON
1.4.2.	Grupo Administración Centro de Cómputo.	GACOM
1.4.3.	Grupo Mesa de Ayuda.	GRUMA
1.4.4.	Grupo Administración y Soporte de Recursos Tecnológicos.	GARTE
1.4.5.	Grupo Ensamble y Servicio Técnico.	GESET
1.4.6.	Grupo Implementación Tecnológica.	GRUIM
1.4.7.	Grupo Investigación y Proyección Tecnológica.	GINTE
1.4.8.	Grupo Desarrollo Tecnológico.	GRUDE

1.4.9.	Grupo Continuidad de la Información.	GUCIN
1.4.10.	Grupo Seguridad de la Información.	GRUSI
1.4.11.	Grupo Respuesta a Incidentes de Seguridad.	CSIRT
1.4.12.	Grupo de Ciberseguridad.	GUCIB
1.4.13.	**Unidades Desconcentradas de Telemática**	**UNDES**
1.4.13.1.	Grupos de Telemática Direcciones.	GRUDI
1.4.13.2.	Grupos de Telemática Policías Metropolitanas.	GRUME
1.4.13.3.	Grupos de Telemática Departamentos de Policía.	GRUDE
1.4.13.4.	Grupos de Telemática Escuelas de Policía.	GRUES

CAPÍTULO III
DE LAS FUNCIONES

ARTÍCULO 3. OFICINA DE TELEMÁTICA: Es la dependencia encargada de asesorar y promover el desarrollo tecnológico de la Institución en lo correspondiente a las Tecnologías de la Información y las Comunicaciones a través de la investigación, desarrollo, implementación, administración, soporte y seguridad de la información, para apoyar el servicio policial. Cumplirá las siguientes funciones:

1. Asesorar a la Dirección General de la Policía Nacional de Colombia en la planeación, diseño, implementación, promoción y administración de telecomunicaciones e informática para el mejoramiento continuo del servicio policial.
2. Orientar y liderar de manera concertada el Plan Estratégico en Telemática respondiendo a las necesidades de la institución y del Sector Defensa.
3. Gerenciar la implementación de los diversos proyectos de tecnología en telecomunicaciones e informática de la Policía Nacional de Colombia.

4. Desarrollar y poner en marcha los proyectos que respondan a las estrategias definidas en el Plan estratégico en Telecomunicaciones e Informática, promoviendo el avance tecnológico en todos los niveles.
5. Asesorar y promover la contratación de Tecnología en telecomunicaciones e informática, así como, investigar y analizar tecnología de punta para satisfacer las necesidades de las diferentes áreas y poder definir racionalmente la inversión institucional.
6. Promover y proponer mecanismos para el uso de la tecnología instalada de telecomunicaciones e informática que permita incrementar la efectividad y productividad en el servicio policial.
7. Administrar y supervisar el funcionamiento de Telecomunicaciones e Informática de la Policía Nacional de Colombia de acuerdo con los niveles de servicio requeridos por la institución, garantizando el óptimo y adecuado funcionamiento del servicio policial.
8. Coordinar técnica y administrativamente en funcionamiento de los Grupos de Telemática de las Direcciones, Oficinas Asesoras, Regiones de Policía, Departamentos de Policía, Policías Metropolitanas, Distritos especiales de policía, Escuelas de formación y unidades especiales con el fin de estandarizar y unificar la política en materia de telecomunicaciones e informática.
9. Desarrollar la Política y Objetivos de Calidad de la Policía Nacional de Colombia.
10. Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de la dependencia.

ARTICULO 4. SECRETARÍA PRIVADA. Es la dependencia de la Oficina de Telemática encargada de la organización, articulación, seguimiento y ajuste de la agenda del señor jefe de la Oficina de Telemática y demás actividades para dinamizar los trámites y tareas que se desarrollan en la unidad. Cumplirá las siguientes funciones:

1. Tramitar oportunamente la documentación que se origine o llegue a la Jefatura del jefe de la Oficina de Telemática, así como verificar los tiempos para su cumplimiento.
2. Ejercer control al cumplimiento del calendario de documentación y órdenes impartidas por el jefe de la Oficina de Telemática.

3. Mantener la reserva y confidencialidad frente al manejo de la documentación y demás asuntos que revistan tal carácter.
4. Organizar y verificar la agenda del jefe de la Oficina de Telemática y ejercer control al cumplimiento de plazos en documentación y órdenes impartidas por la Jefatura.
5. Mantener informado al jefe de la Oficina de Telemática de los hechos que deban ser de su conocimiento.
6. Asistir al jefe de la Oficina de Telemática, en todas las actividades de representación, organización y asistencia a actos protocolarios y relaciones públicas.
7. Atender consultas, procedimientos y solicitudes de información que deben ser resueltos por el jefe de la Oficina de Telemática.
8. Organizar y diseñar el esquema de seguridad del jefe de la Oficina de Telemática, supervisando que el talento humano y logístico cuente con lo necesario para su normal funcionamiento.
9. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTICULO 5. GESTIÓN DOCUMENTAL. Es la dependencia de la Oficina de Telemática encargada del desarrollo de los procesos tales como producción, recepción, distribución organización, recuperación y disposición final de los documentos. Cumplirá las siguientes funciones:

1. Recepcionar, distribuir y tramitar oportunamente la documentación que se origine o allegue a la unidad.
2. Administrar la documentación oficial a través de mecanismos que garanticen el manejo expedito y controlado de la correspondencia.
3. Mantener la reserva y confidencialidad frente al manejo de la documentación.
4. Responder por la integridad, autenticidad, veracidad y fidelidad de la información del patrimonio documental de la unidad.
5. Suministrar información confiable y oportuna a los usuarios.

6. Cumplir con la normatividad expedida por el Archivo General de la Nación y demás entes que controlan el manejo y buen uso de la documentación.
7. Administrar el sistema archivístico mediante acciones de evaluación, seguimiento y mecanismos de mejoramiento continuo acorde con las políticas organizacionales y con el Sistema de Gestión de la Calidad.
8. Dar cumplimiento a los lineamientos del Proceso de Gestión Documental, respecto al control de registros.
9. Ejecutar el procedimiento de archivo central con el fin de garantizar la disponibilidad de la información para consulta.
10. Proyectar las modificaciones o actualizaciones de las Tablas de Retención Documental cuando se requiera, para el trámite al Archivo General de la Policía Nacional de Colombia.
11. Difundir y propender por la aplicación e implementación de las Tablas de Retención Documental en las dependencias de la unidad.
12. Orientar y liderar en la unidad la organización del fondo acumulado, para su remisión al Archivo General de la Policía Nacional de Colombia de acuerdo a la normatividad vigente.
13. Presentar propuestas de mejoramiento para aportar al Comité de Gestión Documental de la unidad.
14. Implantar y fortalecer la cultura archivística a partir de estrategias de capacitación y sensibilización.
15. Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de la dependencia.

ARTICULO 6. SOPORTE Y APOYO: Es la dependencia de la Oficina de Telemática encargada de asesorar al interior de la unidad el desarrollo de los procesos, procedimientos y tareas a su cargo, así como de proponer acciones para el mejoramiento continuo. Cumplirá las siguientes funciones:

1. Promover la cultura de la planeación en todos los niveles, al elaborar, suscitar, desarrollar, hacer seguimiento y evaluación a los planes de mejoramiento continuo, planes de acción y administración del riesgo en la unidad.

2. Propender por el desarrollo del mantenimiento y mejora del Sistema de Gestión Integral de la Unidad.
3. Desarrollar y aplicar al interior de la unidad todos los procesos y procedimientos de talento humano, de acuerdo a los lineamientos que imparta la Dirección de Talento Humano.
4. Coordinar los servicios de bienestar social, consistentes en recreación, deporte, cultura, asistencia social y vivienda fiscal de acuerdo con los lineamientos establecidos por la Dirección de Bienestar Social.
5. Dar aplicabilidad al proceso de integridad policial al interior de la unidad de acuerdo a los lineamientos de la Inspección General a través de acciones preventivas y de mejora, fomentando la cultura de la legalidad en los funcionarios.
6. Gestionar y coordinar los medios tecnológicos necesarios en materia de comunicaciones e informática de la unidad.
7. Gestionar y coordinar los requerimientos de prestación de servicio de apoyo logístico que soliciten las dependencias de la Unidad, para garantizar un servicio efectivo.
8. Desarrollar las actividades que se deleguen del proceso Gerencial de Comunicación Pública.
9. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTICULO 7. COORDINACIÓN ENLACE DE TELEMATICA. Es la dependencia enlace entre la Oficina de Telemática y las unidades desconcentradas. Cumplirá las siguientes funciones:

1. Dirigir y dinamizar la formulación, preparación, operacionalización y cumplimiento del Plan de Acción de la Unidad, a través del acompañamiento en todos los niveles de gestión de la Oficina de Telemática, con el fin de propender por el cumplimiento de las metas y objetivos propuestos.
2. Representar al jefe de la Oficina de Telemática cuando éste lo designe, en las juntas, consejos u otras reuniones a que deba asistir.

3. Crear sinergia entre la Oficina de Telemática y las unidades desconcentradas, en lo referente al direccionamiento tecnológico para la Policía Nacional de Colombia.
4. Establecer y diseñar metodologías de trabajo para consolidar enlaces colaborativos con las unidades desconcentradas para operar la plataforma tecnológica.
5. Conocer y asesorar las necesidades y requerimientos tecnológicos que tengan las unidades desconcentradas de Telemática, para proponer estrategias de solución al jefe de la Oficina de Telemática.
6. Coordinar, controlar y evaluar la gestión de los Grupos de la Oficina de Telemática y unidades desconcentradas de Telemática, con el fin de propender por el cumplimiento de las metas y objetivos propuestos.
7. Coordinar la realización de mesas de trabajo, seminarios, talleres, conversatorios y demás eventos interinstitucionales para unificar la doctrina en materia de tecnologías de la información y las comunicaciones.
8. Garantizar el cumplimiento y aplicación de las directrices y controles tecnológicos por parte de los jefes de los Grupos de Telemática y las Unidades Desconcentradas, con el fin de generar estandarización y unidad de criterio en las tecnologías de la información y las comunicaciones.
9. Supervisar el desarrollo de la gestión de los Grupos de la Oficina de Telemática y las Unidades Desconcentradas, para garantizar la consolidación de la información requerida para la toma de decisiones.
10. Planear, ejecutar y controlar el despliegue del proceso de integridad policial, como líder Ético de la unidad.
11. Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 8. GRUPO CONECTIVIDAD: Es la dependencia de la Coordinación Enlace de Telemática, encargada de implementar y administrar la infraestructura de la red de datos de la institución, con el fin de garantizar la conectividad a nivel nacional. Cumplirá las siguientes funciones:

1. Administrar la red de datos LAN y el servicio de telefonía de la Dirección General de la Policía Nacional de Colombia, garantizando su disponibilidad.
2. Administrar la red de datos MAN y WAN, servicio de internet, firewall interno y externo, garantizando la conectividad y disponibilidad en las unidades de Policía a nivel nacional.
3. Diseñar en coordinación con las unidades desconcentradas, los requerimientos de cableado estructurado, con el fin de estandarizar las tecnologías a nivel nacional.
4. Coordinar la instalación de los canales de datos asignados a las diferentes unidades de policía a nivel nacional, a fin de garantizar la conectividad.
5. Supervisar el mantenimiento y Soporte técnico de los canales de datos de la Policía Nacional de Colombia, garantizando con el proveedor de servicio su funcionamiento.
6. Dar soporte técnico a las unidades desconcentradas de Telemática, para el funcionamiento de los servicios de la red de datos de la Policía Nacional de Colombia.
7. Administrar el servicio de la suite de antivirus institucional a fin mantener la disponibilidad de antivirus institucional.
8. Gestionar el módulo de canales de datos y equipos activos de la herramienta de gestión de disponibilidad.
9. Administrar los servicios de Directorio activo, DNS, DHCP, sitios y servicios WSUS y herramientas colaborativas (Chat, audio y video)
10. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 9. GRUPO ADMINISTRACIÓN CENTRO DE CÓMPUTO: Es la dependencia de la Coordinación Enlace de Telemática, encargada de implementar, administrar y ajustar las bases de datos, servidores y sistemas operativos de la Policía Nacional de Colombia. Cumplirá las siguientes funciones

1. Administrar las bases de datos, servidores y sistemas operativos de la Oficina de Telemática, para garantizar el funcionamiento y la disponibilidad de la información.
2. Coordinar con el grupo de implementación tecnológica, la creación de proyectos que tengan relación con las bases de datos.

3. Documentar los procedimientos, modificaciones y estructura de las bases de datos, servidores y sistemas operativos de la Oficina de Telemática, para estandarizar los procedimientos de back up en la Policía Nacional de Colombia.
4. Dirigir y coordinar la integridad del respaldo de las bases de datos, servidores y sistemas operativos de la Oficina de Telemática, para garantizar la disponibilidad de la información.
5. Establecer procedimientos con el fin de prevenir fallas en las estructuras de las bases de datos, servidores y sistemas operativos de la Oficina de Telemática.
6. Supervisar las actividades de los usuarios en las bases de datos, servidores y sistemas operativos de la Oficina de Telemática, para garantizar la estandarización tecnológica.
7. Proyectar las necesidades de licenciamiento de las diferentes bases de datos y software de aplicaciones.
8. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 10. GRUPO MESA DE AYUDA: Es la dependencia de la Coordinación Enlace de Telemática, encargada de la interface entre el usuario final y los integrantes del ambiente tecnológico de la Policía Nacional de Colombia garantizando la oportunidad de las soluciones a los requerimientos técnicos, con el fin de propender por el eficaz funcionamiento de las herramientas tecnológicas puestas a disposición de los usuarios. Cumplirá las siguientes funciones:

1. Gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las tecnologías de información y comunicaciones.
2. Administrar los requerimientos tecnológicos de los clientes internos de la Policía Nacional de Colombia vía software con el fin de dar seguimiento a los requerimientos del usuario.
3. Realizar seguimiento local de fallas tecnológicas en la policía Nacional de Colombia.
4. Realizar el soporte tecnológico oportuno al cliente interno y externo de la Policía Nacional de Colombia.

5. Recepcionar los requerimientos de los clientes internos de la Policía Nacional de Colombia, con el fin de solucionar las fallas técnicas de la plataforma tecnológica.
6. Rendir informes estadísticos al jefe de la Coordinación enlace de Telemática, sobre la satisfacción del cliente por el soporte técnico prestado.
7. Ser interfaz entre los usuarios de otras actividades de administración de servicios de tecnologías de la información como Gestión de Configuración, Gestión de Cambios, Gestión de Continuidad de Servicios de tecnologías de la información para satisfacer las necesidades de comunicación entre el personal de soporte tecnológico y los usuarios.
8. Administrar y controlar los incidentes registrados por los técnicos de mesa de ayuda, para identificar e implementar planes de mejora.
9. Mantener proactivamente informados a los usuarios de todos los eventos relevantes con el servicio que les pudieran afectar.
10. Dirigir los acuerdos de niveles de servicio de acuerdo a los requerimientos de las unidades desconcentradas, para dar soluciones rápidas, oportunas que satisfagan a los usuarios.
11. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 11. GRUPO ADMINISTRACIÓN Y SOPORTE DE RECURSOS TECNOLÓGICOS: Es la dependencia de la Coordinación Enlace de Telemática, encargada de la administración y mantenimiento de la infraestructura de Telemática para garantizar la disponibilidad de la plataforma tecnológica. Cumplirá las siguientes funciones:

1. Administrar y controlar el desarrollo del plan de mantenimiento y soporte de los equipos que conforman la infraestructura de tecnologías de la información y las comunicaciones de la institución, de acuerdo al segundo y tercer nivel de servicio.
2. Propender por el óptimo funcionamiento de la infraestructura de la red de radio, coordinando con las unidades desconcentradas las necesidades para su fortalecimiento.
3. Responder por la administración eficiente de las herramientas de correo electrónico, plataforma geográfica y pagina web de la institución, velando por su disponibilidad.

4. Actualizar las estructuras orgánicas internas de las diferentes unidades policiales, de acuerdo a las solicitudes realizadas por las unidades y soportadas mediante su resolución.
5. Realizar el soporte tecnológico según las fallas reportadas por las unidades desconcentradas.
6. Informar a la Coordinación enlace de Telemática los eventos que afecten el funcionamiento de la plataforma tecnológica con el fin de realizar acciones de mejoramiento.
7. Responder por el soporte de la red eléctrica regulada y normal para el correcto funcionamiento de los sistemas de potencia e infraestructura tecnológica de la Policía Nacional de Colombia.
8. Monitorear la infraestructura tecnológica a través de las unidades desconcentradas a nivel nacional.
9. Informar a la Coordinación enlace de Telemática, el estado de la operatividad de la administración y soporte de la infraestructura, para la toma de decisiones.
10. Gestionar con entidades públicas y privadas todo lo relacionado con la administración del uso del espectro electromagnético asignado a la Policía Nacional de Colombia.
11. Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 12. GRUPO ENSAMBLE Y SERVICIO TÉCNICO: Es la dependencia de la Coordinación Enlace de Telemática, encargada del ensamble, soporte y servicio técnico de los equipos de radiocomunicación que adquiere la Policía Nacional de Colombia. Cumplirá las siguientes funciones:

1. Dirige el ensamble de los equipos de comunicaciones, adquiridos por la Policía Nacional de Colombia, cumpliendo los protocolos del fabricante y estándares de calidad para garantizar el óptimo funcionamiento de la red de voz de la Policía Nacional de Colombia.
2. Responder por la recepción, clasificación y servicio técnico a los equipos de radiocomunicación que presenten fallas en las unidades policiales y que no tengan garantía vigente.

3. Coordinar y controlar el cumplimiento de garantías para los equipos de radiocomunicación que lo requieran, para garantizar el funcionamiento de la red de voz de la Policía Nacional de Colombia.
4. Brindar soporte técnico oportuno a las redes de voz de las unidades policiales que lo requieran, para garantizar su funcionamiento.
5. Coordinar, controlar y sistematizar los servicios técnicos, uso de repuestos, y solución de problemas en las redes de radio de la institución.
6. Coordinar y administrar la calibración de equipos de medición del grupo de ensamble y servicio técnico.
7. Gestionar la disposición final de los desechos tecnológicos de acuerdo a los patrones ambientales establecidos en la Policía Nacional de Colombia.
8. Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 13. GRUPO IMPLEMENTACIÓN TECNOLÓGICA: Es la dependencia de la Coordinación Enlace de Telemática, encargada realizar y orientar a las unidades policiales, en lo referente a la implementación de los proyectos tecnológicos, a fin de estandarizar y alinear las tecnologías de la información y las comunicaciones. Cumplirá las siguientes funciones:

1. Realizar la implementación de los proyectos de Tecnologías de la información y las comunicaciones, para su correcta instalación y funcionamiento.
2. Actuar la implementación de proyectos de Tecnologías de la información y las comunicaciones.
3. Realizar la entrega de proyectos al Grupo de Administración y Soporte de Recursos Tecnológicos, para seguimiento de su operación, uso y sostenimiento del mismo.
4. Generar informes al grupo de Investigación y Proyección Tecnológica con el fin de contribuir con la mejora continua de los mismos.

5. Realizar las actividades necesarias con los usuarios finales con el propósito de que los proyectos suplan las necesidades establecidas dentro de los tiempos, costos y calidad requerida.
6. Acompañar a las unidades policiales en la implementación de proyectos Tecnológicos, en procura de optimizar el rendimiento y funcionalidad de las tecnologías adquiridas.
7. Fomentar la implementación de proyectos Tecnológicos asignados al Grupo de Implementación Tecnológica, de acuerdo a la operación y el uso adecuado de los mismos, a fin de coordinar su implementación.
8. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 14. GRUPO INVESTIGACIÓN Y PROYECCIÓN TECNOLÓGICA: Es la dependencia de la Coordinación Enlace de Telemática, encargada de fomentar la investigación, análisis y proyección de nuevas tecnologías a la institución, con el fin de asesorar y orientar a la institución en la aplicación de nuevas tecnologías. Cumplirá las siguientes funciones:

1. Presentar y asesorar proyectos de investigación tecnológica que pretendan implementar las unidades policiales, para garantizar la optimización del servicio policial.
2. Estudiar y analizar técnicamente los nuevos sistemas, tecnologías y aplicaciones, con el fin de determinar la viabilidad de incorporación para el fortalecimiento del servicio policial.
3. Asesorar al mando institucional en cuanto a las prioridades en la consecución de nuevas tecnologías.
4. Coordinar con la Dirección Nacional de Escuelas y/o entes de investigación tecnológica públicos o privados la evaluación y seguimiento de tendencias tecnológicas aplicadas al servicio policial.
5. Proponer y orientar la ejecución de proyectos de investigación y desarrollo tecnológico en la Oficina de Telemática.

6. Gestionar los recursos asignados para la investigación y el desarrollo tecnológico de acuerdo a las normas existentes para tal fin.
7. Coordinar el proceso de certificación ante la oficina de derechos de autor, los softwares de desarrollos tecnológicos de la Policía Nacional de Colombia.
8. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 15. GRUPO DESARROLLO TECNOLÓGICO: Es la dependencia de la Coordinación Enlace de Telemática, encargada del diseño y desarrollo de software para ponerlos al servicio de la institución. Cumplirá las siguientes funciones:

1. Estudiar la posible aplicación de desarrollos tecnológicos al servicio de la Institución.
2. Promover la innovación y la proyección de soluciones de software.
3. Orientar a la Policía Nacional de Colombia en los requerimientos para el diseño de software con el fin de fortalecer el servicio de policía.
4. Documentar los soportes para la expedición de los certificados de derechos de autor del software desarrollado por la Policía Nacional de Colombia.
5. Organizar y dirigir los procesos de adquisición de software, para optimizar el servicio en la institución.
6. Asesorar a las unidades en el desarrollo de soluciones informáticas ajustadas a la plataforma tecnológica institucional.
7. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 16. GRUPO CONTINUIDAD DE LA INFORMACIÓN: Es la dependencia de la Coordinación Enlace de Telemática, encargada de supervisar el desarrollo, implementación, mantenimiento y actualización de la calidad, el ciclo de vida y continuidad de la información en la Policía Nacional de Colombia. Cumplirá las siguientes funciones:

1. Garantizar la conservación de la memoria digital de la institución para que la información cumpla las características de calidad, exactitud, totalidad, oportunidad y continuidad.
2. Definir la metodología para adoptar las mejores prácticas del ciclo de vida de la información alineadas a los objetivos de Tecnología de la Información con los de la Policía Nacional de Colombia.
3. Realizar monitoreo de la herramienta de disponibilidad, para optimizar los recursos de la red, servidores y canales de datos.
4. Clasificar, diseñar e implantar la gestión de datos informáticos de la institución, para facilitar el acceso y búsqueda de la información.
5. Controlar los mecanismos requeridos para la clasificación de la información teniendo en cuenta sus niveles de criticidad.
6. Definir y aplicar una metodología para mejorar la calidad de la información al interior de la Institución, para estandarizar los sistemas de información.
7. Asesorar el desarrollo de software seguro, con el fin de realizar la integración de la seguridad en las aplicaciones desarrolladas en la institución.
8. Realizar pruebas de software desarrollados, adquiridos o implementados en la institución, con el fin de garantizar que cumplan las características de calidad establecidas por la institución.
9. Definir y aplicar controles para la destrucción segura de la información cuando esta finalice su ciclo de vida.
10. Definir lineamientos para la realización de los respaldos de los sistemas de información de la institución.
11. Establecer e implementar los planes de recuperación ante desastres, con el fin de garantizar la continuidad de los activos de la información de mayor criticidad.
12. Difundir y realizar pruebas de contingencia de la información a fin de medir la efectividad de los planes de recuperación ante desastres.
13. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de su dependencia.

ARTÍCULO 17. GRUPO SEGURIDAD DE LA INFORMACIÓN: Es la dependencia de la Coordinación Enlace de Telemática, encargada de proteger la disponibilidad, confidencialidad e integridad de las tecnologías de la información. Cumplirá las siguientes funciones:

1. Supervisar los lineamientos y políticas de seguridad de la información institucional, de acuerdo a su clasificación, con el fin de cumplir los estándares y buenas prácticas para el cumplimiento con las regulaciones que apliquen a la Institución.
2. Brindar asesoría en la adquisición de tecnologías de seguridad de la información a nivel institucional.
3. Elaborar, clasificar y analizar los riesgos de los activos de la información, a fin de aplicar controles para mitigar el riesgo.
4. Supervisar el cumplimiento de las políticas de implementación, configuración y operación de los controles de seguridad de información existentes.
5. Administrar proyectos de implementación de nuevas tecnologías en seguridad de la información.
6. Realizar administración de identidades y controles de acceso a sistemas y aplicaciones, para que se cumplan las políticas de control de acceso.
7. Aplicar controles de seguridad de la información, para garantizar su confidencialidad, integridad y disponibilidad, con el fin de minimizar el riesgo de pérdida, fuga o modificación de la información.
8. Aplicar controles de seguridad de la información con el fin de proteger la propiedad intelectual.
9. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

ARTÍCULO 18. GRUPO RESPUESTA A INCIDENTES DE SEGURIDAD: Es la dependencia de la Coordinación Enlace de Telemática, encarga de la atención a incidentes informáticos de la Policía Nacional de Colombia. Cumplirá las siguientes funciones:

1. Detectar, reportar y solucionar, vulnerabilidades, amenazas e incidentes informáticos que afecten la disponibilidad, confidencialidad e integridad de la información en la Policía Nacional de Colombia a su vez verificar, monitorear y auditar la plataforma de antivirus de la Policía Nacional de Colombia, generando reportes, estadísticas y control sobre su licenciamiento.
2. Realizar la difusión, concientización y prevención de las políticas de seguridad de la información.
3. Alertar y advertir los incidentes de seguridad de la información, para mantener informado a las unidades de la Policía Nacional de Colombia.
4. Realizar el tratamiento de incidentes de seguridad de la información, para garantizar su protección y minimizar los riesgos de seguridad de la información.
5. Apoyar y dar respuesta a los incidentes de seguridad de la información que se presenten en la institución, para evitar daños en la infraestructura tecnológica.
6. Supervisar la actualización y aplicación de parches de seguridad de la información, para controlar la seguridad de la información.
7. Coordinar con la Oficina de comunicaciones estratégicas, el diseño de campañas de concientización, sobre seguridad de la información en la Institución.
8. Aplicar mecanismos de detección de intrusos internos y externos sobre la red institucional.
9. Implementar y hacer seguimiento a la Estrategia Nacional para la protección del ciberespacio a fin de contribuir a la sensibilización del ciber ciudadano sobre la importancia de la seguridad de la información.
10. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de su dependencia.

ARTÍCULO 19. GRUPO DE CIBERSEGURIDAD: es la dependencia de la Coordinación Enlace de Telemática, que se encarga de validar, monitorear, supervisar y controlar, la calidad e integridad de los datos, registrados en los sistemas de información de la Policía Nacional de Colombia. Cumplirá las siguientes funciones:

1. Definir la metodología, procedimientos y controles, basados en las buenas prácticas de estándares internacionales para la inserción de datos en los sistemas de información institucional, garantizando la calidad de los datos.
2. Establecer procedimientos y controles que garanticen la no alteración de la integridad de los datos institucionales, sin previa autorización y justificación por parte de los dueños de proceso.
3. Realizar las coordinaciones necesarias con los dueños de la información, con el fin de estandarizar el procedimiento de gestión de la información que garantice la calidad e integridad de los datos en los sistemas de información de la Policía Nacional de Colombia, para evitar que se materialice alguna ciberamenaza.
4. Diseñar, Implementar y parametrizar las herramientas o desarrollos tecnológicos necesarios, para garantizar la no alteración a la calidad e integridad de los datos desde el ciberespacio.
5. Detectar, reportar y contener los comportamientos anómalos ejercidos desde el ciberespacio, a través del ingreso autorizado por parte de los administradores de sistemas de información y que de esta conducta modifiquen, eliminen, creen o actualicen datos, almacenados en los sistemas de información.
6. Crear los formatos y procedimientos necesarios, para documentar los incumplimientos de ciberseguridad, que vulneren el procedimiento de gestión de la información.
7. Aplicar el procedimiento 1DT-PR-0008 cuando se vulnere la integridad de la información, para enviar los respectivos informes a la Inspección General de la Policía Nacional de Colombia, competente de investigar este tipo de conductas.
8. Gestionar convenios y acuerdos con entidades del estado, empresas públicas, privadas y organismos internacionales, que permitan hacer alianzas estratégicas en ciberseguridad dando escalabilidad al procedimiento de gestión de la información en la Policía Nacional de Colombia.
9. Las demás que le sean asignadas de acuerdo con la ley, los reglamentos o la naturaleza de la dependencia.

CAPÍTULO IV
UNIDADES DESCONCENTRADAS

ARTÍCULO 20. Para el cumplimiento de su misión la Oficina de Telemática contará con las siguientes unidades desconcentradas:

1. GRUPOS DE TELEMÁTICA DIRECCIONES

1.1 Grupo de Telemática de la Dirección de Seguridad Ciudadana
1.2 Grupo de Telemática de la Dirección de Carabineros y Seguridad Rural
1.3 Grupo de Telemática de la Dirección de Investigación Criminal
1.4 Grupo de Telemática de la Dirección de Inteligencia Policial
1.5 Grupo de Telemática de la Dirección de Antinarcóticos
1.6 Grupo de Telemática de la Dirección de Protección y Servicios Especiales
1.7 Grupo de Telemática de la Dirección Antisecuestro y Antiextorsión
1.8 Grupo de Telemática de la Dirección de Tránsito y Transporte
1.9 Grupo de Telemática de la Dirección Nacional de Escuelas
1.10 Grupo de Telemática de la Dirección Administrativa y Financiera
1.11 Grupo de Telemática de la Dirección de Talento Humano
1.12 Grupo de Telemática de la Dirección de Sanidad
1.13 Grupo de Telemática de la Dirección de Bienestar Social
1.14 Grupo de Telemática de la Dirección de Incorporación

2. GRUPOS DE TELEMÁTICA DE LAS POLICÍAS METROPOLITANAS

2.1 Grupo de Telemática de la Policía Metropolitana de Bogotá
2.2 Grupo de Telemática de la Policía Metropolitana de Barranquilla
2.3 Grupo de Telemática de la Policía Metropolitana de Bucaramanga
2.4 Grupo de Telemática de la Policía Metropolitana de Santiago de Cali
2.5 Grupo de Telemática de la Policía Metropolitana de Cartagena de Indias

2.6 Grupo de Telemática de la Policía Metropolitana de Valle de Aburra
2.7 Grupo de Telemática de la Policía Metropolitana de Cúcuta
2.8 Grupo de Telemática de la Policía Metropolitana de Pereira
2.9 Grupo de Telemática de la Policía Metropolitana de Santa Marta
2.10 Grupo de Telemática de la Policía Metropolitana de Ibagué
2.11 Grupo de Telemática de la Policía Metropolitana de Villavicencio
2.12 Grupo de Telemática de la Policía Metropolitana de Popayán
2.13 Grupo de Telemática de la Policía Metropolitana de Neiva

3. GRUPOS DE TELEMÁTICA DE LOS DEPARTAMENTOS DE POLICIA

3.1 Grupo de Telemática del Departamento de Policía Amazonas
3.2 Grupo de Telemática del Departamento de Policía Antioquia
3.3 Grupo de Telemática del Departamento de Policía Arauca
3.4 Grupo de Telemática del Departamento de Policía Atlántico
3.5 Grupo de Telemática del Departamento de Policía Bolívar
3.6 Grupo de Telemática del Departamento de Policía Boyacá
3.7 Grupo de Telemática del Departamento de Policía Caldas
3.8 Grupo de Telemática del Departamento de Policía Caquetá
3.9 Grupo de Telemática del Departamento de Policía Casanare
3.10 Grupo de Telemática del Departamento de Policía Cauca
3.11 Grupo de Telemática del Departamento de Policía Cesar
3.12 Grupo de Telemática del Departamento de Policía Chocó
3.13 Grupo de Telemática del Departamento de Policía Córdoba
3.14 Grupo de Telemática del Departamento de Policía Cundinamarca
3.15 Grupo de Telemática del Departamento de Policía Guajira
3.16 Grupo de Telemática del Departamento de Policía Guainía
3.17 Grupo de Telemática del Departamento de Policía Guaviare
3.18 Grupo de Telemática del Departamento de Policía Magdalena

3.19 Grupo de Telemática del Departamento de Policía Magdalena Medio
3.20 Grupo de Telemática del Departamento de Policía Meta
3.21 Grupo de Telemática del Departamento de Policía Nariño
3.22 Grupo de Telemática del Departamento de Policía Norte de Santander
3.23 Grupo de Telemática del Departamento de Policía Putumayo
3.24 Grupo de Telemática del Departamento de Policía Quindío
3.25 Grupo de Telemática del Departamento de Policía Risaralda
3.26 Grupo de Telemática del Departamento de Policía Santander
3.27 Grupo de Telemática del Departamento de Policía San Andrés y Providencia
3.28 Grupo de Telemática del Departamento de Policía Sucre
3.29 Grupo de Telemática del Departamento de Policía Tolima
3.30 Grupo de Telemática del Departamento de Policía Huila
3.31 Grupo de Telemática del Departamento de Policía Urabá
3.32 Grupo de Telemática del Departamento de Policía Valle
3.33 Grupo de Telemática del Departamento de Policía Vaupés
3.34 Grupo de Telemática del Departamento de Policía Vichada

4. GRUPOS DE TELEMÁTICA DE LAS ESCUELAS DE POLICÍA

4.1 Grupo de Telemática Escuela de Cadetes de Policía General Francisco de Paula Santander
4.2 Grupo de Telemática Escuela de Postgrados de Policía Miguel Antonio Lleras Pizarro
4.3 Grupo de Telemática Escuela de Suboficiales y Nivel Ejecutivo Gonzalo Jiménez de Quesada
4.4 Grupo de Telemática Escuela de Aviación Policial
4.5 Grupo de Telemática Escuela de Policía Simón Bolívar
4.6 Grupo de Telemática Escuela Nacional de Carabineros Alfonso López Pumarejo
4.7 Grupo de Telemática Escuela de Tránsito y Transporte

4.8 Grupo de Telemática Escuela de Policía Carlos Eugenio Restrepo
4.9 Grupo de Telemática Escuela de Policía Carlos Holguín Mallarino
4.10 Grupo de Telemática Escuela de Carabineros Eduardo Cuevas García
4.11 Grupo de Telemática Escuela de Policía Gabriel González
4.12 Grupo de Telemática Escuela de Investigación Criminal Teniente Coronel Elkin Leonardo Molina Aldana
4.13 Grupo de Telemática Escuela de Carabineros Alejandro Gutiérrez
4.14 Grupo de Telemática Escuela de Policía Metropolitana de Bogotá Teniente Coronel Julián Ernesto Guevara Castro
4.15 Grupo de Telemática Escuela Antonio Nariño
4.16 Grupo de Telemática Escuela de Carabineros Rafael Núñez
4.17 Grupo de Telemática Escuela de Policía Rafael Reyes
4.18 Grupo de Telemática Escuela de Provincia de Vélez Mayor General Manual José López Gómez

ARTÍCULO 21. FUNCIONES DE LAS UNIDADES DESCONCENTRADAS: las unidades desconcentradas de Telemática, son las encargadas de dirigir, coordinar, vigilar, asesorar y promover el desarrollo tecnológico de la Institución en las unidades policiales, están conformadas por los Grupos de Telemática a nivel nacional, dependen de Coordinación enlace de Telemática. Cumplirán las siguientes funciones:

1. Ejecutar las políticas en materia tecnológica y de seguridad que se establezcan por parte la Oficina de Telemática.
2. Suministrar soporte técnico y proyectar las necesidades en Tecnologías de la Información y las Comunicaciones de las unidades a nivel nacional.
3. Coordinar con la Oficina de Telemática los proyectos y el crecimiento tecnológico de la unidad.
4. Elaborar, ejecutar y hacer seguimiento, al plan de mantenimiento preventivo y correctivo de la infraestructura tecnológica de la unidad.

5. Administrar los recursos tecnológicos asignados a su unidad mediante la elaboración del cuadro de distribución de elementos tecnológicos de acuerdo al plan de necesidades de la unidad.
6. Asesorar las actividades del proceso contractual en materia tecnológica de la unidad.
7. Informar a la Oficina de Telemática el desarrollo de los proyectos tecnológicos de la unidad y ejecutar aquellos que le sean delegados.
8. Mantener y mejorar el Sistema de Gestión Integral en los procesos y procedimientos a su cargo.
9. Apoyar con la implementación de herramientas tecnológicas, las actividades del proceso de la unidad.
10. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia

PARÁGRAFO 1°. En el caso de las Direcciones, Policías Metropolitanas, Departamentos de Policía, Escuelas de Policía y unidades especiales, deberán ajustar en las estructuras orgánicas las funciones establecidas por la Oficina de Telemática para las unidades desconcentradas.

PARÁGRAFO 2°. Los Grupos de Telemática de las unidades desconcentradas, serán los encargados de consolidar, monitorear, supervisar y realizar seguimiento a los requerimientos tecnológicos de las unidades bajo su jurisdicción, administrando los bienes tecnológicos de la unidad en coordinación con la Dirección Administrativa y Financiera y la Oficina de Telemática, para efecto de necesidades de la unidad y distribución de los bienes tecnológicos alineados con las políticas tecnológicas de la Policía Nacional de Colombia.

PARÁGRAFO 3°. El talento humano adscrito a la Oficina de Telemática de las unidades desconcentradas en las Direcciones, Policías Metropolitanas, Departamentos de Policía, Escuelas de Policial, para efectos de vinculación, desvinculación, capacitación, orientación, nominación, traslados, aplicación de políticas y directrices, dependerá directamente de la Oficina de Telemática.

PARÁGRAFO 4°. El personal de las unidades desconcentradas de Telemática en las Direcciones, Policías Metropolitanas, Departamentos de Policía, Escuelas de Policía, no debe ser utilizado en labores que interfieran en el normal desarrollo administrativo y de funcionamiento de la infraestructura Telemática, establecido en el Direccionamiento Tecnológico de la Oficina de Telemática.

PARÁGRAFO 5°. El jefe de la Oficina de Telemática podrá asignar responsables de Telemática en las unidades que por su complejidad no requieran grupo de Telemática y sea necesario para la administración de la plataforma tecnológica de la unidad.

ARTÍCULO 21. La creación, cambio de denominación, supresión o modificación de los grupos o unidades funcionales de la Oficina de Telemática, será potestad del Director General de la Policía Nacional de Colombia.

PARÁGRAFO 1°. La Oficina de Telemática coordinara con la Oficina de Planeación el desarrollo del proceso de rediseño organizacional de su estructura, de acuerdo a la normatividad legal vigente y principios establecidos por el Departamento Administrativo de la Función pública.

PARÁGRAFO 2°. La Oficina de Telemática de la Policía Nacional de Colombia a partir de la promulgación de la presente resolución, contara con un (01) año para realizar la entrega de los almacenes de Telemática a la Dirección Administrativa y Financiera.

PARÁGRAFO 3°. Hasta tanto no sea aprobada la nueva Estructura para la Dirección Administrativa y Financiera y se modifiquen los entornos administrativos en las unidades policiales, estos continuarán organizados y funcionando tal y como están especificados en los actos administrativos de estructura orgánica interna de las Direcciones, Policías Metropolitanas, Departamentos de Policía, y Escuelas de Policía.

ARTÍCULO 22. VIGENCIA: La presente resolución rige a partir de la fecha de expedición, y deroga la Resolución No. 02536 del 08 de julio de 2013.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C. a los

General **OSCAR ATEHORTUA DUQUE**

Director General Policía Nacional de Colombia

Elaboro: IT. Nelson Javier Peñaranda Lizcano – OFITE GARTE

Reviso: IT. Wilmer Wilmer Molano Hernández – OFPLA

MY. Jhon Mario Delgado Buenaventura - OFITE - JEFAT GUSAP

TC. John Alexander Gonzalez Perez- OFPLA

BG. Cein Castro Gutiérrez- JEFAT OFITE

BG. Ramiro Alberto Riveros Arévalo- JEFAT OFPLA

Fuente. Elaboración propia basado en la estrutura vigente.

11. Plan de operación del Grupo de Ciberseguridad

El plan de operaciones de una empresa, engloba todos los aspectos organizativos y técnicos relacionados con la elaboración de los productos y servicios prestados; contiene cuatro partes productos o servicios, procesos, programa de producción y aprovisionamiento en la gestión de existencias; esto le permite determinar y describir de manera más detallada los recursos necesarios entre ellos, humanos, tecnológicos y materiales para realizar la parte productiva y medir las variables de costo versus beneficio, para la toma de decisiones (Centro Europeo de Empresas e Innovación del Principado de Asturias, 2016)

En consecuencia, al ser la Policía Nacional de Colombia una institución pública y del Estado, le compete también la terea de planear y evaluar sus procesos y procedimientos; la Dirección de Talento Humano de la institución, es la encargada de realizar todos los trámites administrativos del personal activo de la institución y con ello evaluar, por medio de herramientas tecnológicas, el desempeño de sus unidades descentralizadas a nivel país. En su estructura organizacional cuenta con el Grupo de planeación y este a su vez con el responsable del Direccionamiento Estratégico y de Recursos, encargados de parametrizar los indicadores tanto de gestión como de producto, para poder medir los procesos administrativos que las dependencias a diario realizan.

A continuación, se presenta el esquema del Grupo de Ciberseguridad, con sus cargos, perfiles, funciones y grados, quienes deberán interiorizar el plan de operación propuesto y ponerlo en marcha, cumpliendo con cada fase propuesta. Al momento de su implementación, se deben aplicar los procedimientos estandarizados para el grupo y propender por darle cumplimiento a los indicadores propuestos por el jefe de la Oficina de Telemática de la Institución.

Ilustración 9 Esquema del Grupo de Ciberseguridad

Fuente. Elaboración propia.

En esta sección se describen las diversas fases de la elaboración del plan de operación del grupo, que son las siguientes:

1. Fase I – Iniciación
2. Fase II – Análisis
3. Fase III- Producción y ejecución
4. Fase IV – Seguimiento y evaluación

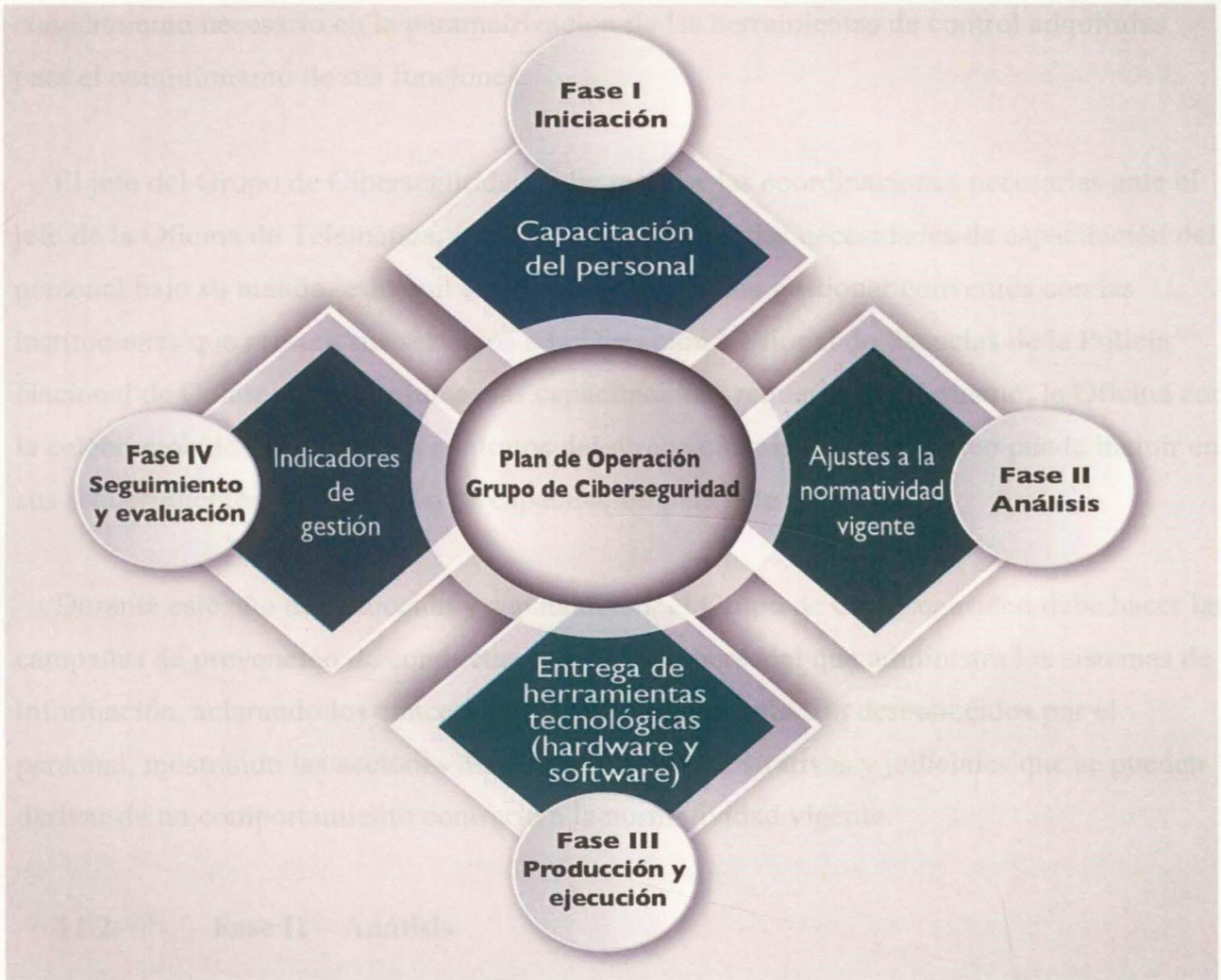


Ilustración 10 Plan de Operación del Grupo de Ciberseguridad

Fuente. Elaboración propia

11.1. Fase I – Iniciación:

La capacitación del personal es fundamental en el despliegue operacional de un plan de operación, se tiene estimado que durante el lapso de un año, el personal que integre el Grupo de Ciberseguridad debe ser capacitado y entrenado en temas relacionados con calidad de los datos, ciberespacio, ciberdelitos, bases de datos, programación de los lenguajes que han sido desarrollados los sistemas de información; esto con el fin de entender como interactuar con los objetos almacenados en las bases de datos y tener el

conocimiento necesario en la parametrización de las herramientas de control adquiridas para el cumplimiento de sus funciones.

El jefe del Grupo de Ciberseguridad debe realizar las coordinaciones necesarias ante el jefe de la Oficina de Telemática, con el fin de presentar las necesidades de capacitación del personal bajo su mando, esto con el fin de que se puedan gestionar convenios con las instituciones que prestan sus servicios a la Dirección Nacional de Escuelas de la Policía Nacional de Colombia y programar las capacitaciones requeridas; así mismo, la Oficina con la celebración de los diferentes contratos del direccionamiento tecnológico puede incluir en sus requerimientos, la condición de capacitación para este personal.

Durante este año de inducción y capacitación, el Grupo de Ciberseguridad debe hacer las campañas de prevención de conductas negativas al personal que administra los sistemas de información, aclarando los conceptos que para el momento son desconocidos por el personal, mostrando las acciones disciplinarias, administrativas y judiciales que se pueden derivar de un comportamiento contrario a la normatividad vigente.

11.2. Fase II – Análisis

La Policía Nacional de Colombia tiene vigente la Ley 1015 de 2006, sancionada por el Congreso de la República, por la cual se expide el régimen disciplinario, que identifica las conductas contrarias a las normas en las que pueden caer inmersos los funcionarios activos de la institución; además señala pautas que garantizan el debido proceso en las actuaciones disciplinarias, ajustándose a las demás leyes que tiene el país.

En su título VI habla de las faltas y de las sanciones disciplinarias, en el capítulo I artículo 33 se encuentra la clasificación y descripción de las faltas disciplinarias así: gravísimas, graves y leves; posteriormente, en los últimos artículos, las sanciones dependiendo del tipo de falta; es de mencionar que solo en el artículo 34 que tipifica las faltas gravísimas, en su literal 29 señala: *"Afectar los sistemas informáticos de la Policía*

Nacional.", pero este literal no es lo suficientemente objetivo, para tener el fundamento jurídico si se presentara una afectación desde el ciberespacio (Congreso de la República, 2006).

De la normatividad vigente colombiana, existe la Ley 1273 de 2009 o llamada ley de delitos informáticos; en esta norma se encuentran tipificados nueve tipos penales orientados a la protección de la información, los datos y el patrimonio económico (Congreso de la República de Colombia, 2009), de los cuales la Policía Nacional de Colombia podría tomar el de "*Acceso abusivo a un sistema informático*" *y* a través de la Inspección General realizar una modificación a la Ley 1015, adicionando un nuevo literal que trate de "*manipulación de la información almacenada desde los sistemas de información, en las bases de datos de la Institución con fines fraudulentos*".

En esta fase, se puede contemplar un tiempo de ejecución de seis meses, para realizar todo el trámite administrativo y jurídico por medio de la Inspección General de la institución y la Oficina de Telemática para agregar este nuevo literal que modifique la Resolución número 08310 del 28 de diciembre de 2016 "Por la cual se expide el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional de Colombia" y se adicione el nuevo artículo direccionado a controlar la gestión realizada por los administradores de sistemas de información, para la preservación de la calidad e integridad de la información almacenada en las bases de datos institucionales.

11.3. Fase III – Producción y ejecución:

El Grupo de Ciberseguridad debe contar con las herramientas tecnológicas, capaces de realizar el monitoreo 24/7 de las transacciones que se realicen a las bases de datos de la institución. Se debe contar con equipos de cómputo que tengan los recursos apropiados para interactuar entre los sistemas de información y las bases de datos; así mismo, el software debe permitir la parametrización de nuevas reglas del negocio, que le admita al administrador realizar las validaciones necesarias, para arrojar las alertas y restricciones

cuando los administradores de los sistemas de información ejecuten sentencias por fuera de las permitidas.

Validaciones que se deben parametrizar para ejercer control:

- No permitir que ningún usuario borre la trazabilidad que queda registrada en las tablas journal de la base de datos, enviando un correo electrónico al jefe del Grupo de Ciberseguridad y los analistas de ciberseguridad, cuando el administrador intente borrar una tabla journal.

- No permitir la inserción, actualización y eliminación de información, sin realizar primero un comité de control de cambios por parte de la Oficina, que se apruebe dicha transacción, guardando el registro de las sentencias ejecutadas por el administrador.

- Obtener un panel único de administración de vidrio en las bases de datos relacionales, mainframes, almacenes de datos y almacenes de archivos institucionales, generando reportes semanales al Grupo de Ciberseguridad, donde se reflejen los procedimientos anómalos realizados en las bases de datos.

- Creación de perfiles dinámicos, para generar automáticamente una lista blanca de objetos de datos a los que acceden regularmente las cuentas de bases de datos individuales. Así mismo, crear políticas que alerten el acceso cuando una cuenta de base de datos con perfil, intenta acceder a un objeto de datos que no está en la lista blanca.

- Debe permitir la usabilidad y escalabilidad de la herramienta, con un equilibrio automático de carga, la agrupación en clústeres y la gestión automatizada del software, para garantizar la alta disponibilidad y el funcionamiento ininterrumpido.

Para dotar totalmente en hardware y software al Grupo de Ciberseguridad, se tiene un tiempo estimado de un año, lapso en el cual, además de acondicionar el espacio físico (que

es dentro del mismo C-SIRT actual), el grupo debe estar en la capacidad de parametrizar las herramientas adquiridas, con las validaciones propuestas y tener en cuenta la posibilidad de agregar o quitar otras validaciones que para el momento sean necesarias.

Ilustración 11 Proyección de la implementación del Grupo de Ciberseguridad

Fuente. Elaboración Propia.

Para la implementación de esta fase se diseñaron dos procedimientos para estandarizar las labores del Grupo de Ciberseguridad:

1. Procedimiento 1DT-PR-0007 (Gestion de la Informacion en las Bases de Datos, Objetivo: crear un protocolo para validar la inserción, actualización o eliminación de información en las bases de datos por parte de los administradores técnicos de los sistemas de información, Alcance: inicia con la evaluación para modificar, eliminar o insertar el dato, termina con la gestión del administrador del sistema de información.)

Este procedimiento se realiza para el estudio de la calidad de los datos almacenados desde los sistemas de información, con el objetivo de crear un protocolo para validar la calidad de los datos almacenados desde los sistemas de información por el Grupo de Ciberseguridad para posteriormente ser actualizado por el dueño del proceso.

Código: 1DT-PR-0007
Fecha: 20-02-2020
Versión: 1

DIRECCIONAMIENTO TECNOLÓGICO

GESTION DE LA INFORMACION EN LAS BASES DE DATOS

POLICÍA NACIONAL

OBJETIVO: Crear un protocolo para validar la inserción, actualización o eliminación de información en las bases de datos por parte de los administradores técnicos de los sistemas de información.

ALCANCE: Inicia con la evaluación para modificar, eliminar o insertar el dato, termina con la gestión del administrador del sistema de información.

DOCUMENTO ENTRADA	TAREA	DOCUMENTO SALIDA	DESCRIPCIÓN	CARGO DEL RESPONSABLE	PUNTO DE CONTROL	DOCUMENTO ASOCIADO	FUNDAMENTO LEGAL
Comunicación Oficial.	1. Evaluar la solicitud de eliminar, insertar o modificar el dato		Realizar la verificación de la solicitud, que debe ser enviada por escrito mediante comunicación oficial. El requerimiento debe ser hecho por el dueño del proceso y apoyado por el jefe de la oficina, dirección, metropolitana o departamento.	Analista y Desarrollador (A) de Sistemas de Información		1DT-MA-0001 Manual del Sistema de Gestión de Seguridad de la información para la Policía Nacional.	CONSTITUCION POLITICA DE COLOMBIA. LEY 906 del 2004. LEY 1015 DE 2006 Por medio de la cual se expide el Régimen Disciplinario para la Policía Nacional. 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 se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". LEY ESTATUTARIA 1581 DE 2012 Por la cual se dictan disposiciones generales para la protección de datos personales. LEY 1712 DE 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Resolución 04691 del 29/09/2017 "por medio de la cual se adopta el índice de Información Clasificada y Reservada para la Policía Nacional".
	1 NO 2. ¿Proviene de usuario funcional? SI		El administrador del sistema de información, verifica que la fuente de origen sea el funcionario de la unidad descentralizada dueña del proceso y que es veridico el apoyado del comandante de la unidad.	Analista y Desarrollador (A) de Sistemas de Información			
	3. Realizar la búsqueda en base de datos.	Consulta en las bases de datos.	El administrador del sistema de información, realiza la respectiva busqueda en la base de datos, donde debe validar los datos que existen, comparandolos los ajustes del requerimiento presentado por el usuario funcional.	Analista y Desarrollador (A) de Sistemas de Información			
	4. Preconfigura el cambio en el sistema	Gestión en las bases de datos.	la gestión a realizar por parte del administrador del sistema de información, puede ser insertar, eliminar o modificar los datos almacenados, teniendo en cuenta el tipo de solicitud.	Analista y Desarrollador (A) de Sistemas de Información			
	5. Autorización por parte del grupo de ciberseguridad y dueño del proceso	Caso SIGMA	Al grupo de ciberseguridad y al administrador funcional del sistema, le llega un caso SIGMA del procedimiento que va a realizar el administrador. El dueño del proceso con el administrador funcional autorizan o no el procedimiento en el mismo SIGMA y el jefe del grupo de ciberseguridad en la herramienta tecnológica, aprueba la transacción para que el sistema actualice y tome los cambios realizados.	• Dueño de la Información • Administrador Funcional del Sistema de Información • Analista de Ciberseguridad			
	1 NO 6. ¿Es viable la solicitud? SI	Comunicación Oficial	Se proyecta el comunicado oficial al peticionario por parte del administrador del sistema de información, donde se explique al detalle la gestión realizada, debe ir con el apoyado del jefe del grupo de ciberseguridad y el administrador funcional del sistema de información.	• Dueño de la Información • Analista y Desarrollador (A) de Sistemas de Información • Administrador funcional del Sistema de Información • Jefe grupo de de Ciberseguridad	QUE: Se cumplan los parámetros establecidos en el procedimiento 1DT-PR-0007, para la gestión de la información en las bases de datos. QUIEN: Jefe Grupo Ciberseguridad. Administrador funcional del sistema de información CUANDO: Exista la solicitud para la gestión de los datos almacenados EVIDENCIA: comunicación oficial.		
	7. Notificar al solicitante	Comunicación Oficial	Enviar al solicitante comunicación oficial, con el concepto del jefe del grupo de ciberseguridad y el administrador funcional del sistema de información, manifestando la no viabilidad a la solicitud, soportada jurídicamente, de acuerdo a las disposiciones generales para la protección de datos personales, y a lo ordenado en el Art 244 de la ley 906 de 2004.	• Dueño de la Información • Analista y Desarrollador (A) de Sistemas de Información • Administrador funcional del Sistema de Información • Jefe grupo de de Ciberseguridad	QUE: Emitir Respuesta QUIEN: administrador técnico del sistema de información, jefe del grupo de ciberseguridad, dueño de la información CUANDO: no sea viable la gestión solicitada. EVIDENCIA: comunicación oficial.		

ANEXOS:

GLOSARIO:
- **Propietario de Activos de Información:** funcionario, unidad organizacional que tiene responsabilidad aprobada del alto mando por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos
- **Responsable Información:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

ELABORÓ	REVISÓ:	APROBÓ:
IT. NELSON JAVIER PEÑARANDA LIZCANO **Analista y Desarrollador de Sistemas de Información**	**CT. JOHN ALBEIRO GUEVARA PULIDO** **Jefe Grupo Seguridad de la Información**	**BG. CEIN CASTRO GUTIÉRREZ** **Jefe Oficina de Telemática**

Ilustración 12 Procedimiento para la Gestión de la Información en las Bases de Datos

Fuente. Elaboración Propia.

2. Procedimiento 1DT-PR-0008 (Estudio de la Calidad de los Datos Almacenados desde los Sistemas de Información, Objetivo: crear un protocolo para validar la calidad de los datos almacenados desde los sistemas de información por el grupo de ciberseguridad para posterior ser actualizado por el dueño del proceso, Alcance: inicia con la evaluación de la solicitud para revisar los datos almacenados y termina con la gestión realizada por el analista de ciberseguridad e informe a la Inspección General.)

Este procedimiento es para la Gestión de la Información en las Bases de Datos, con el objetivo de crear un protocolo para validar la inserción, actualización o eliminación de información en las bases de datos por parte de los administradores técnicos de los sistemas de información.

La Policía Nacional de Colombia está certificada con la norma ISO 9001, que se define como el estándar internacional que especifica los requisitos para un sistema de gestión con calidad (SGC); por ende, para la creación de un procedimiento, se debe cumplir rigurosamente con el protocolo establecido en la Suite Visión Empresarial, que es el sistema donde se almacenan todos los procesos y procedimientos estandarizados por la Institución. Cuando una dependencia de la Policía Nacional diseña un procedimiento, debe pasar por la Oficina de Planeación y la Secretaría General, quienes revisan la propuesta y dan o no viabilidad para su implementación, de ser positiva el resultado de la propuesta, el Grupo de Planeación de la dependencia sube Suite Visión Empresarial el nuevo procedimiento, el cual debe ser cumplido en su totalidad para evitar hallazgos en las auditorias.

A continuación, se muestra el procedimiento 1DT-PR-0008, diseñado con el propósito de validad la calidad de los datos almacenados desde los sistemas de información y su protocolo a seguir para que los dueños del proceso gestionen la actualización de manera correcta de los datos.

Código: 1DT-PR-0008 Fecha: 20-02-2020 Versión: 1	DIRECCIONAMIENTO TECNOLÓGICO ESTUDIO DE LA CALIDAD DE LOS DATOS ALMACENADOS DESDE LOS SISTEMAS DE INFORMACIÓN	POLICÍA NACIONAL

OBJETIVO: Crear un protocolo para validar la calidad de los datos almacenados desde los sistemas de información por el grupo de ciberseguridad para posterior ser actualizado por el dueño del proceso

ALCANCE: inicia con la evaluación de la solicitud para revisar los datos almacenados y termina con la gestión realizada por el analista de ciberseguridad e informe a la Inspección General.

DOCUMENTO ENTRADA	TAREA	DOCUMENTO SALIDA	DESCRIPCIÓN	CARGO DEL RESPONSABLE	PUNTO DE CONTROL	DOCUMENTO ASOCIADO	FUNDAMENTO LEGAL
Comunicación Oficial.	1. Evaluar la solicitud de revisar y actualizar los datos		Realizar la verificación de la solicitud, que debe ser enviada por escrito mediante comunicación oficial. El requerimiento debe ser hecho por un funcionario que pertenezca a ese proceso y apoyado por el jefe de la Dirección.	• Analista de ciberseguridad			CONSTITUCION POLITICA DE COLOMBIA. Ley 734 del 2002 "Por la cual se expide el Código Disciplinario Único". "SIJUR" LEY 962 de 2005, "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados." Ley 1015 del 2006 "Regimen Disciplinario Policia Nacional". "SIJUR" 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 se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". LEY ESTATUTARIA 1581 DE 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
	2. ¿Es viable el requerimiento y ajustado en derecho? (NO → 1)		El administrador técnico del sistema de información, con el asesor jurídico de la Oficina de Telemática y el jefe del grupo de ciberseguridad, analizan el requerimiento y aprueban o no la intervención al sistema de información	• Asesor jurídico OFITE • Jefe grupo de ciberseguridad • Administrador técnico del sistema de información			
	3. Realizar el cronograma de trabajo para mejorar la calidad del dato	Cronograma de actividades	El analista del grupo de ciberseguridad, realiza el cronograma para atender tres requerimientos de este tipo anualmente, con fechas y tiempos estimados en cada proceso de revisión.	• Analista de ciberseguridad			
	4. ¿Existe disponibilidad? (NO → 1)		El jefe del grupo de ciberseguridad, revisa la disponibilidad de su personal, respecto a los requerimientos recibidos.	• Jefe grupo de ciberseguridad			
	5. Hacer el procedimiento solicitado por el dueño del proceso	Gestión en las bases de datos.	El analista del grupo de ciberseguridad, debe realizar el proceso de calidad del dato, haciendo búsquedas aleatorias de la información almacenada en las bases de datos, con la información física (soportes documentales) allegada por la unidad.	• Dueño de la Información • Analista de Ciberseguridad	QUE: se cumplan los parámetros establecidos en el procedimiento 1DT-PR-0008, para revisar las bases de datos QUIEN: Jefe Grupo Ciberseguridad, analista de ciberseguridad CUANDO: Exista la solicitud que cumpla con los requisitos EVIDENCIA: comunicación oficial.		
	6. Informar a la unidad solicitante, la gestión realizada	Comunicación Oficial	El grupo de ciberseguridad, emite concepto técnico de todos los hallazgos encontrados, para que el usuario funcional y el dueño de la información deleguen la función de actualizar los datos.	• Dueño de la Información • Jefe grupo de ciberseguridad • Administrador Funcional del Sistema de Información • Analista de Ciberseguridad	QUE: Emitir Respuesta QUIEN: analista de ciberseguridad, jefe del grupo de ciberseguridad. CUANDO: se culmine el procedimiento de revisión EVIDENCIA: comunicación oficial.	1DT-MA-0001 Manual del Sistema de Gestión de Seguridad de la información para la Policía Nacional.	
	7. Documentar y evidenciar	Comunicación Oficial	Los hallazgos encontrados en la calidad de la información almacenada en las bases de datos, se debe documentar en un comunicado oficial, para determinar en el comité de seguridad de la información, la gravedad del caso y tomar decisiones.	• Jefe grupo de ciberseguridad • Comité seguridad de la información			
	8.¿Conducta penal o disciplinaria? (NO → 10; SI → 9)						
	9. Informar a la Inspección General de la Policía Nacional	Comunicación Oficial	Enviar la información del caso y la trazabilidad de la información, con el fin se realicen las acciones pertinentes, por parte del ente investigador y defina si la conducta se encuentra tipificada como penal o disciplinaria	• Asesor jurídico OFITE • Jefe grupo de ciberseguridad • Analista de ciberseguridad			
	10. Identificación de lecciones aprendidas	Comunicación Oficial	la lección aprendida debe llevar a identificar patrones, áreas críticas, implementación de acciones preventivas para reducir la probabilidad de futuros incidentes, estas deben ser consignadas en el formato de atención a incidentes y enviadas (numeral 16. lecciones aprendidas del formato de atención de incidentes) mediante comunicado oficial al responsable del activo	• Jefe grupo de ciberseguridad • Analista de ciberseguridad			

ANEXOS:

GLOSARIO:

- **BASE DE DATOS:** datos registrados en bases mecánicas, magnéticas u otros similares.
- **CIBERSEGURIDAD:** es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

ELABORÓ	REVISÓ:	APROBÓ:
IT. NELSON JAVIER PEÑARANDA LIZCANO **Analista y Desarrollador de Sistemas de Información**	**CT. JOHN ALBEIRO GUEVARA PULIDO** **Jefe Grupo Seguridad de la Información**	**BG. CEIN CASTRO GUTIÉRREZ** **Jefe Oficina de Telemática**

Ilustración 13 Procedimiento para el estudio de la calidad de los datos almacenados desde los sistemas de información

Fuente. Elaboración Propia.

11.4. Fase IV – Seguimiento y evaluación:

En esta última fase con una duración indefinida y un total de tiempo de tres años desde la creación del Grupo de Ciberseguridad, se pretende hacer seguimiento al cumplimiento de las funciones y planes asignadas al grupo, por medio de indicadores con los que se medirá la gestión realizada por el jefe del grupo y sus analistas, de ello depende la evaluación y calificación que se realiza mensualmente, la cual es registrada en el formulario de evaluación y seguimiento; aunado a lo anterior, y por medio de estos indicadores, directamente se evaluará al jefe de la Oficina de Telemática, con el fin de crear un nivel de compromiso más alto en el desarrollo de las actividades asignadas (Dirección General, 2019).

Un indicador es una expresión cualitativa o cuantitativa, que permite describir características propias frente a comportamientos o fenómenos de la realidad, según la evolución de una variable o el establecimiento de una relación entre variables diseñadas o parametrizadas por el dueño del proceso, donde su resultado es frecuentemente comparado con períodos (diario, semanal, mensual, trimestral o anual) anteriores, metas o compromisos, permitiendo evaluar el desempeño y su evolución en el tiempo (DANE, 2009).

La adopción de los indicadores en la Institución se realizó con el fin de unificar metas, temporizadores, responsables, fórmula y ficha técnica; los indicadores son medidos de acuerdo con las necesidades planteadas y dependiendo del tipo de indicador: eficacia, efectividad o eficiencia. Esta acción es realizada en la Suite Visión Empresarial, que es una herramienta gerencial utilizada para definir y hacer seguimiento a la estrategia de la Institución, por parte de los dueños y responsables de procesos, direcciones y oficinas asesoras, comandantes de departamento, policías metropolitanas y directores de escuelas, con la meta establecida y para generar la línea base según sea el caso.

Los indicadores propuestos, deben estar alineados al objetivo estratégico del Direccionamiento Tecnológico el cual es: diseñar y ejecutar el plan estratégico de tecnologías de la información y las comunicaciones para el servicio de policía.

Así mismo, al objetivo del proceso que es: diseñar y ejecutar el plan estratégico de tecnologías de la información y las comunicaciones para el servicio de policía, orientado a garantizar la oportunidad, calidad y seguridad de la información, para que el uniformado preste un servicio efectivo a la ciudadanía.

En la Policía Nacional de Colombia, el director o jefe de la unidad debe ordenar al Grupo de Planeación de la unidad, realizar los indicadores que estime pertinentes para tener y poder evaluar la gestión que realiza el personal bajo su mando; luego de tener estos indicadores, se remiten mediante comunicado oficial a la Oficina de Planeación y la Secretaría General, quienes revisan la solicitud y le dan la viabilidad o no correspondiente, para luego ser subidos a la Suite Visión Empresarial, que es la herramienta gerencial diseñada para evaluar la gestión realizada por los comandantes y el personal bajo su mando.

El Grupo de Ciberseguridad deberá cumplir con los siguientes tres indicadores, los cuales están dirigidos a medir la efectividad, eficacia y eficiencia;

1. Índice de disminución de incidentes que comprometen la integridad de la información (EFECTIVIDAD).

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informacióny las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

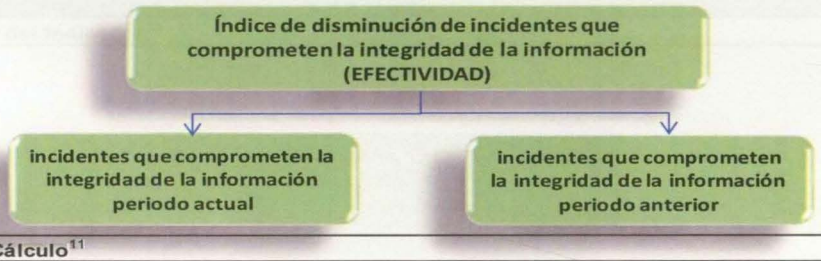
Nombre del Indicador[3]	Temporizador[4]
Índice de disminución de incidentes que comprometen la integridad de la información (EFECTIVIDAD)	Mensual

Descripción / Intención del Indicador[5]

Indicador que establece el índice de disminución histórica de los incidentes que se identifican a través de la parametrización de la herramienta tecnológica.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Porcentaje	Porcentaje	Hacia Abajo	Hacia Arriba	Calculada

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

((incidentes que comprometen la integridad de la información periodo actual - incidentes que comprometen la integridad de la información periodo anterior) / incidentes que comprometen la integridad de la información periodo anterior)*100

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]
Jefe Oficina de Tlemática Policía Nacional	Lograr la disminución proyectada de incidentes que comprometen la integridad de la información. 2023= -3% 2024= -5% 2025= -7% 2026= -10%	Manual	Mensual

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informacióny las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

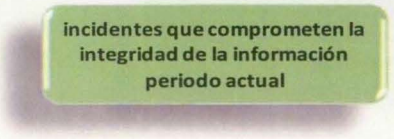
Nombre del Indicador[3]	Temporizador[4]
incidentes que comprometen la integridad de la información periodo actual	Mensual

Descripción / Intención del Indicador[5]

Variable que se extracta del reporte generado por parte del Comité de Seguridad de la Información según la gestión realizada por la herramienta tecnológica.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Incidentes	Incidentes	Sin Orientación	Sin Orientación	Manual

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informacióny las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

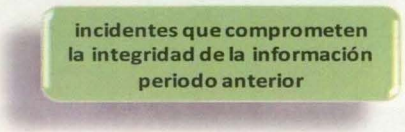
Nombre del Indicador[3]	Temporizador[4]
incidentes que comprometen la integridad de la información periodo anterior	Mensual

Descripción / Intención del Indicador[5]

Variable que se extracta de manera automática según los valores historicos para el mismo perodo del a;o anterior.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Incidentes	Incidentes	Sin Orientación	Sin Orientación	Calculada

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]

2. Tratamiento a los incidentes de ciberseguridad (EFICACIA).

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informaciónу las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

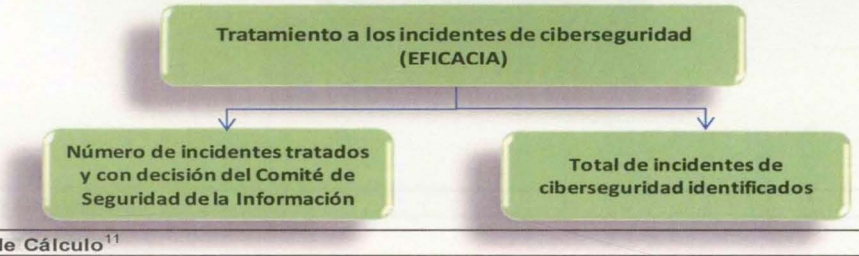
Nombre del Indicador[3]	Temporizador[4]
Tratamiento a los incidentes de ciberseguridad (EFICACIA).	Mensual

Descripción / Intención del Indicador[5]

Indicador que mide el tratamiento realizado a los incidentes de ciberseguridad identificados, garantizando que el 100% de los mismos sean socializados y presenten decisiones del Comité de Seguridad de la Información.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Porcentaje	Porcentaje	Hacia Arriba	Hacia Arriba	Calculada

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

(Número de incidentes tratados y con decisión del Comité de Seguridad de la Información / Total de incidentes de ciberseguridad identificados)*100

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]
Jefe Oficina de Tlemática Policía Nacional	Lograr que el 100% de los incidentes que comprometen la ciberseguridad sean socializados y presenten decisiones del Comité de Seguridad de la Información.	Manual	Mensual

1DE-FR-0030 Ver: 0		Aprobación: 29-04-2010

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informacióny las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

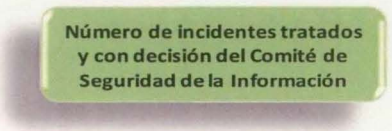
Nombre del Indicador[3]	Temporizador[4]
Número de incidentes tratados y con decisión del Comité de Seguridad de la Información.	Mensual

Descripción / Intención del Indicador[5]

Variable que establece el número de incidentes tratados y con decisión del Comité de Seguridad de la Información.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Número	Número	Sin Orientación	Sin Orientación	Manual

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

No Aplica (Manual)

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informacióny las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

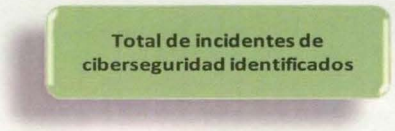
Nombre del Indicador[3]	Temporizador[4]
Total de incidentes de ciberseguridad identificados	Mensual

Descripción / Intención del Indicador[5]

Variable que establece Total de incidentes de ciberseguridad identificados en el periodo.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Número	Número	Sin Orientación	Sin Orientación	Manual

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

No Aplica (Manual)

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]

3. "Horas hombre en atención al soporte técnico de los sistemas de información (EFICIENCIA)"

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informacióny las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

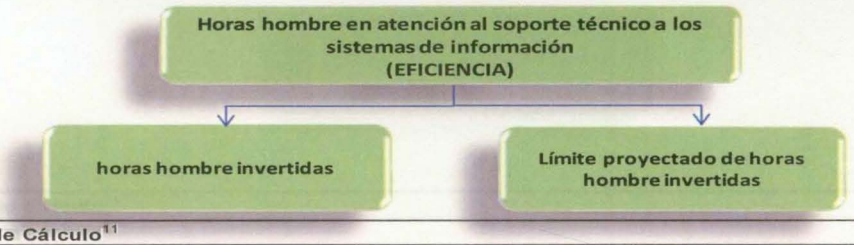
Nombre del Indicador[3]	Temporizador[4]
Horas hombre en atención al soporte técnico a los sistemas de información (EFICIENCIA)	Mensual

Descripción / Intención del Indicador[5]

Indicador que mide las horas hombre invertidas en la atención y soporte técnico a los diferentes sistemas de información de la institución, por gestión inadecuada de los administradores con altos privilegios (superusuarios) de las bases de datos.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Porcentaje	Porcentaje	Hacia Abajo	Hacia Arriba	Calculada

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

(1-((horas hombre invertidas-Límite proyectado de horas hombre invertidas)/Límite proyectado de horas hombre invertidas))*100

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]
Jefe Oficina de Tlemática Policía Nacional	Lograr que el 100% de cumplimiento al indicador al mantener dentro del rango programado, el número de horas/hombre invertidas en la atención y soporte técnico a los diferentes sistemas de información de la institución, por gestión inadecuada de los administradores con altos privilegios (superusuarios) de las bases de datos.	Manual	Mensual

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informacióny las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

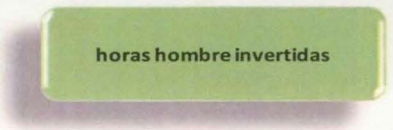
Nombre del Indicador[3]	Temporizador[4]
horas hombre invertidas	Mensual

Descripción / Intención del Indicador[5]

Variable que establece las horas hombre invertidas en el soporte técnico a los diferentes sistemas de información de la institución, por gestión inadecuada de los administradores con altos privilegios (superusuarios) de las bases de datos.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Incidentes	Incidentes	Sin Orientación	Sin Orientación	Manual

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]

POLICÍA NACIONAL	DIRECCIONAMIENTO TECNOLÓGICO	Página 1 de 1
		Código:
	FICHA TÉCNICA INDICADOR	Fecha:
		Versión:

Perspectiva/Proceso[1]	Objetivo Estratégico[2]	Objetivo Proceso[2]
DIRECCIONAMIENTO TECNOLÓGICO	DHO9 Diseñar y ejecutar el Plan Estratégico de Tecnológías de la Informacióny las Comunicaciones para el servicio de pollicía.	Disenar y ejecutar el plan estrategico de tecnologias de la informacion y las comunicaciones para el servicio de policia, orientado a garantizar la oportunidad, calidad y seguridad de la informacion, para que el uniformado preste un servicio efectivo a la ciudadanía.

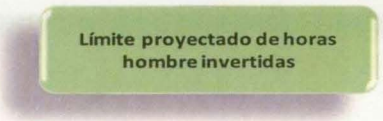
Nombre del Indicador[3]	Temporizador[4]
Límite proyectado de horas hombre invertidas	Mensual

Descripción / Intención del Indicador[5]

Variable que establece el límite establecido de horas/hombre invertidas en la atención y soporte técnico a los diferentes sistemas de información de la institución, por gestión inadecuada de los administradores con altos privilegios (superusuarios) de las bases de datos.

Unidad de Captura[6]	Unidad de Almacenamiento[7]	Orientación Valor absoluto[8]	Orientación Valor relativo[8.1]	Obtención[9]
Incidentes	Incidentes	Sin Orientación	Sin Orientación	Calculada

Árbol Dupont del Indicador[10]



Fórmula de Cálculo[11]

Responsable del Indicador[12]

Jefe Grupo Ciberseguridad

Indicador Elaborado Por[13]	Fecha de Creación[14]	Fecha Última Revisión[15]
IT. NELSON PEÑARANDA	20/02/2020	20/02/2020

Información de la meta (s)

Responsable[16]	Descripción[17]	Obtención[18]	Temporizador Meta[19]

1DE-FR-0030 Ver: 0		Aprobación: 29-04-2010

Ilustración 14 Indicadores de Gestión para el Grupo de Ciberseguridad

Fuente. Elaboración propia

La Policía Nacional de Colombia, tiene estandarizada dentro del Proceso Direccionamiento del Sistema de Gestión Integral, la Guía de herramientas de seguimiento y evaluación, cuyo objetivo es brindar los lineamientos metodológicos para la determinación de herramientas de seguimiento, medición, análisis y evaluación necesarios para asegurar los resultados válidos del Sistema de Gestión Integral (Oficina de Planeación - Policía Nacional de Colombia, 2019).

El seguimiento de los indicadores, la institución lo realiza a través de la herramienta tecnológica Suite Visión Empresarial y de acuerdo con el porcentaje de cumplimiento genera la alerta conforme a la escala de medición definida para cada indicador, esta determina el máximo o mínimo de cada semáforo, con un nivel de tolerancia. Para el seguimiento de los indicadores, la Institución define la siguiente escala de niveles de medición, comparando los avances y resultados así:

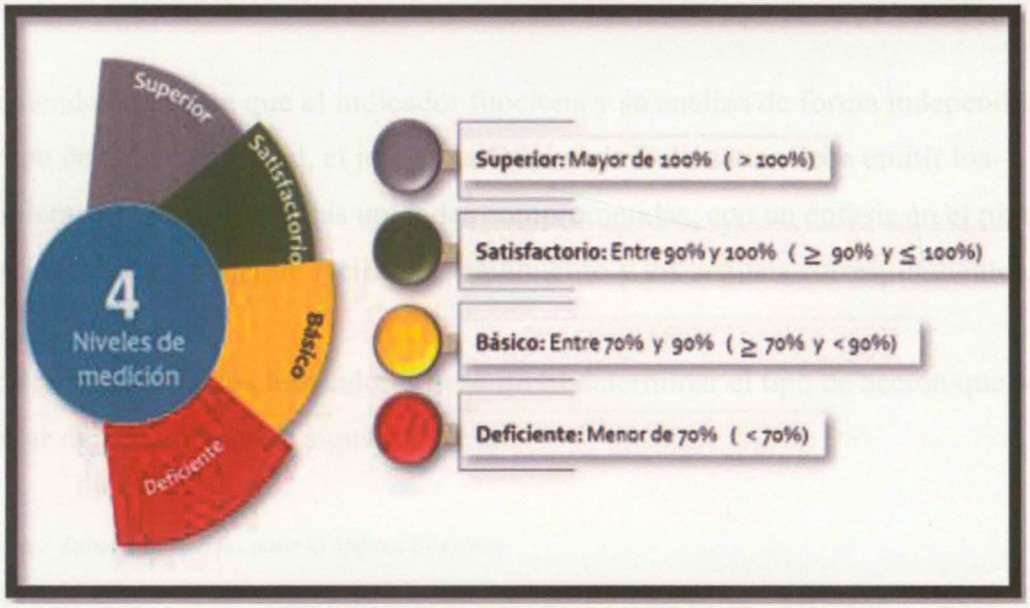


Ilustración 15 Escala de medición

Fuente. Recuperado de "Guía de herramientas de seguimiento y evaluación en la Policía Nacional de Colombia".

Conforme a los resultados presentados, se debe determinar qué tipo de acción debe formular la unidad de acuerdo a la siguiente tabla:

Tabla 6 Formulación de Acciones

Escala de indicador	Descripción
Satisfactorio	Cuando el cumplimiento del plan se encuentra situado en "satisfactorio" significa que el plan cumplió a cabalidad todas las tareas en el tiempo estipulado.
Básico	Cuando el cumplimiento del plan de acción se encuentra en estado "Básico", se refiere a que fueron cargadas algunas de sus tareas posterior a la fecha estipulada o algunas de estas se encuentran pendientes por ser alimentadas en la SVE.
Deficiente	Cuando el cumplimiento del plan este en estado de "deficiente", se refiere a que no se cumplieron las tareas propuestas para el plan de acción, por lo tanto, se deberá verificar el motivo por el cual no fueron realizadas y solicitar a la Subdirección General la modificación del mismo en caso de ser necesario.

Fuente. Recuperado de "Guía de herramientas de seguimiento y evaluación en la Policía Nacional de Colombia".

Teniendo en cuenta que el indicador funciona y se analiza de forma independiente para el Grupo de Ciberseguridad, el jefe de la Oficina de Telemática debe emitir los lineamientos o directrices a las unidades comprometidas, con un énfasis en el nivel operacional, de manera que facilite el seguimiento y los análisis correspondientes.

Los resultados de los indicadores permitirán determinar el tipo de acción que se debe formular de acuerdo con la siguiente tabla.

Tabla 7 Tabla de Criterios para la Mejora Continua

TABLA DE CRITERIOS PARA LA MEJORA CONTINUA		
Escala de indicador	**Acción**	**Ejemplo**
Superior	Solicitar aumento de meta o cambio de indicador (Comunicación oficial) al dueño del proceso y este a su vez a la	

	Oficina de Planeación, siempre y cuando, el indicador evidencie tendencia de sobrepaso en más de dos periodos consecutivos (aplica para medición trimestral). En caso de que la meta sea anual, con seguimiento periódico (mensual), se realizará solicitud de cambio de meta solo hasta que finalice la vigencia donde se corrobore el cumplimiento o no de la meta anualizada planteada. Para los indicadores semestrales que en dos periodos se muestren en escala superior deberán solicitar aumento de meta o cambio de indicador (Comunicación oficial) al dueño del proceso y este a su vez a la Oficina de Planeación. Por último, si la medición anual presenta en un periodo escala superior se deberá solicitar aumento de meta o cambio de indicador (Comunicación oficial) al dueño del proceso y este a su vez a la Oficina de Planeación.	La meta del indicador es 95% y el resultado, durante el trimestre 1, 2 y 3 se encuentra en la escala "superior", durante el trimestre 4 deberá solicitar mediante comunicación oficial al dueño de proceso el aumento de la meta para el próximo año. Si la meta es semestral y se tiene un cumplimiento durante dos mediciones consecutivas en escala superior deberá solicitar al dueño del proceso y este a la Oficina de Planeación el respectivo aumento de la meta para el próximo año. Las metas de las tasas son de evaluación anual, pero estas se particionan para realizarse un seguimiento mensual y para cada mes se determina una meta, la cual se acumula hasta finalizar la vigencia, por tanto, si la meta es superada en los periodos mensuales 1, 2 y 3 no debe modificarse la meta programada para los periodos posteriores, hasta que se corrobore que fue superada la meta anualizada planteada. Cuando se tienen resultados de indicadores anuales y su resultado es superior deberá solicitar el aumento de la meta.
Satisfactorio	**No requiere acción,** deberán realizar el análisis en los campos establecidos de la SVE de las acciones	El Indicador "X" en el trimestre 1, se encuentra en la escala "Satisfactorio" por lo tanto no requiere de acción solo análisis en la SVE.

	que realizaron para lograr el cumplimiento del indicador. Sin embargo, cuando el indicador presente escala satisfactoria como se estipula en el ejemplo superior deberán solicitar el cambio del indicador o cambio de meta al dueño del proceso mediante comunicación oficial y este lo enviará a la Oficina de Planeación para ser revisado.	El mismo indicador "X" en los siguientes resultados de su medición trimestral 2, 3 y 4, se evidencia satisfactorio o paso a superior deberá solicitar cambio de meta o medición.
Básico	**Requiere avance significativo (plan de trabajo en módulo mejora de la SVE).** Excepto si el indicador presenta mejora en el resultado pasando de estado de "deficiente" a "básico", o tiene vigente una acción correctiva o un plan de trabajo.	Cuando del indicador se encuentra en estado "básico", se debe proceder a verificar que aspectos están influyendo al incumplimiento del indicador, para finalmente formular un avance significativo "plan de trabajo".
Deficiente	**Acción correctiva en módulo mejora de la SVE** Excepto si el indicador ya tiene vigente una acción correctiva.	Bajo cualquier circunstancia que el resultado del indicador, se encuentre en la escala deficiente, se realiza acción correctiva, sin embargo, si se encuentra vigente una acción por el indicador no se apertura una nueva, solo se realiza la revisión de las tareas si son pertinentes para conseguir una mejora en el resultado, (estos tiempos se manejan como lo estipula la Guía para la mejora 1MC-GU-0006).

Fuente. Recuperado de "Guía de herramientas de seguimiento y evaluación en la Policía Nacional de Colombia".

Es importante tener en cuenta que los indicadores sirven como instrumento para evaluar objetivos, actividades y metas de la Policía Nacional de Colombia, permite a los señores directores y jefes de oficinas asesoras, conocer el grado de avance y desarrollo de todas las actividades en todos los niveles de gestión, como lo es (táctico, estratégico y operacional). Teniendo en cuenta lo anterior es importante dejar claro que los indicadores están a cargo de los dueños de los procesos, previo concepto de validación por parte de la Oficina de Planeación. Así mismo, una vez se tenga definido, aprobado y cumpliendo con todos los requisitos establecidos, se debe realizar la parametrización del indicador en la Suite Visión Empresarial, de tal manera que su análisis y seguimiento se haga por esta herramienta.

12. Conclusiones

1. Los sistemas de información, optimizan el trabajo realizado por los empleados de una empresa, generando la mejora continua en los procesos y procedimientos que se ejecutan. La seguridad de la información que se emplea para garantizar la confidencialidad y la disponibilidad de los datos es de gran importancia; más aún, se debe garantizar la integridad y calidad de la información almacenada en las bases de datos para que desde el ciberespacio no se materialice ninguna amenaza.

2. El resultado de las entrevistas fue positivo para la investigación, teniendo en cuenta que para el Grupo de Seguridad de la Información y los administradores técnicos de los sistemas, es imprescindible la creación del grupo de Ciberseguridad.

3. Aplicando el procedimiento que la Oficina de Planeación tiene estandarizado para modificar la estructura interna de una dependencia; se diseño y estructuro el Grupo de Ciberseguridad, enfocado a controlar y monitorear el trabajo realizado por los administradores técnicos de sistemas de información de la Oficina de Telemática de la Policía Nacional.

4. La implementación del Grupo de Ciberseguridad, le aportará al proceso misional de administración de la información, garantizando la integridad y calidad de los datos almacenados desde los sistemas de información en las bases de datos, beneficiando a la institución en factores como: efectividad en las tareas realizadas,

optimización de los recursos tecnológicos, avances institucionales con relación a la seguridad de la información y blinda a la institución ante posibles requerimientos judiciales o administrativos por permitir la vulneración de la Ley 1581 de 2012.

5. Con la creación del Grupo de Ciberseguridad, la Oficina de Telemática de la Policía Nacional de Colombia, garantizará la calidad e integridad de los datos almacenados desde los sistemas de información y manipulados desde el Ciberespacio.

13. Referencias

Abrego Almazán, D., Sánchez Tovar, Y., & Medina Quintero, J. M. (2017). Influencia de los sistemas de información en los resultados organizacionales. *Contaduria y Administracion*. https://doi.org/10.1016/j.cya.2017.03.001

Aguirre, J. (2015). Inteligencia estratégica: un sistema para gestionar la innovación. *Estudios Gerenciales*. https://doi.org/10.1016/j.estger.2014.07.001

Asobancaria. (2018). La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. *Semana Económica*.

Ajzen, I. (2014). *la teoría del Comportamiento Planificado.* New Jersey: Health Psychology Rewiew.

Belloch, C. (2012). Las Tecnologías de la Información y Comunicación en el Aprendizaje.

Bernal, C. (2010). Metodología de la investigación. In *México: Editorial Mc ....*

Bertoglio, O. J. (1994). *Introducción a la Teoría General de Sistemas.* Noriega Editores.

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*. https://doi.org/10.1016/S1353-4858(16)30086-1

Chicano Tejada, E. (2014). Gestión de Incidentes de Seguridad Informática. In *proyecto Amparo*.

Colombia. (1991). Constitucion Politica de Colombia. *Journal of Chemical Information and Modeling*. https://doi.org/10.1017/CBO9781107415324.004

Comunicaciones, M. de T. de la I. y las. (2017). Impacto de los Incidentes de Seguridad Digital en Colombia 2017. *Informacion Tecnologica*.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. *Serie de Tratados*

Europeos. https://doi.org/BOE-A-2012-5403

Congreso de la República de Colombia. (2012). *Ley 1581 de protección de datos personales.* Bogotá: Congreso.

Congreso de la Reública de Colombia. (2009). *Ley 1273 de 2009"de la protección de la información y de los datos".* Bogota: Diario Oficial.

Cortés Borrero, R. (2015). Estado Actual de la Política Pública de Ciberseguridad y Ciberdefensa en Colombia. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*. https://doi.org/10.15425/redecom.14.2015.06

DANE. (2009). *Metodología Linea Base de Indicadores.* Bogotá: Dirección de Regulación, planeación, estandarización y normalización - DIRPEN.

Departamento Nacional de Planeación. (2006). *Documento CONPES 3437.* Bogotá: Diario Oficial.

Departamento Nacional de Planeacion. (2011). Documento CONPES 3701. *Lineamientos de politica para Ciberseguridad y Ciberdefensa*, 1-43.

Departamento Nacional de Planeacion. (2016). Documento CONPES 3854. *Politica Nacional de Seguridad Digital*, 1-91.

Dirección General . (2019). *Resolución 05884 "Manual para la administración de los recursos logísticos".* Bogotá: Policía Nacional.

Dirección General - Policía Nacional. (2006). *Directica transitoria nro 077 - Pagina web.* Bogotá: Policía Nacional.

Dirección General. (2019). *Resolución 01233 "Por la cual se adopta la matriz de indicadores asociados a los procesos de la Policía Nacional".* Bogotá: Policía Nacional.

Direccion General de la Policia Nacional . (2016). *Resolucion 05309 del 24 de agosto 2016, "por la cual se establecen las tablas deorganizacion policial TOP".* Bogota: Oficina de Planeacion.

Direccion General de la Policía Nacional. (2002). *Directiva NRO. 004 Implementacion A Nivel Nacional Del Nuevo Sistema De Administracion De Talento Humano SIATH.* Bogota.

Dirección General de la PolicÍa Nacional. (2019). *Resolución 03374 del 20019 "Por la cual se adopta la declaración de prácticas de certificación digital".* Bogotá : Policía Nacional.

Dirección General Policía Nacional. (2017). *Resolución 03253 del 2017 "Por la cual se adopta el formato único de orden de comparendo y/o medida correctiva".* Bogotá: Policía Nacional.

Dirección General. (2019). *Resolución 00760 Estructura Orgánica Interna de la DIJIN.* Bogotá: Policía Nacional.

Dirección General Policía Nacional. (2019). *Resolución 00941 del 2019 "por la cual se reglamenta el sistema adenunciar".* Bogotá: Policía Nacional.

Dirección General. (2019). *Resolución 00760 Estructura Orgánica Interna de la DIJIN.* Bogotá: Policía Nacional.

Direccion General Policía Nacional de Colombia. (2013). *Aplicabilidad Portal de Servicios Internos (PSI).* Bogota.

Direccion Policia Nacional de Colombia. (2016). Resolución No. 00937 del 10 de Marzo DE 2016 . *Manual de funciones para el personal uniformado de la Policia Nacional*, 12.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*. https://doi.org/10.4236/jis.2013.42011

EcuRed contributors. (08 de 08 de 2019). *Enfoque sistémico*. Obtenido de https://www.ecured.cu/index.php?title=Enfoque_sist%C3%A9mico&oldid=349327

El Concepto de Responsabilidad Social de la Empresa. (2018). *Economía*.

Enciso, B. (2018). Teoría General De Sistemas: In *La biblioteca, bibliosistemática e información*. https://doi.org/10.2307/j.ctv51307z.7

Fabiano Couto Corrêa. (2016). Gestión de datos de investigación. In *EPI scholar*.

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. In *Symantec Security Response*. https://doi.org/20 September 2015

Garcia, O. A., Gonzalez, H. A., Luis, R. M., & Elmer, R. C. (2015). Sistemas De Informacion Gerencial. *Universidad Don Bosco*. https://doi.org/10.1017/CBO9781107415324.004

Gomez Bastar, S. (2012). Metodologia de la investigacion. In *Red Tercer Milenio S.C.* https://doi.org/- ISBN 978-92-75-32913-9

González Longatt, F. M. (2007). Introducción a los Sistemas de Información: Fundamentos. *Sistemas de Información*.

Gutierrez, J. M. (2008). Sistemas Expertos Basados en Reglas.

Hernan gómez de Mateo, J. L. (2014). Dilemas cibernéticos y la estrategia de seguridad nacional. In *ieee.es - Instituto Español de Estudios Estratégicos*.

Hernández Sampieri, R., Fernandez Collado, C., & Lucio, B. (2014). *Metodología de la Investigación.* Mexico: McGraw-Hill.

Inc, IDG Communications. (23 de 02 de 2018). *Computerworld Colombia*. Obtenido de https://computerworld.co/el-cibercrimen-cuesta-600-000-millones-de-dolares-la-economia-mundial/?unapproved=1194&moderation-hash=1bb8a4fb27e63a967a3d330406eadd72#comment-1194

K Newmeyer, E Cubeiro, M. S. (2015). Ciberespacio, Ciberguridad Y Ciberseguridad. *II Simposio Internacional de Seguridad y Defensa: Perú 2015.*

Karen, D. (2015). La toma de decisiones de la empresa. *Sistema de Información Para La Toma de Decisiones*.

Kenneth e. Kendall, & julie e. Kendall. (2011). Analisis y Diseño de Sistemas. In *Pearson*.

kyocera. (2018). *Kyocera Document Solutions*. Obtenido de http://smarterworkspaces.kyocera.es/blog/los-6-principales-tipos-sistemas-informacion/

Leopold, H. (2013). Business Process Management. In *Lecture Notes in Business Information Processing*. https://doi.org/10.1007/978-3-319-04175-9_1

Liu, X., Lftikhar, N., & Xie, X. (2014). Survey of real-time processing systems for big data *ACM International Conference Proceeding Series*. https://doi.org/10.1145/2628194.2628251

Mankiw, G. N. (2012). Principios de economía. In *Sección de Obras de Economía*.

Martínez Gómez, J., Higuera Marín, M., & Aguilar Díaz, E. (2013). Enfoque metodológico para el diseño de interfaces durante el ciclo de vida del desarrollo de software. *Gerencia Tecnológica Informática*.

Neira, A. L., & Spohr, J. R. (2010). Sistema de Gestión de la Seguridad de la Información. *Www.Iso27000.Es*.

Niño Camazón, J. (2011). Introdicción a los sistemas informáticos. In *Sistemas operativos monopuesto*. https://doi.org/8497719719

Niemimaa, E. &. (2017). Information systems security policy implementation in practice: from best practices to situated practices . *European Journal of Information Systems*

Oficina de Planeación - Policía Nacional. (2019). *Guía de herramientas de seguimiento y evaluación.* Bogotá: Policía Nacional.

Oficina de Planeacion Policía Nacional. (2016). *Resolución 00937, Manual de Funciones.* Bogotá: Policía Nacional de Colombia.

Oficina de Planeación Policía Nacional de Colombia. (2016). *Resolución 05309, por la cual se establecen las TOP.* Bogotá : Policía Nacional.

Organizacion de los Estados Americanos "OEA". (2004). Estrategia de Ciberseguridad Cibernetica. *CICTE*, 2-14.

Organización de los Estados Americanos OEA. (16 de 07 de 2015). Buenas prácticas para establecer un CSIRT Nacional. *Seguridad Cibernética*. Obtenido de https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Organización de los Estados Americanos OEA. (2015). Metodología de Respuesta a Incidentes (IRMs) IRM10-IngenieriaSocial-OEA. *Seguridad Ciberética.*

Pérez-Montoro, M. (2010). Arquitectura de la información en entornos web. *El Profesional de La Informacion*. https://doi.org/10.3145/epi.2010.jul.01

Policía Nacional De Colombia. (2013). *Resolución número 02536 de 08 de julio.* Bogota: Policía Nacional De Colombia.

Policía Nacional de Colombia. (2016). *Resolución número 08310 de 28 dic.* Bogota : Policía Nacional .

Policía Nacional de Colombia. (05 de 11 de 2018). *Oficina de Telemática de la Policía Nacional*. Obtenido de https://www.policia.gov.co/oficinas-asesoras/telematica

Policía Nacional de Colombia. (25 de 06 de 2018). *POLIRED*. Obtenido de http://polired/Institucion/NivelAsesor/Oftelematica/default.aspx

Ramos, M. A. (1993). Los directivos y los sistemas de informacion. *Dirección y Progreso*.

Ramos, L. (2009). Seguridad De La Informacion. *Gerencia General de Tecnologias de La Información-Agencia de Recaudación de La Provincia de Buenos Aires (Arba)*.

República, c. d. (2006). *Ley 1015 DE 2006.* Bogota: La Gaceta del Congreso.

República, c. d. (2012). *Ley Estatutaria 1581 DE 2012.* Bogota: La Gaceta del Congreso.

Revista Dinero. (26 de 09 de 2017). Los sectores económicos más impactados por el cibercrimen en Colombia. *Dinero*, 5. Obtenido de https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

Revista, Gestión. (01 de 02 de 2016). Empresas invierten cada vez más en sistemas de seguridad informática. *Gestión*, 1-5. Obtenido de https://gestion.pe/tecnologia/empresas-invierten-vez-sistemas-seguridad-informatica-144913-noticia/

Rodríguez, D., & Valldeoriola, J. (2010). Metodología de la investigación. *Universitat Oberta de Catalunya*, 613. Retrieved from http://www.casadellibro.com/libro-metodologia-de-la-investigacion-5-ed-incluye-cd-rom/9786071502919/1960006

Román, J. L. (2016). La Transformación Digital de la Industria. *Conferencia de Directores*

y Decanos de Ingeniria Informatica. https://doi.org/10.1080/14015430802688385

Ruus, V. R., & Reiska, P. (2015). Estonia. In *The Education Systems of Europe, Second Edition*. https://doi.org/10.1007/978-3-319-07473-3_14

Sampieri, R. H., Collado, C. F., María, D., Lucio, B., Valencia, S. M., Paulina, C., & Torres, M. (2014). Dr. Roberto Hernández Sampieri. *Mc Graw Hill*.

Sánchez Medero, G. (2012). La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom*.

Secretaría General - Policía Nacional. (2011). *Directiva administrativa permanente "Implementación del Sistema IPD"*. Bogotá: Policía Nacional.

Secretaria General Policía Nacional. (2016). *Resolución 5633 de 2016 "Infraestructura tecnológica para el proceso de autenticacción biometrica"*. Bogotá: Policía Nacional.

Secretaria General Policía Nacional. (2017). *Resolución número 06581 "Por la cual se actualizan los lineamientos generales de implementación y fortalecimiento del aplicativo GECOP"*. Bogota: Policía Nacional.

Sierra, G., Escobar, B., Gago, S., Navarro, T., & Rocha, C. (2007). Sistemas de Información Integrados (ERP). In *Asociación Española de Contabilidad y Administración de Empresas (AECA)*.

Tejena-Macías, M. A. (2018). Análisis de Riesgos en Seguridad de la Información. *Polo de Conocimiento*. https://doi.org/10.23857/pc.v3i4.809

Tello, E. A., Alberto, J. M., & Velasco, P. (2016). Inteligencia de negocios: estrategia para el desarrollo de competitividad en empresas de base tecnológica Business intelligence:Strategy for competitiveness development in technology-based firms. *Contaduría y Administración*. https://doi.org/10.1016/j.cya.2015.09.006

Valencia, D. C. (2015). Plan Nacional de Tecnologías de la Información y las Comunicaciones. *Revista de Derecho Comunicaciones y Nuevas Tecnologias*.

Vargas García, D. (2015). Las TIC en la educación. *Plumilla Educativa*. https://doi.org/10.30554/plumillaedu.16.1598.2015

Vargas, J. (2018). Balanced scoredcard – importancia en los sistemas de calidad. https://doi.org/10.1201/9781315178141-14

Vegas-Fernández, F. (2015). Gestión de riesgos. *XII Jornadas Valencianas de Dirección de Proyectos*.

Von, B. (1976). *Teoría General de los Sistemas.* México: Fondo de la Cultura Económica.

Wireless, C., Gmbh, M., Ii, A., Enisa, Wollman, D. a., Strippers, M., … Sandra, C. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference On*. https://doi.org/10.1109/IEEESTD.2008.4453853

Yu, C. P., Chen, H. G., Klein, G., & Jiang, R. (2015). The roots of executive information system development risks. *Information and Software Technology*. https://doi.org/10.1016/j.infsof.2015.08.001

14. Bibliografía

Abrego Almazán, D., Sánchez Tovar, Y., & Medina Quintero, J. M. (2017). Influencia de los sistemas de información en los resultados organizacionales. *Contaduria y Administracion*. https://doi.org/10.1016/j.cya.2017.03.001

Aguirre, J. (2015). Inteligencia estratégica: un sistema para gestionar la innovación. *Estudios Gerenciales*. https://doi.org/10.1016/j.estger.2014.07.001

Asobancaria. (2018). La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. *Semana Económica*.

Ajzen, I. (2014). *la teoría del Comportamiento Planificado.* New Jersey: Health Psychology Rewiew.

Belloch, C. (2012). Las Tecnologías de la Información y Comunicación en el Aprendizaje.

Bernal, C. (2010). Metodología de la investigación. In *México: Editorial Mc ....*

Bertoglio, O. J. (1994). *Introducción a la Teoría General de Sistemas.* Noriega Editores.

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*. https://doi.org/10.1016/S1353-4858(16)30086-1

Chicano Tejada, E. (2014). Gestión de Incidentes de Seguridad Informática. In *proyecto AMPARO*.

Colombia. (1991). Constitucion Politica De Colombia. *Journal of Chemical Information and Modeling*. https://doi.org/10.1017/CBO9781107415324.004

Comunicaciones, M. de T. de la I. y las. (2017). Impacto de los Incidentes de Seguridad Digital en Colombia 2017. *Informacion Tecnologica*.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. *Serie de Tratados*

Europeos. https://doi.org/BOE-A-2012-5403

Congreso de la República de Colombia. (2012). *Ley 1581 de protección de datos personales.* Bogotá: Congreso.

Congreso de la Reública de Colombia. (2009). *Ley 1273 de 2009"de la protección de la información y de los datos".* Bogota: Diario Oficial.

Cortés Borrero, r. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en colombia. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*. https://doi.org/10.15425/redecom.14.2015.06

DANE. (2009). *Metodología Linea Base de Indicadores.* Bogotá: Dirección de Regulación, planeación, estandarización y normalización - DIRPEN.

Departamento Nacional de Planeación. (2006). *Documento CONPES 3437.* Bogotá: Diario Oficial.

Departamento Nacional de Planeacion. (2011). Documento CONPES 3701. *Lineamientos de politica para Ciberseguridad y Ciberdefensa*, 1-43.

Departamento Nacional de Planeacion. (2016). Documento CONPES 3854. *Politica Nacional de Seguridad Digital*, 1-91.

Dirección General . (2019). *Resolución 05884 "Manual para la administración de los recursos logísticos".* Bogotá: Policía Nacional.

Dirección General - Policía Nacional. (2006). *Directica transitoria nro 077 - Pagina web.* Bogotá: Policía Nacional.

Dirección General. (2019). *Resolución 01233 "Por la cual se adopta la matriz de indicadores asociados a los procesos de la Policía Nacional".* Bogotá: Policía Nacional.

Direccion General de la Policia Nacional . (2016). *Resolucion 05309 del 24 de agosto 2016, "por la cual se establecen las tablas deorganizacion policial TOP".* Bogota: Oficina de Planeacion.

Direccion General de la Policía Nacional. (2002). *Directiva Nro. 004 Implementacion a Nivel Nacional del Nuevo Sistema de Administracion de Talento Humano SIATH.* Bogota.

Dirección General de la PolicÍa Nacional. (2019). *Resolución 03374 del 20019 "Por la cual se adopta la declaración de prácticas de certificación digital".* Bogotá : Policía Nacional.

Dirección General Policía Nacional. (2017). *Resolución 03253 del 2017 "Por la cual se adopta el formato único de orden de comparendo y/o medida correctiva".* Bogotá: Policía Nacional.

Dirección General. (2019). *Resolución 00760 Estructura Orgánica Interna de la DIJIN.* Bogotá: Policía Nacional.

Dirección General Policía Nacional. (2019). *Resolución 00941 del 2019 "por la cual se reglamenta el sistema adenunciar".* Bogotá: Policía Nacional.

Direccion General Policía Nacional de Colombia. (2013). *Aplicabilidad Portal de Servicios Internos (PSI).* Bogota.

Direccion Policia Nacional de Colombia. (2016). Resolución No. 00937 del 10 de Marzo DE 2016 . *Manual de funciones para el personal uniformado de la Policia Nacional*, 12.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*. https://doi.org/10.4236/jis.2013.42011

EcuRed contributors. (08 de 08 de 2019). *Enfoque sistémico*. Obtenido de https://www.ecured.cu/index.php?title=Enfoque_sist%C3%A9mico&oldid=34932

El concepto de responsabilidad social de la empresa. (2018). *Economía*.

Enciso, B. (2018). Teoría General De Sistemas: In *La biblioteca, bibliosistemática e información*. https://doi.org/10.2307/j.ctv51307z.7

Fabiano Couto Corrêa. (2016). Gestión de datos de investigación. In *EPI scholar*.

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. In *Symantec Security Response*. https://doi.org/20 September 2015

Garcia, O. A., Gonzalez, H. A., Luis, R. M., & Elmer, R. C. (2015). Sistemas De Informacion Gerencial. *Universidad Don Bosco*. https://doi.org/10.1017/CBO9781107415324.004

Gomez Bastar, S. (2012). Metodologia de la investigacion. In *Red Tercer Milenio S.C.* https://doi.org/- ISBN 978-92-75-32913-9

González Longatt, F. M. (2007). Introducción a los Sistemas de Información: Fundamentos. *Sistemas de Información*.

Gutierrez, J. M. (2008). Sistemas Expertos Basados en Reglas.

Hernangómez de Mateo, J. L. (2014). Dilemas cibernéticos y la estrategia de seguridad nacional. In *ieee.es - Instituto Español de Estudios Estratégicos*.

Hernández Sampieri, R., Fernandez Collado, C., & Lucio, B. (2014). *Metodología de la Investigación.* Mexico: McGraw-Hill.

Inc, IDG Communications. (23 de 02 de 2018). *Computerworld Colombia*. Obtenido de https://computerworld.co/el-cibercrimen-cuesta-600-000-millones-de-dolares-la-

economia-mundial/?unapproved=1194&moderation-hash=1bb8a4fb27e63a967a3d330406eadd72#comment-1194

K Newmeyer, E Cubeiro, M. S. (2015). Ciberespacio, Ciberguridad y Ciberseguridad. *II Simposio Internacional de Seguridad y Defensa: Perú 2015.*

Karen, D. (2015). La toma de decisiones de la empresa. *Sistema de Información Para La Toma de Decisiones*.

Kenneth e. Kendall, & julie e. Kendall. (2011). Analisis y Diseño de Sistemas. In *Pearson*.

Kyocera. (2018). *Kyocera Document Solutions*. Obtenido de http://smarterworkspaces.kyocera.es/blog/los-6-principales-tipos-sistemas-informacion/

Leopold, H. (2013). Business Process Management. In *Lecture Notes in Business Information Processing*. https://doi.org/10.1007/978-3-319-04175-9_1

Liu, X., Lftikhar, N., & Xie, X. (2014). Survey of real-time processing systems for big data. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/2628194.2628251

Mankiw, G. N. (2012). Principios de economía. In *Sección de Obras de Economía*.

Martínez Gómez, J., Higuera Marín, M., & Aguilar Díaz, E. (2013). Enfoque metodológico para el diseño de interfaces durante el ciclo de vida del desarrollo de software. *Gerencia Tecnológica Informática*.

Neira, A. L., & Spohr, J. R. (2010). Sistema de Gestión de la Seguridad de la Información. *Www.Iso27000.Es*.

Niño Camazón, J. (2011). Introdicción a los sistemas informáticos. In *Sistemas operativos monopuesto*. https://doi.org/8497719719

Niemimaa, E. &. (2017). Information systems security policy implementation in practice: from best practices to situated practices . *European Journal of Information Systems*

Oficina de Planeación - Policía Nacional. (2019). *Guía de herramientas de seguimiento y evaluación.* Bogotá: Policía Nacional.

Oficina de Planeacion Policía Nacional. (2016). *Resolución 00937, Manual de Funciones.* Bogotá: Policía Nacional de Colombia.

Oficina de Planeación Policía Nacional de Colombia. (2016). *Resolución 05309, por la cual se establecen las TOP.* Bogotá : Policía Nacional.

Organizacion de los Estados Americanos "OEA". (2004). Estrategia de Ciberseguridad Cibernetica. *CICTE*, 2-14.

Organización de los Estados Americanos OEA. (16 de 07 de 2015). Buenas prácticas para establecer un CSIRT Nacional. *Seguridad Cibernética*. Obtenido de https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Organización de los Estados Americanos OEA. (2015). Metodología de Respuesta a Incidentes (IRMs) IRM10-IngenieriaSocial-OEA. *Seguridad Ciberética.*

Pérez-Montoro, M. (2010). Arquitectura de la información en entornos web. *El Profesional de La Informacion*. https://doi.org/10.3145/epi.2010.jul.01

Policía Nacional De Colombia. (2013). *Resolución número 02536 de 08 de julio.* Bogota: Policía Nacional de Colombia.

Policía Nacional de Colombia. (2016). *Resolución número 08310 de 28 dic.* Bogota : Policía Nacional .

Policía Nacional de Colombia. (05 de 11 de 2018). *Oficina de Telemática de la Policía Nacional*. Obtenido de https://www.policia.gov.co/oficinas-asesoras/telematica

Policía Nacional de Colombia. (25 de 06 de 2018). *POLIRED*. Obtenido de http://polired/Institucion/NivelAsesor/Oftelematica/default.aspx

Ramos, M. A. (1993). Los Directivos y los Sistemas de Informacion. *Dirección y Progreso*.

Ramos, L. (2009). Seguridad de la Informacion. *Gerencia General de Tecnologias de La Información-Agencia de Recaudación de La Provincia de Buenos Aires (Arba)*.

República, c. d. (2006). *Ley 1015 DE 2006.* Bogota: La Gaceta del Congreso.

República, c. d. (2012). *Ley Estatutaria 1581 DE 2012.* Bogota: La Gaceta del Congreso.

Revista Dinero. (26 de 09 de 2017). Los sectores económicos más impactados por el cibercrimen en Colombia. *Dinero*, 5. Obtenido de https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

Revista, Gestión. (01 de 02 de 2016). Empresas invierten cada vez más en sistemas de seguridad informática. *Gestión*, 1-5. Obtenido de https://gestion.pe/tecnologia/empresas-invierten-vez-sistemas-seguridad-informatica-144913-noticia/

Rodríguez, D., & Valldeoriola, J. (2010). Metodología de la investigación. *Universitat Oberta de Catalunya*, 613. Retrieved from http://www.casadellibro.com/libro-metodologia-de-la-investigacion-5-ed-incluye-cd-rom/9786071502919/1960006

Román, J. L. (2016). La Transformación Digital de la Industria. *Conferencia de Directores y Decanos de Ingeniria Informatica*. https://doi.org/10.1080/14015430802688385

Ruus, V. R., & Reiska, P. (2015). Estonia. In *The Education Systems of Europe, Second*

Edition. https://doi.org/10.1007/978-3-319-07473-3_14

Sampieri, R. H., Collado, C. F., María, D., Lucio, B., Valencia, S. M., Paulina, C., & Torres, M. (2014). Dr. Roberto Hernández Sampieri. *Mc Graw Hill*.

Sánchez Medero, G. (2012). La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom*.

Secretaría General - Policía Nacional. (2011). *Directiva administrativa permanente "Implementación del Sistema IPD"*. Bogotá: Policía Nacional.

Secretaria General Policía Nacional. (2016). *Resolución 5633 de 2016 "Infraestructura tecnológica para el proceso de autenticacción biometrica"*. Bogotá: Policía Nacional.

Secretaria General Policía Nacional. (2017). *Resolución número 06581 "Por la cual se actualizan los lineamientos generales de implementación y fortalecimiento del aplicativo GECOP"*. Bogota: Policía Nacional.Abrego Almazán, D., Sánchez Tovar, Y., & Medina Quintero, J. M. (2017). Influencia de los sistemas de información en los resultados organizacionales. *Contaduria y Administracion*. https://doi.org/10.1016/j.cya.2017.03.001

Sierra, G., Escobar, B., Gago, S., Navarro, T., & Rocha, C. (2007). Sistemas de Información Integrados (ERP). In *Asociación Española de Contabilidad y Administración de Empresas (AECA)*.

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*. https://doi.org/10.23857/pc.v3i4.809

Tello, E. A., Alberto, J. M., & Velasco, P. (2016). Inteligencia de negocios: estrategia para el desarrollo de competitividad en empresas de base tecnológica Business intelligence: Strategy for competitiveness development in technology-based firms. *Contaduría y*

Administración. https://doi.org/10.1016/j.cya.2015.09.006

Valencia, D. C. (2015). Plan Nacional de Tecnologías de la Información y las Comunicaciones. *Revista de Derecho Comunicaciones y Nuevas Tecnologias*.

Vargas García, D. (2015). Las TIC en la educación. *Plumilla Educativa*. https://doi.org/10.30554/plumillaedu.16.1598.2015

Vargas, J. (2018). Balanced scoredcard – importancia en los sistemas de calidad. https://doi.org/10.1201/9781315178141-14

Vegas-Fernández, F. (2015). Gestión de riesgos. *XII Jornadas Valencianas de Dirección de Proyectos*.

Von, B. (1976). *Teoría General de los Sistemas.* México: Fondo de la Cultura Económica.

Wireless, C., Gmbh, M., Ii, A., Enisa, Wollman, D. a., Strippers, M., … Sandra, C. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference On*. https://doi.org/10.1109/IEEESTD.2008.4453853

Yu, C. P., Chen, H. G., Klein, G., & Jiang, R. (2015). The roots of executive information system development risks. *Information and Software Technology*. https://doi.org/10.1016/j.infsof.2015.08.001

15. Anexos

1. Solicitud mesa de trabajo para validar el proyecto.
2. Viabilidad para la elaboración del proyecto.
3. Solicitud mesa de trabajo a la Oficina de Planeación.
4. Tabla de Retención Documental para el Grupo de Ciberseguridad.
5. Estudio de Planeación.
6. Cargo, perfil y funciones del jefe de ciberseguridad.
7. Cargo, perfil y funciones del analista de ciberseguridad.
8. Solicitud recepción y revisión de documentos para la creación del Grupo de Ciberseguridad.
9. Concepto Dirección de Talento Humano de la Policía Nacional de Colombia.
10. Concepto Oficina de Planeación de la Policía Nacional de Colombia.
11. Concepto de Secretaría General de la Policía Nacional de Colombia.
12. Ficha técnica indicador uno.
13. Ficha técnica indicador dos.
14. Ficha técnica indicador tres.
15. Procedimiento 1DT-PR-0007 Gestion de la Informacion en las Bases de Datos.
16. Procedimiento 1DT-PR-0008 Calidad del dato.
17. Propuesta de la nueva estructura orgánica de la Oficina de Telemática.