Escuela Superior de Guerra

"General Rafael Reyes Prieto"
Maestría en Ciberseguridad y Ciberdefensa

LA PROTECCIÓN DE DATOS PERSONALES DE LOS MIEMBROS DE LAS FUERZAS MILITARES DE COLOMBIA EN EL CUMPLIMIENTO DE LABORES MISIONALES

MY. JHON JAIRO BERNAL HERNÁNDEZ
Alumno Maestría Ciberseguridad y Ciberdefensa

Doc. JAIDER OSPINA NAVAS
Director de trabajo de grado

Localidad, Colombia; 14 de marzo de 2022

Tabla de contenido

Lista de Figura

Listado de Tablas

Resumen

En Colombia las Fuerzas Militares (FFMM) es la institución más grande y con más miembros activos, esto se puede considerar una fortaleza refiriendo a todo lo que abarca el termino seguridad y defensa nacional, pero en un contexto más limitado se puede señalar una problemática específica, para el tema del estudio de la presente investigación se abarca la protección de datos y ciberseguridad en todos sus aspectos para las FFMM, teniendo en cuenta que, para el cumplimiento de sus objetivos misionales debe garantizar la seguridad del territorio nacional, dicha seguridad refiere todos los temas que conciernen al país, en este sentido, es importante entender que para abordar este tema, se debe iniciar por la seguridad de sus miembros.

Teniendo en cuenta lo anterior, en la presente investigación es necesario revisar el DAMA (Data Management Framework), la norma técnica ISO 27001 y los estándares técnicos relacionados a la clasificación y custodia de la información, también se hace la revisión y recomendaciones relacionadas con seguridad física y lógica para acceder a la información, la revisión del ciclo de vida de los datos, considerando el tipo de dato, el proceso para el cual se ha consignado y la trazabilidad necesaria para asegurar el control de los datos.

Palabras clave: Seguridad, Datos personales, Miembros de las FFMM, labores misionales

Abstrac

In Colombia, the Armed Forces is the largest institution with the most active members, this can be considered a strength referring to everything covered by the term security and national defense, but in a more limited context a specific problem can be pointed out, for the topic The study of the present investigation covers the specific case of the National Army, taking into account that, in order to fulfill its missionary objectives, it must guarantee the security of the national territory, said security refers to all the issues that concern the country, security that must start from the safety of its members.

Taking into account the above, in the present investigation it is necessary to review the DAMA (Data Management Framework), the ISO 27001 technical standard and the technical standards related to the classification and custody of information, we will also review recommendations related to physical and logical security for access to information, review of the life cycle of the data, considering the type of data, the process for which it has been consigned and the necessary traceability to ensure control of the data.

Key Words: Security, Personal data, Members of the Armed Forces, missionary work

Introducción

Es importante tener en cuenta que, es misión constitucional de las FFMM es garantizar la seguridad nacional por lo que, la protección de datos personales se ha convertido en una gestión de datos críticos al interior de las instituciones, cada una de las actividades confidenciales y no confidenciales contiene información asociada a datos personales, convirtiendo los protocolos de gestión de información en elementos relevantes para asegurar la integridad, confidencialidad y seguridad de la información, estos protocolos tienen gran importancia pues están diseñados con miras de garantizar la seguridad tanto personas, como de las tecnología y procesos que son diseñados y definidos en función de la criticidad de la información, la misionalidad de los roles de las personas que intervienen, el ciclo de vida de los datos y la evaluación de riesgos sobre el control de la información.

Actualmente han surgido protocolos y mecanismos de gestión de la información, que han variado de acuerdo al entorno de la institución dando lugar a modificaciones o especializaciones por tipo de institución o por tipo de industria, ahora bien, en el presente trabajo se pretende explicar cuáles son los principales elementos a tener en cuenta en la seguridad de los datos personales para los miembros de las FFMM, partiendo de best practice de referencia, marco regulatorio local, frameworks existentes, y las condiciones actuales dispuestas para la gestión de la información de datos personales.

Considerando lo anterior, se hará necesario revisar el DAMA (Data Management Framework), la norma técnica ISO 27001 y los estándares técnicos relacionados a la clasificación y custodia de la información, también se revisan recomendaciones relacionadas con ciber seguridad y protección de los datos para acceder a la información, la revisión del ciclo de vida de los datos, considerando el tipo de dato, el proceso para el cual se ha consignado y la trazabilidad necesaria para asegurar el control de los datos.

Con el aumento del uso del internet de manera incremental desde los años 90, y con las posibilidades de mantener la conectividad y el incremento de los dispositivos móviles ha evolucionado la democratización de los datos, se ha generado riesgos inherentes a la gestión de la información que involucran fuga, perdida de información confidencial, violación de la privacidad y hasta suplantación de la identidad o revelación de información sensible a nivel institucional, por esto se hace necesario, se cuente con mecanismos y protocolos que involucren políticas, procedimientos, roles, funciones y hasta permisos sobre la información, en específico sobre los dominios de información que se relacionan a la información y datos personales, con esto se espera que puedan identificarse vulnerabilidades tecnológicas, culturales y procedimentales que evidencien las necesidades de controles específicos durante el ciclo de vida de los datos y así tener visibilidad a nivel institucional de los riesgos asociados a la gestión de la información personal de los miembros de la fuerza.

Teniendo como base lo anterior, este documento propone desarrollar una metodología y recomendaciones pertinentes para realizar la gestión de los datos personales, basados en las mejores prácticas, marcos de trabajo y metodologías relacionadas a la gestión de la información y desde la cual se extenderá la propuesta para ser implementada en la institución. Es importante tener en cuenta que las recomendaciones de implementación, deberán ser validadas previamente con las unidades de tecnología, procedimientos y cultura organizacional, con el fin retroalimentar el plan de implementación, considerando las dependencias y ruta crítica, así como la adopción cultural y la gestión de los nuevos procedimientos que habilitarán el proceso de custodia y protección de los datos personales de la institución.

Bajo este contexto, se plantea como pregunta de investigación ¿Cómo determinar la protección de los datos personales de los miembros de las Fuerzas Militares en el

cumplimiento misional de la labor alineado a las definiciones y protocolos institucionales relacionados con seguridad de la información?

Formulación del problema

¿Cómo determinar la protección de los datos personales de los miembros de las FFMM en el cumplimiento misional de la labor alineado a las definiciones y protocolos institucionales relacionados con Seguridad de la información?

Objetivos de la investigación

Objetivo general

Determinar cómo proteger los datos personales de los miembros de las FFMM en el cumplimiento de la misión.

Objetivos específicos

1. Justificar la importancia de la protección de datos personales, teniendo en cuenta la normativa existente en Colombia.
2. Identificar los elementos relevantes para la formulación de un procedimiento que permita garantizar la gestión segura de los datos de los miembros de las Fuerzas militares.
3. Definir los lineamientos para la construcción de una política de buenas prácticas para el manejo de información.

CAPÍTULO I. Planteamiento de la Investigación

Abordar el tema de la seguridad en Colombia requiere es lo suficiente complejo, pues evidentemente en la evolución del conflicto ha dinamizado el mismo y las técnicas y métodos utilizados en la guerra han variado notablemente, uno de los temas actuales que más, genera preocupación dentro de las instituciones que componen las FFMM es la ciberseguridad y la protección de los datos, pues el uso de nuevas tecnologías ha generado nuevas amenazas.

Teniendo en cuenta lo anterior, es de considerar que el conflicto colombiano ha alcanzado grandes niveles de violencia y se han utilizado mecanismo poco usuales, lo que ha convertido este conflicto interno en una guerra irregular con dinámicas diversas, en el cual las FFMM ha tenido una destacada funcionalidad convirtiéndose en el principal objetivo de los grupos subversivos. De esta manera se evidencia la necesidad de garantizar la seguridad de la información, a fin de que, no tenga puntos de quiebre o vulnerabilidad que puedan ni a la institución en riesgo, ni la infraestructura, ni al personal, por lo que se evidencia la necesidad de estandarizar los protocolos de seguridad cibernética y de protección de datos en las instituciones que componen las FFMM (Diazgranados, 2015).

Pero el tema de la seguridad no solo implica la información de asuntos y personal militar ya que cada unidad cuenta con un personal civil que presta sus servicios profesionales a la institución, los cuales también hacen para del equipo para el caso específico de esta personal, sea cual sea si tipo de contratación (Machuca, 2013).

En este orden de ideas es importante tener en cuenta que, tal como lo plantea (Pérez, 2017), la administración de la información económica y social en Colombia y el uso de tecnologías para esto, va en aumento y complejidad cada día, por esto mismo es preciso adquirir prácticas que mejoren y brinden soporte a los procesos de las entidades, teniendo en cuenta los riesgos inherentes de seguridad. Para el caso de las FFMM, se debe conseguir un

mecanismo que permita mantener la integridad, confidencialidad y disponibilidad en la información de los miembros de la Institución, por lo que resulta fundamental estandarizar los protocolos de seguridad de la información en las tres instituciones que componen las FFMM.

Estado del Arte

El presente estado del arte permite entender la relevancia del tema con base a los planteamientos de otros autores, de tal manera que pueda soportar la hipótesis de esta investigación. Adicional, considerando que en la actualidad las diferentes instituciones tanto a nivel privado como publico han adoptado arquitecturas de información hibridas en donde integran sus sistemas administrados de manera local con aplicaciones o capacidades aprovisionadas en la nube, será importante para este trabajo considerar punto de vista de los principales proveedores de nube, que para este caso serán: Google, Amazon y Microsoft.

Tabla 1 Estado del Arte

Referencia	Síntesis	Aporte
(Mok, 2010)	El trabajo presenta un análisis de la privacidad y protección de datos desde la perspectiva del comercio electrónico. Se presenta los principios y las garantías de protección de datos que deben prevalecer y su aplicación e interpretación en un ambiente de comercio electrónico. Se realiza un análisis comparativo de las normas constitucionales, leyes y proyectos relacionados con la temática de privacidad y protección de datos de seis países latinoamericanos: Chile, Colombia, Costa Rica, Ecuador, México y Perú.	Como aporte se puede decir que, expone el derecho fundamental de la protección de los datos persigue garantizar a la persona un poder de control sobre cualquier tipo de dato personal, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho afectado
(Corrochano, et al , 2021)	Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías	Los responsables y encargados del tratamiento de da - tos deberían adoptar e implementar medidas técnicas y organizacionales

	de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos	que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con estos Principios
Fuente especificada no válida.	El deber de seguridad, señala que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad	El documento de seguridad es el instrumento en el que los responsables describen y dan cuenta de manera general, sobre las medidas de seguridad, técnicas, físicas y administrativas adoptadas para garantizar precisamente esos tres pilares de la seguridad.
(Tamayo, 2020)	La evaluación de los activos de información de la organización en relación a s tres ( )dim ensiones de la seguridad determina la dirección a seguir en la implantación y selección de medidas, también denominadas controles o salvaguardas.	Identificar, clasificar y valorar la información según las dimensiones de seguridad son los pasos previos que van a dirigir la selección de las salvaguardas.
(Arellano, 2021)	En el documento se plasma la nueva dimensión otorgada a los Datos Personales, a partir de diversas reformas constitucionales y disposiciones legales relacionadas con los sistemas locales y nacional en materia de Transparencia y Protección de Datos Personales, que responsabiliza a los sujetos obligados, a transitar de un concepto de Gestión de Datos Personales (GDP) al de un Sistema de Gestión de Protección de Datos Personales (SGPDP), integrado a las políticas de la transparencia, acceso a la información, derecho a la verdad, privacidad, intimidad, autodeterminación informativa, libertad personal, dignidad humana, interés público, límites al estado y memoria colectiva, lo que conlleva obligaciones de carácter humano, materiales, administrativas, tecnológicas y	los responsables carecen de los conocimientos adecuados para aplicar la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Es así, que sería conveniente trabajar un esquema con diversos tópicos que nos permita delinear nuevos paradigmas para la Protección de Datos Personales, materia de otro trabajo, que estén a su vez alineados a los Parámetros instaurados tanto en el Acuerdo mediante el cual se aprueban los Parámetros de Mejores Prácticas en

	de estructura organizacional de alto nivel, entre ellas, el minimizar los riesgos por discrecionalidad, desconocimiento y abuso de poder en el tratamiento y transferencias de Datos Personales durante el proceso de implementación de los Sistema de Gestión de Protección de Datos Personales Institucionales (SGPDPI) especialmente en las épocas de transición, por relevos de personal, trienios o sexenales.	Materia de Protección de Datos Personales del Sector Público, así como lo establecido en el Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.
(Mora, 2021)	Internet y los servicios que a través de ella se prestan se han convertido en un elemento imprescindible para nuestras vidas. Además, la explosión de la conectividad ubicua mediante el uso masivo de dispositivos móviles inteligentes, especialmente los smartphones, y redes de datos móviles cada vez más rápidas, hace que todos estos servicios se puedan consumir en cualquier lugar y a cualquier hora del día o de la noche, por lo que podemos hablar de "personas conectadas" más que de dispositivos y ordenadores conectados.	Se abordan temas como la importancia de tener contraseñas robustas, de hacer copias de seguridad, consejos para comprar en línea, cómo evitar los programas maliciosos, aspectos de privacidad en redes sociales y servicios en la nube, la mediación parental y en general, la protección de nuestros datos personales.
(Meraz, 2018)	El desarrollo tecnológico y el Internet1 han traído consigo la necesidad de proteger diversos aspectos inherentes a las personas, la privacidad y la información de carácter personal son algunos de ellos. Esta necesidad de proteger los datos personales, la información y la privacidad, deriva del derecho que poseen las personas a la protección de sus datos personales, que se traduce en su derecho a la autodeterminación informativa, es el individuo quien decide qué se hace, qué no se hace, quién puede poseerla y para qué fines puede ser utilizada su información personal.	en estricto sentido entre los mecanismos a través de los cuales se puede garantizar el derecho a la protección de datos personales en cualquier organización pública o privada en cualquier parte del mundo son las medidas de seguridad, las cuales se agrupan en administrativas, técnicas y físicas. Si no existen tales mecanismos de protección resulta imposible lograr la protección de información personal y, por ende, hacer efectivo el derecho humano a la protección de datos personales.

(Maldonado, et al, 2019)	Este trabajo tiene como objetivo presentar una experiencia en la que se utilizó Google Drive como herramienta de trabajo colaborativo en la Nube, en la asignatura Manejo de Software I para estudiantes de ingeniería. El uso de dicha herramienta permitió verificar la productividad y la integración de los estudiantes en términos del trabajo colaborativo, al producirse documentos de manera compartida siendo una de las bondades de Google Drive. La experiencia es de carácter descriptivo enfocado en una investigación de campo, además de ser transeccional descriptivo por haberse realizado en un único momento en el tiempo sobre un grupo determinado.	Tomando como referencia este documento se puede afirmar que, en el manejo copioso de todo tipo de información, se asume una gran responsabilidad para salvaguardar todo tipo de documentos. La tecnología, tan necesaria para el funcionamiento efectivo de las corporaciones, tiene también un lado sensible que puede ser contraproducente en la efectividad de la organización y de sus procesos cotidianos

Fuente; recopilación propia

Formulación del problema

¿Cómo determinar la protección de los datos personales de los miembros de las FFMM en el cumplimiento misional de la labor alineado a las definiciones y protocolos institucionales relacionados con Seguridad de la información?

Objetivos de la investigación

Objetivo general

Determinar cómo proteger los datos personales de los miembros de las FFMM en el cumplimiento de la misión.

Objetivos específicos

1. Justificar la importancia de la protección de datos personales, teniendo en cuenta la normativa existente en Colombia.

2. Identificar los elementos relevantes para la formulación de un procedimiento que permita garantizar la gestión segura de los datos de los miembros de las Fuerzas militares.
3. Definir los lineamientos para la construcción de una política de buenas prácticas para el manejo de información.

Metodología

La investigación se realizará utilizando el método cualitativo, entendido como un enfoque basado en comprender los fenómenos y problemáticas desde la perspectiva del autor con referencia al tema específico de la ciberseguridad. Tomando como referencia a (Hernández, et al , 2014), quien afirma que, "El enfoque cualitativo se selecciona cuando el propósito es examinar la forma en que los individuos perciben y experimentan los fenómenos que los rodean, profundizando en sus puntos de vista, interpretaciones y significados" (p.358) Este enfoque implica emplear un proceso caracterizado en proceso ser inductivo, recurrente, analiza múltiples realidades subjetivas y no mantener una secuencia lineal.

En este sentido es importante, tener en cuenta que, el objetivo de esta investigación, consiste en determinar cómo proteger los datos personales de los miembros de las FFMM en el cumplimiento de la misión. Como resultado de estudios analíticos, para lo cual se fundamenta en la revisión documental de documentos que soportan el tema.

Por lo tanto, en esta investigación esta direccionada a todos los miembros de las FFMM, tanto lo activos (Oficiales y Suboficiales) y personal civil vinculado laboralmente, que esta amparados por los beneficios, regímenes y políticas establecidos por la institución.

Teniendo en cuenta que, en esta era digital se han presentado tanto grandes beneficios para el progreso de los países, como grandes problemas.

CAPÍTULO II. Marco de Referencia

El presente marco de referencia se construye teniendo en cuenta que, la seguridad de la información y la protección de los datos personales resultan ser responsabilidad institucional de las FFMM que opera en todo el territorio nacional, lo que exhibe la necesidad para realizar cualquier trámite legal o administrativo u operacional de sus miembros. Una particularidad precisa de este documento de identificación integrado del personal activo de cada una de las fuerzas, el cual debe contener la información necesaria para reconocer plenamente a su portador.

Marco teórico

En este punto es importante destacar que, el tema de ciberseguridad posee fuertes carencias en el desarrollo de una política nacional en la construcción de capacidades para enfrentar los riesgos y amenazas provenientes del ciberespacio en dimensiones que afectan la seguridad nacional. Por lo que, el presente marco teórico se genera un vínculo La ciberseguridad es un tema central de la seguridad nacional.

El poder que genera el ciberespacio

Tal como lo plantea (Vargas et, al, 2017), tanto el uso como la aplicación del ciber poder están direccionados a aspectos específicos como lo son, los aspectos tácticos, técnicos y operacionales en el internet. Por lo que ha tomado gran relevancia en la creación de un objetivo estratégico, perseguir los Estado-Nación, tanto en épocas de armonía como de conflicto, y tiene la función de manipular el contexto de un dominio estratégico, en este caso el ciberespacio, con el fin de obtener algún tipo de superioridad frente a adversarios y degradar o limitar el desarrollo de capacidades semejantes por los mismos.

En ese sentido, (Sheldon, 2012), el ciberpoder es “la suma de todos los efectos estratégicos generados por ciberoperaciones en el mundo virtual” en este sentido, se puede afirmar que el ciberpoder es un conjunto nuevo de conceptos y doctrinas que son una palanca clave en el desarrollo y ejecución de política, ya sea contra el terrorismo, crecimiento económico o asuntos diplomáticos, etc.”. que se dinamiza a medida que evoluciona, optimizando cada una de las palancas del poder nacional, en especial el militar y el informático.

Por lo que, se puede considerar que durante la evolución de las FFMM en el conflicto interno colombiano se han evidenciado diferentes casos susceptibles a revisión1, análisis y control en lo relacionado a la gestión de información personal de los miembros de la institución, generando eventos de riesgo reputacional, operativo, logístico y legal, considerando el impacto de estos riesgos y la evolución en cuanto a seguridad de la información, capacidades de ciberseguridad y capacidades tecnológicas, se puede plantear una propuesta que permita definir las recomendaciones asociadas a integrar procesos, metodologías y tecnologías que permitan la mitigación del riesgo durante la operación diaria

La ciberseguridad y las teorías clásicas de la guerra

Para abordar el tema de la teoría de la guerra y la comprensión constructivista, se requiere destacar las capacidades y factores individuales o contextuales, los cuales están vinculados de manera directa a las características geográficas y físicas de cada teatro de guerra, por lo que presentan el hecho de que los cuatro campos de confrontación de la teoría clásica de la guerra ostentan características intersubjetivas ligadas al espacio físico, así como capacidad de influencia y poder para cada Estado-Nación (Aguilar, 2021).

1

Con base el planteamiento anterior, se puede establecer que, el desarrollo de las armas se determinó por el medio geográfico en que estas eran utilizadas, y debían estructurarse para causar daño e impacto al enemigo, pero con la evolución de los métodos de guerra e incluso de las mismas armas, el tema de ciber seguridad a tomado gran relevancia, puesto que, evidentemente la confrontación bélica, diseño estrategias, técnicas y armamento que no resulta de gran ayuda en la guerra cibernética, pues difícilmente se consigue identificar al atacante, por lo que para concluir cabe mencionar que la guerra cibernética modifica todos los estándares de guerra hasta ahora planteados.

La Ciberdefensa en un contexto global

La ciberdefensa en un contexto global representa un reto para gran cantidad de países, esto ha conseguido que, aumente el gasto en defensa y la necesidad de fortalecer las capacidades para enfrentar riesgos y amenazas provenientes del ciberespacio. Por lo tanto, diversos portales han expresado su preocupación en el tema puesto que desde 2004 el mercado global de ciberseguridad pasó de los 3,500 a los 120,000 millones de dólares en solo tres años, esto indica un crecimiento de 35 veces a su tamaño, pero eventualmente para el año en curos se prevé que el gasto mundial en productos y servicios de ciberseguridad para la defensa contra el ciberdelito supere los mil millones de dólares de forma acumulativa (Aguilar, 2021).

Por otro lado, (Vargas et, al, 2017) afirma que, con referencia al tema regional, el informe Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuestas de los Gobiernos presentó que desde el 2012 los ciberataques a entidades o sitios de Internet públicos y privados han crecido a cifras anuales de más del 61% (OEA/Symantec 2014). A

la par que países como Ecuador, Guatemala, Bolivia, Perú y Brasil, estuvieron dentro de las diez principales países que con más afectaciones por malware. Del mismo modo, Uruguay, Colombia y Chile presentaron cifras de infección por malware por encima de la media global, situación que enmarcó a la región, junto a Asia, con las tasas más altas de virus maliciosos a nivel global

Así las cosas, es importante tener en cuenta que, dada la importancia del tema y a fin de enmarcarnos en la teoría del tema de estudio es importante analizar el concepto presentado por Carlota Bustelo y Raquel Amarilla (2001) mediante el cual se refiriere que Gestión del Conocimiento es la base y fundamento de cualquier tipo de estudio y hace énfasis en que "es todo el conjunto de actividades realizadas con el fin de utilizar, compartir y desarrollar los conocimientos de una organización y de los individuos que en ella trabajan, encaminándolos a la mejor consecución de sus objetivos." (Tamayo, 2020)

En este sentido es importante tener en cuenta el marco jurídico que soporta la legalidad y resalta la importancia de este tema. La protección de datos se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber qué datos están siendo retenidos y usados y de corregir las inexactitudes. Si la gestión involucra a personas, se deben considerar las obligaciones legales y éticas con respecto a compartir los datos (Ramiro, 2015).

Son considerados *Datos personales* datos como teléfono, edad, dirección personal o laboral, colegios o establecimientos educacionales a los que asistió una persona, entre otros” (Herrán, 2017) De igual forma, el Estado colombiano cuenta con la ley estatutaria No.1581 del 2012, (Congreso de Colombia, 2021) y (Ley 1712, 2014); por la cual se dictan disposiciones generales para la protección de datos.

Como un mecanismo de la protección de datos personales es la siguiente normatividad.

- Seguridad de la Información

  Según (ISO 27001, 2005), la 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.

- Política De Tratamiento De Datos Personales para la Fuerza Aérea Colombia

"Esta Política de Protección de Datos Personales se aplicará a todas las Bases de Datos y/o Archivos que contengan Datos Personales que sean objeto de Tratamiento por parte de la Fuerza Aérea Colombiana y que sean recolectados a través de la página web www.fac.mil.co y/o aplicación móvil. La presente política obedece al mandato legal, en cuanto el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías frente a la metería, que desarrolle la Ley y la Constitución Política de Colombia" (Fuerza Aérea Colombiana, 2016) (Comando General de las Fuerzas Militares de Colombia, 2018) por la cual se actualiza la Política de Tratamiento de Datos Personales del COGFM.

Lineamientos para la definición de la política de tratamiento de datos personales en el Ministerio de Defensa Nacional

Tomado de la Directiva Permanente No 3 de 2019 donde se definen "los lineamientos para que las entidades ejecutoras, tales como las FFMM como responsables del tratamiento de los datos personales adopten la política para la recolección, manejo, tratamiento y

proteccion de los datos personales y privacidad de todas las personas que estan o hayan estado vinculadas a la entidad", y específicamente en el numeral 2.a se refiere que para el "tratamiento de datos personales deberán tenerse en cuenta los lineamientos precisos de la Directiva Permanente DIR2014-18 y sus modificaciones, en particular lo relacionado con:

- Implementación de los controles de seguridad requeridos para todos los sistemas de información e infraestructura tecnológica por parte de las oficinas de tecnología. ting las as Inclusión de los temas relacionados con seguridad de la información y tratamiento de datos personales en los programas de inducción y re inducción.
- Cumplimiento de instrucciones generales sobre Gestión de Terceros, Gestión y Uso de Activos de Información, Acuerdos de Intercambio de Información y Software, Clasificación de la Información, Copias de Respaldo y Gestión de Medios Removibles"

Asi como las recomendaciones para la gestion y tratamiento de los datos sensibles donde especifican que "Los datos que afecten la intimidad del titular o cuyo uso indebido pueda generar su discriminación sólo pueden ser objeto de tratamiento, por parte de las unidades ejecutoras/dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Ministerio de Defensa Nacional, en los siguientes casos:

- Cuando el titular de la información manifieste su conformidad y dé su autorización, por cualquier medio que permita su conservación, para el tratamiento de sus datos sensibles.
- Cuando el tratamiento se requiera para proteger la vida del titular y este se encuentre física o juridicamente incapacitado. En estos eventos, el representante legal en su calidad de responsable del tratamiento deberá otorgar su autorización.

- Cuando el tratamiento sea efectuado en el curso de las actividades legitimas y con las debidas garantías por parte de un ente de control, fundación, ONG, asociación, o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea judicial, política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos reguladores por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin autorización del titular.
- Cuando el tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho de un proceso judicial; .
- Cuando el tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de Identidad de los titulares"

Finalmente sobre la transferencia y transmisión de datos personales e informacion personal refiere en el numeral XV que "las unidades ejecutoras/dependencias del Ministerio de Defensa Nacional Policia Nacional y las entidades adscritas y vinculadas al Ministerio de Defensa Nacional podran transfenr información de datos personales, sin que medie autorizacion expresa del titular, a las autoridades gubernamentales, administrativas, de impuestos, organismos de investigacion y autondades judiciales, cuando a soliciter en ejercicio de sus funciones, y atendiendo a las garantias constitucionales y legales, v al contenido de la presente Directiva Permanente La transferencia y transmision internacional de datos personales, para su almacenamiento permanente y posterior tratamiento, solo se realizara a países que proporcionen niveles adecuados de proteccion de catos, ce accerco a os estandares establecidos y previa declaración de conformidad por parte de la Superintendencia de Industria y Comercio, quen verificara la viabilidad de la operación"

Adicionalmente la FAC en la Directiva permanente Nº 014-2020- MDN-COGFM-COFAC-JEMFA-CAF-JETIC define las Politicas de seguridad y privacidad de la informacion para la FAC, en donde en numeral C registra sus generalidades expresando “La Política de Seguridad y Privacidad de la Información es la posición de la Institución, con respecto a la protección de los activos de información, que soportan los procesos por medio de la generación y publicación de politicas, instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información. A continuación, se establecen las bases que soportan la Seguridad y Privacidad de la У Información de la FAC:

1. La responsabilidad frente a la seguridad de la información será definida, compartida, publicada y aceptada por cada uno de los funcionarios y terceros.

2. La información que sea generada, procesada, transmitida y archivada, así como la infraestructura tecnológica y los activos de información, será protegida de los riesgos que se puedan generar por los accesos otorgados o el uso indebido de la información por parte de los funcionarios y terceros.

3. La protección de las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

4. El control de la operación de los procesos institucionales para no vulnerar la seguridad de la información.

5. El control del acceso a la información, sistemas y recursos de red.

6. La seguridad de la información será parte integral del ciclo de vida de los sistemas informáticos.

7. La gestión adecuada de los eventos de seguridad y las debilidades asociadas con los sistemas de información en pro de la mejora continua.

8. La disponibilidad de los procesos institucionales, a través de la continuidad de la operación en los servicios de las Tecnologías de la Información (TI) y las Tecnologías de la Operación (TO), soportados en el análisis del impacto que pueden generar los eventos de seguridad. y contractuales

9. El cumplimiento de las obligaciones legales, regulatorias establecidas en seguridad de la información.

d**. Objetivos Específicos**

1. Establecer los requisitos para el uso aceptable, activos asociados e instalaciones de procesamiento de la información.

2. Garantizar que la información, las áreas restringidas y los activos de información de la FAC, estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

3. Mitigar el riesgo del uso inadecuado de dispositivos móviles que accedan a información o servicios de TI en la FAC

4. Definir las reglas para el desarrollo y mantenimiento seguro de todos los servicios, arquitectura, software, portales web y sistemas de información que hacen parte de la FAC 5. Prevenir el acceso no autorizado, pérdida, robo o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraibles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral.

6. Proteger la integridad y confidencialidad de la información transmitida dentro de la Institución y con cualquier entidad externa.

7. Gestionar el instructivo para la realización y restauración de las copias de seguridad de los sistemas de información de la institución, para garantizar la continuidad de sus operaciones".

y finalmente en el numeral 4. Comando de Operaciones (COA), se definen sus actividades y responsabilidades, expresándolas de la siguiente forma:

"4.1) Promueve el cumplimiento de las políticas de seguridad y privacidad de la información por parte del personal bajo su responsabilidad.

4.2) Selecciona el custodio de la seguridad de la información (titular y suplente) para cada dependencia de acuerdo con el plan de contrainteligencia aérea.

4.3) Define, documenta, y actualiza permanentemente las actividades relacionadas con sus procesos, incluyendo aquellas que sean consideradas como controles de seguridad de la información dentro de dichos procesos. A través de la Jefatura de Inteligencia (JIN).

4.4) Promueve el cumplimiento de las políticas de seguridad y privacidad de la información por parte del personal bajo su responsabilidad.

4.5) Establece, difunde y controla el cumplimiento de las funciones que desarrollan los custodios de seguridad de la información de la FAC.

4.6) Imparte instrucciones para la elaboración y actualización de los estudios de seguridad de personal (ESP), las actas de promesa de reserva, las pruebas técnicas de confidencialidad y las tarjetas de autorización para manejo de documentación clasificada, de funcionarios y terceros que laboran o tienen algún vinculo laboral con la FAC.

4.7) Programa inspecciones técnicas y de seguridad de la información a las diferentes Unidades y dependencias de la FAC.

4.8) Implementa un programa permanentemente de concienciación y entrenamiento en seguridad de la información para todos los funcionarios de la FAC.

4.9) Establece y difunde el instructivo para definir el nivel de clasificación de la información según los requisitos legales, criticidad y afectación por su divulgación o modificación no autorizados e implementa los instructivos necesarios para su elaboración, trámite, difusión y archivo según el nivel de clasificación adoptado.

4.10) Establece y difunde el instructivo para la elaboración de acuerdos de confidencialidad, que refleje las necesidades de la Institución respecto a la protección de la información que goza de reserva legal para la FAC.

4.11) Realiza seguimiento de las redes transmisión de datos disponibles en la FAC, empleando software y hardware de monitoreo, con el fin de prevenir y detectar la fuga de la información.

4.12) Implementa protocolos internos para el proceso de selección, contratación, incorporación y capacitación del personal de inteligencia y contrainteligencia.

4.13) Establece y difunde el instructivo para la protección de la confidencialidad de la información que goza de reserva legal según se requiera.

4.14) Divulga y mantiene la política e instructivos para la transferencia de información que goza de reserva legal, que permita mantener la confidencialidad de esta al ser enviada al interior de la Institución y/o a cualquier entidad externa.

4.15) Desarrolla actividades de monitoreo del uso de los activos de información para prevenir el impacto de los riesgos derivados de pérdida de integridad, disponibilidad y confidencialidad de la información.

4.16) Realiza escaneo de vulnerabilidades de la infraestructura tecnológica crítica con el fin de prevenir y detectar cualquier amenaza que atente contra los activos de información.

4.17) Establece y mantiene convenios de intercambio de información con entidades Gubernamentales, a nivel nacional e internacional, con el fin de tener insumos necesarios para la protección y confidencialidad de la información"

Marco conceptual

Tabla 2 Conceptos y definiciones

Concepto	Definición	Referencia
Framework	Se define como estructura software compuesta de componentes personalizables e intercambiables para el desarrollo de una aplicación	• (Arimetrics, 2017).
Confidencialidad	Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información	• (Ferrero, et al, 2018).
Gobierno de datos	La gobernanza de datos es un término que se utiliza tanto a nivel macro como micro. El primero es un concepto político y forma parte de las relaciones internacionales y la gobernanza de Internet; este último es un concepto de gestión de datos y forma parte del gobierno corporativo de dato	• (Mejía, 2020)
Integridad de los datos	El término integridad de datos se refiere a la correctitud y completitud de la información en una base de datos. Cuando los contenidos se modifican con sentencias INSERT, DELETE o UPDATE, la integridad de los datos almacenados puede perderse de muchas maneras diferentes	• (Escobar, et al, 2019)
Trazabilidad	La trazabilidad es definida por la Organización Internacional para la Estandarización, en su International Vocabulary of Basic and General Terms in Metrology	• (Urbina, 2011)

Documento	Un documento es un testimonio material de un hecho o acto realizado en el ejercicio de sus funciones por instituciones o personas físicas, jurídicas, públicas o privadas, registrado en una unidad de información en cualquier tipo de soporte (papel, cintas, discos magnéticos, fotografías, etc.) en lengua natural o convencional. "Es el testimonio de una actividad humana fijada en un soporte, dando lugar a una fuente archivística, arqueológica, audiovisual, etc."	• (Escobar, et al, 2019)
Análisis de intrusos	Un sistema de detección de intrusiones (o IDS de sus siglas en inglés Intrusion Detection System) es un programa de detección de accesos no autorizados a un computador o a una red. El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, las anomalías que pueden ser indicio de la presencia de ataques y falsas alarmas	• (Capó, 2015)
Vulnerabilidad	Vulnerabilidad puede ser aplicado en diversos campos con distintas acepciones. Vulnerabilidad es la cualidad de Ser vulnerable. El concepto puede aplicarse a una persona o a un grupo social según su capacidad para prevenir, resistir y sobreponerse de un impacto.	• (Significados, 22015)
Ataques informáticos	En computadora y redes de computadoras un ataque es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar un activo.	• (Mieres, 2019)
Ciberseguridad	La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional	• (Mosquera, 2019)
Ciber protección	La ciber protección es la integración de la protección de datos y la seguridad cibernética, una necesidad para operaciones comerciales seguras respecto del panorama actual de ciber amenazas. En el mundo moderno, las empresas enfrentan una	• (Mosquera, 2019)

	variedad de amenazas contra los datos y las operaciones digitales.	
Identidad Digital	La Identidad Digital es el conjunto de informaciones publicadas en Internet sobre nosotros y que componen la imagen que los demás tienen de nosotros: datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, etc.	• (Escobar, et al, 2019)

CAPÍTULO III

La importancia de la protección de datos personales, teniendo en cuenta la normativa existente en Colombia

Durante muchos años en Colombia se han desarrollados políticas y estrategias que el Gobierno Nacional tiene para la seguridad y defensa en el ciberespacio y la importancia de esto está enfocada a la seguridad de los datos personales, considerando el riesgo que genera las plataformas virtuales. (Departamento Nacional de Planeación, 2020)

Colombia legisla a favor de los datos personales

Entendiendo la necesidad del Estado por garantizar la seguridad de los datos personales como una la Primero el gobierno creo el Conpes 3701 de 2011 el cual tiene como nombre *Lineamientos de política para la ciberseguridad y Ciberdefensa*, esto previendo que el mayor riesgo a los datos personales son debido a la información que se suministran en las diferentes plataformas virtuales, en este Conpes se determinaron estrategias como la creación del Grupo de Respuestas a Emergencias Cibernéticas de Colombia (ColCERT)- el centro Cibernético Policial (CECIP) y el Comando Conjunto -Cibernético (CCOCI) y desarrollaba otras estrategia para el fortalecimiento de la legislación y la cooperación internacional en

materia de ciberseguridad y ciberdefensa, Sin embargo esta política se orientó al desarrollo solo de las capacidades gubernamentales en ciberdefensa y no atendió capacidades para ciudadanos y otros sectores. (Departamento Nacional de Planeación, 2020)

Menciona también el documento que fue un gran avance la creación de la Ley 1581 de 2012 al cual es la Ley de protección de datos personales cuyo objeto es desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar su información personal.

Luego se creó el documento CONPES 3854 de 2011 *Política Nacional de Seguridad Digital* cuyo objeto era fortalecer las capacidades de las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital. (Departamento Nacional de Planeación, 2020)

El gran aporte fue el enfoque de gestión de riesgos, el cual tenía una mirada preventiva y no reactiva si se presentaban eventos en seguridad digital, crearon condiciones para incluir partes interesadas, aceptaron la cooperación de colaboración y asistencia de seguridad digital. Sin embargo, esta política mostro pocos avances en temas relacionados con la Defensa y Seguridad Nacional en el entorno digital.

En el año 2018 se expide el Decreto 1008 el cual estableció los lineamientos generales de la política del gobierno digital. Desde lo relativo a la confianza digital, esta política también busca preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. (Departamento Nacional de Planeación, 2020)

Posterior a esto, el gobierno desarrolla el *Manual de Gobierno Digital* expedido por MINTIC, donde se establecen las pautas para la implementación de la Política de Gobierno Digital y se dictan las medias para las entidades públicas entre ellas la aplicación del Modelo de Seguridad y Privacidad de la Información (MSPI), cuyos lineamientos e indicadores

permiten establecer el nivel de madurez en materia de seguridad digital para las entidades públicas. (Departamento Nacional de Planeación, 2020)

Además, dicho manual se encuentra alineado con las buenas prácticas en seguridad (Norma ISO/IEC 27001:201311), con la Ley 1581 de 2012 que trata de la Protección de Datos Personales y con la Ley 1712 de 2014 (conocida como ley de transparencia y del derecho de acceso a la información pública nacional). (Departamento Nacional de Planeación, 2020) Claro está que dentro de esta política se centró solo en el sector público y no intervienen a todos los sectores que se encuentran dentro de la seguridad de la información.

Así las cosas, el PND en el capítulo VII, Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento, se busca que el país se encamine hacia una sociedad digital y hacia la industria 4.0, a través de la generación de confianza en el entorno digital y del desarrollo de estrategias sobre seguridad digital en los territorios. (Presidencia de la Republica, 2018) y en el capítulo I Pacto por la legalidad: seguridad efectiva y justicia transparente para que todos vivamos con libertad y en democracia, se establece como estrategia para promover el control integral marítimo, terrestre, aéreo, fluvial, espacial y ciberespacial que el Gobierno nacional fortalezca las capacidades de ciberseguridad y ciberdefensa para garantizar los intereses nacionales. (Presidencia de la Republica, 2018)

Así las cosas, en el año 2019, el Ministerio de Defensa Nacional formuló la Política de Defensa y Seguridad para la legalidad, el emprendimiento y la equidad de Colombia, que busca generar condiciones de seguridad y convivencia para preservar y potencializar los intereses nacionales, la independencia, soberanía e integridad del Estado. (Departamento Nacional de Planeación, 2020)

Mas adelante el Ministerio de Tecnologías de la Información y las Comunicaciones presentó el Plan TIC 2018-2022 El Futuro Digital es de Todos, con los proyectos e iniciativas del sector TIC, varios de estos relacionados con seguridad digital. Entre ellos se pueden nombrar la generación de habilidades enfocada en igualdad de género, la creación y potencialización de emprendimientos femeninos, al igual que el fortalecimiento de las capacidades nacionales para impulsar la transformación digital del Estado. (MinTIC, 2018)

Finalmente, en noviembre de 2019 se expidió el Documento CONPES 3795 Política Nacional para la Transformación Digital e Inteligencia Artificial13, cuyo objetivo es aumentar la generación de valor social y económico a través de la transformación digital del sector público y del sector privado, para que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la 4RI (Cuarta Revolución Industrial). (Departamento Nacional de Planeación, 2020)

Debilidades en las capacidades en seguridad digital de los ciudadanos

Dentro de toda la evolución de las nuevas tecnologías están también involucrados en sector público y el sector privado y es lo que se explicara a continuación. Si se observan las Bases del Plan Nacional de Desarrollo 2018-2022: Pacto por Colombia Pacto por la Equidad, la meta del cuatrienio para el porcentaje de hogares con conexión a Internet suscrita es del 70 % de hogares, teniendo como línea base el 50 % de hogares conectados. Para el cumplimiento de estas metas se adelantan iniciativas que se encuentran priorizadas en beneficio de la población pobre y vulnerable, o en zonas apartadas y que tienen una baja interacción con la tecnología y por ende menos capacidades en seguridad digital. (Presidencia de la Republica, 2018)

Por lo anterior y a lo ambicioso del objetivo trae como consecuencias que una vez más personas se encuentren conectadas aumentan las amenazas en la seguridad digital. En contraste, al inspeccionar programas dentro del ámbito TIC, tales como los relacionados con sistemas de información se encuentran 81 programas activos, de los cuales 20 son de nivel académico posgrado entre los que se cuenta 1 maestría y adicionalmente se encuentran 61 programas de nivel académico pregrado, de los cuales 4 son programas universitarios. Esto evidencia que la oferta de programas educativos relacionados con seguridad digital es baja en el nivel de académico pregrado. (Departamento Nacional de Planeación, 2020)

Con lo anterior como contexto, es claro que se debe incrementar la oferta académica en materia de seguridad digital sin descuidar que el acceso a las Tecnologías de la Información y las Comunicaciones (TIC) sea equitativo para todos. Según datos disponibles en 2015 del Observatorio de Tecnologías de la Información (TI)21, la participación de mujeres en empresas de Teleinformática, Software y TI fue del apenas del 39 %, mientras que los hombres representaron un 61 %. En el campo de seguridad digital, el estudio Genero y TIC en América Latina (5G Américas, 2019), resalta cómo las TIC se presentan como una herramienta para mejorar las condiciones de vida de mujeres y niñas y llama la atención sobre la importancia de que se realicen esfuerzos conjuntos entre los sectores públicos y privado para generar diferentes estrategias que busquen potenciar el acceso de las mujeres a las TIC. (Departamento Nacional de Planeación, 2020)

En lo concerniente al sector público, el Global Cibersecurity Index (Unión Internacional de Telecomunicaciones (UIT), 2018), mide el compromiso de los 175 países evaluados en torno a la ciber seguridad y generando un ranking mundial al respecto. Esta evaluación se realiza a través de 5 pilares (legal, técnico, organizacional, construcción de nuevas capacidades y cooperación), que como se describió en el marco teórico, describen

adecuadamente las capacidades que se deben generar en el país para mejorar la confianza y la seguridad digital. (Departamento Nacional de Planeación, 2020)

Según la política Conpes 3995 para el sector privado en Colombia, el Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales, analizó las medidas de seguridad implementadas para recolectar, almacenar, usar, circular o tratar datos personales en 31.41025 empresas (entre privadas, sin ánimo de lucro y mixtas) del país (Superintendencia de Industria y Comercio -SIC, 2019). Este estudio refleja que el 44 % de las empresas que hacen parte del estudio, tienen un nivel de implementación menor o igual al 25 % de las medidas apropiadas y efectivas para garantizar la seguridad de los datos personales y sólo el 15 % tienen un nivel de implementación igual o superior al 76 %, de todos los requerimientos de seguridad emitidos por la SIC. Esto muestra una falta de preparación para garantizar la seguridad de los datos personales y por ende una ausencia de capacidades al respecto. (Departamento Nacional de Planeación, 2020)

En este documento concluye que en Colombia hay muchas deficiencias, en los sectores privado, publico y claro también la densa demografía, no permite que la tecnología llegue a todos los rincones de todo el territorio nacional.

El marco de gobernanza en materia de seguridad no ha alcanzado un grado de desarrollo adecuado:

En Colombia existen dos instancias de alto nivel dentro del marco de la gobernanza La primera es la figura del coordinador nacional de seguridad digital que dispuso el Documento CONPES 3854 aprobado en 2016, La otra instancia es el Comité de Seguridad Digital creado con el Acuerdo no. 002 de 2018 del Consejo para la Gestión y el Desempeño Institucional. (Departamento Nacional de Planeación, 2020)

El primero en cabeza de la consejería de Asuntos Económicos y transformación digital de presidencia, y según el documento la seguridad digital no es uno de ellos, Esto limita su rol como coordinador nacional de seguridad digital y dificulta la coordinación de acciones y el seguimiento efectivo a las tareas relacionadas con la seguridad digital del país. (Departamento Nacional de Planeación, 2020)

Están nombrados dos comités que no cuentan con los enfoques de seguridad nacional, el documento también evidencia que la evaluación colombiana en el NCSI (Índice de ciberseguridad Nacional), la ausencia de un marco de coordinación de políticas de ciberseguridad, que es un subindicador que se pondera dentro del indicador *desarrollo de políticas de ciberseguridad* y en el cual el país no tiene ningún puntaje. (Departamento Nacional de Planeación, 2020)

Así pues, Colombia dentro de su marco de gobernanza y al carecer de un marco de coordinación de políticas de ciberseguridad no puede lograr una adecuada interacción e identificación entre las diversas entidades alrededor del tema. Lo anterior genera la desarticulación y la duplicación de esfuerzos, así como una baja cohesión y coordinación para dar respuesta a incidentes y a contener amenazas que se den en el entorno digital. A esto se le suma que no se cuenta con una instancia lo suficientemente robusta y especializada para coordinar adecuadamente los aspectos de seguridad digital a nivel nacional. Estos factores se constituyen en una debilidad para el avance en materia de seguridad digital y terminan debilitando la confianza digital en el país. (Departamento Nacional de Planeación, 2020)

Diagnóstico

El Informe Global de Riesgos 2019 presenta que el fraude de datos, los ciberataques y las vulnerabilidades tecnológicas, aparecen como grandes preocupaciones junto a eventos

climáticos o desastres naturales, ubicándose dentro de los diez principales riesgos globales con mayor grado de probabilidad de ocurrencia. (Departamento Nacional de Planeación, 2020)

~~Según el centro para la ciberseguridad, el delito cibernético puede alcanzar lo s3 billones de dólares para el año 2020,~~ y el 74% de las empresas del mundo podrían ser hackeadas y esperan que para el 2021 los delitos alcancen los 6 trillones de dólares. (Departamento Nacional de Planeación, 2020)

Sumado a que toda esta generación digital y lo que con ello conlleva lo que son sus amenazas, están expuestos todos, tanto empresas, como las entidades públicas. Si consideramos que el entorno digital es un entorno que nos conecta con el resto del mundo, entonces hay un gran número de ataques a los cuales se encuentran expuestos los ciudadanos en Colombia, no sólo por los ataques que se originen en el país, sino por la sumatoria de ataques que se originan globalmente indudablemente esto lleva a una sensación de desconfianza en el entorno digital. (Departamento Nacional de Planeación, 2020)

Se requiere la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital con énfasis en nuevas tecnologías:

Teniendo en cuenta los planteamientos anteriores es de resaltar que, en Colombia se presenta un avance del 40 %, lo que deja claro que la identificación de amenazas cibernéticas no es suficiente en el entorno tecnológico actual. En consecuencia, si no se hace una rápida adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, en el futuro esta identificación será poco efectiva ante la aparición de nuevas tecnologías. (Departamento Nacional de Planeación, 2020)

Así como anuncia el texto que el mundo se encuentra en camino a cuarta revolución industrial, podemos afirmar lo siguiente, las tecnologías de la información Las tecnologías de la información, potencializadas por la cuarta revolución industrial y su amplia adopción en el mundo, vienen dando lugar a una serie de nuevos y revolucionarios modelos comerciales, así como al surgimiento de nuevos desafíos en términos de seguridad. Por ejemplo, en un ambiente económico y productivo cada vez más dependiente del ciberespacio y la automatización, la seguridad de la información debería considerarse como un componente crítico de la seguridad integral de las organizaciones, ya que su función debe ser establecer la confianza entre organizaciones e individuos y permitir que el intercambio de información a través de Internet sea seguro y proporcione a las personas la tranquilidad necesaria para realizar sus actividades productivas. (Álvarez, 2020)

CAPÍTULO IV Protección de los datos personales de los miembros de las FFMM

~~En un mundo globalizado donde los avances tecnológicos están a la vanguardia del progreso de todos los países del mundo, Colombia~~ y las FFMM cuenta con el Sistema de Información y Administración del Talento Humano SIATH dicho sistema contiene toda información personal de los miembros de las FFMM, esto puede representar un ventaja en los procesos administrados y, pero en la actualidad puede verse como una potencial debilidad, pues de llegar a ser vulnerado dicho sistema se pondría en riesgo la información de los integrantes de las FFMM.

Teniendo en cuenta lo anterior este capítulo se divide en tres apartados el primero de esto hace un análisis del Sistema de Información y Administración del Talento Humano SIATH y, en el segundo apartado se plantean las herramientas dispuestas para la protección

de datos a nivel nacional y, finalmente en el apartado número tres se hace un análisis de los antecedentes de los ataques cibernéticos no solo en Colombia sino en el mundo.

SIAT, sistema que garantiza la seguridad de la información de las FFMM

El SIATH, es un sistema operativo que integra información del personal de las FFMM, esto permite tener un control sobre el talento humano del personal adscrito a las fuerzas, para que de esta manera se puedan determinar procesos que fortalezcan su misión constitucional (Molano, 2021), en este sistema operativo se soporta la propuesta de la unificación de los documentos de identificación del personal civil y militar del Ejército Nacional, ya que este contienen información puntual de dicho personal y se puede mantener actualizado.

Base de datos y sistemas de información

El sistema de información gerencial SIATH está planeado para recolectar, almacenar y divulgar información, que permita ejercer un control sobre el personal activo del Ejército. Este sistema operativo se ocupa de optimizar los procesos referidos al personal de la institución, en especial en tareas de planeación y control, así mismo contienen la información personal de los miembros de la institución. El concepto de SIATH se relaciona con la tecnología informática, que incluye el computador o una red de microcomputadores, además de programas específicos para procesar datos e información.

~~Conceptos de datos e información~~

Los Datos son los elementos que sirven de base para resolver problemas o formar juicios. En sí mismo cada dato tiene poco valor. Sin embargo, cuando son clasificados, almacenados y relacionados entre sí, los datos permiten obtener información. La información tiene significado e intencionalidad, aspectos que la diferencian del dato. Se denomina base de datos el conjunto de datos almacenados para emplearlos posteriormente.

En el área del Talento Humano las diversas bases de datos conectadas entre sí permiten obtener y almacenar datos de distintos estratos o niveles de complejidad.

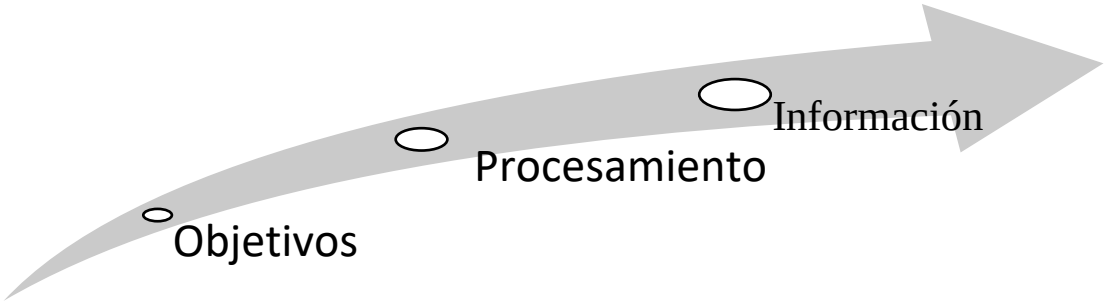
- Datos personales de cada del personal que labora en la institución, que forman un registro de personal.
- Datos sobre los ocupantes de cada cargo, que forman un registro de cargos.
- Datos acerca de los miembros y funcionarios de cada sección, departamento o división, que forman un registro de los mismos.
- Datos sobre los salarios e incentivos salariales, que forman un registro de remuneración.
- Datos acerca de los beneficios y servicios sociales, que forman un registro de beneficios.
- Datos sobre los candidatos (registro de candidatos), sobre cursos y actividades de entrenamiento (registro de entrenamiento), etc.

El sistema de procesamiento de datos requiere de entradas (datos) para suministras salidas (información). El procesamiento de datos en sí incluye clasificación, almacenamiento, recuperación y tratamiento de los datos. Así como la información

consiguiente para ponerla a disposición de quienes la necesitan y requieren en el momento oportuno (diaria, semanal, mensual, trimestral o anualmente), o sea en tiempo real.

El sistema de procesamiento de datos tiene objetivos que varían de una organización a otras.

Figura 1 Sistema de información general



Fuente, (Rodríguez, 2021)

La información puede provenir del ambiente externo (fuera de la organización, por ejemplo, mercado de trabajo, competidores, proveedores, etc.) o del ambiente interno (dentro de la organización, por ejemplo, organigrama de cargos y salarios respectivos en la organización, personas que trabajan en ella, etc.). Los antiguos sistemas tradicionales de información constituyen sistemas cerrados.

El punto de partida de un sistema de información del talento humano del Ejército. Es la base de datos. El objetivo final de un sistema de información de RR.HH. es suministrar a las jefaturas información acerca del personal.

El montaje de un sistema de información de RR.HH. requiere análisis y evaluación de la organización o de sus subsistemas y de sus respectivas necesidades de información.

Proyección del SIATH

Un sistema de información de RR.HH. utiliza como fuentes de datos elementos suministrados por:

- Bases de datos
- Reclutamiento y selección de personal
- Entrenamiento y desarrollo de personal
- Evaluación del desempeño
- Administración de salarios
- Registro y control de personal (ausencias, atrasos, disciplina, etc.)
- Estadísticas de personal
- Higiene y seguridad
- Jefaturas respectivas, etc.

En este punto cabe destacar que un solo software contenga toda la información de los miembros de la institución realmente representa un verdadero riesgo, pero cabe mencionar que dicho software se ha convertido en una herramienta fundamental en la disciplina militar, por lo que cambiarlo representa un verdadero desafío.

En tal sentido es de anotar que, debería distribuirse la información de los militares en diferentes programas y oficina de tal manera que una sola persona no tenga acceso a toda la información de los datos personales.

Herramientas dispuestas para la protección de datos a nivel nacional

El Departamento Administrativo de la Presidencia de la República, a través del coordinador nacional de seguridad digital, planteo ante el Comité de Seguridad Digital la estructuración oficial de la gobernanza de seguridad digital en el país, definiendo los

objetivos, alcance, roles, responsabilidades y competencias tanto de las diferentes instancias encargadas de la seguridad digital en el país. (Departamento Nacional de Planeación, 2020)

Así mismo, a través del coordinador nacional de seguridad digital, presentará ante el Comité de Seguridad Nacional las decisiones prioritarias que puedan requerirse para la implementación de la política de confianza y seguridad digital y para todo lo relacionado en materia de seguridad digital. Lo anterior con el fin fortalecer los mecanismos de toma de decisiones para la articulación estratégica en torno a la seguridad digital en Colombia. (Departamento Nacional de Planeación, 2020)

Por otro lado, Coordinador Nacional de Seguridad Digital, presentará anualmente ante el Comité de Seguridad Digital anualmente los resultados del seguimiento a la agenda nacional de seguridad digital. Esto con el fin de fortalecer, a través de la divulgación dichos resultados, los mecanismos de información y toma de decisiones preventiva, para la articulación estratégica en torno a la seguridad digital en Colombia. (Departamento Nacional de Planeación, 2020)

Medidas tomadas por El Ministerio de Defensa Nacional

El Ministerio de Defensa Nacional plantea un sistema nacional de gestión de incidentes cibernéticos que tendrá como fin:

- articular los esfuerzos institucionales para la gestión oportuna de los incidentes cibernéticos,
- ser la fuente oficial de las estadísticas de los incidentes cibernéticos reportados en el país,

- estandarizar un mecanismo de reporte periódico de incidentes y vulnerabilidades cibernéticas que permita identificarlos, evaluarlos y comunicarlos a los interesados y
- servir de fuente para la toma de decisiones por parte del Gobierno nacional. La información de este sistema la podrán consultar en tiempo real los organismos de seguridad del Estado. (Departamento Nacional de Planeación, 2020)

de tal manera que, establecerá, a través de un documento, un modelo para la divulgación periódica de vulnerabilidades en todos los sectores con un alcance definido entre los puntos de contacto de los propietarios y operadores de activos que soportan actividades críticas y las instancias pertinentes del Gobierno nacional. Este modelo deberá incluir, entre otros:

- el objetivo del intercambio,
- la definición de estándares para el intercambio,
- el (los) punto(s) único(s) de contacto,
- las responsabilidades en el intercambio de información dentro de un marco de confidencialidad y privacidad de la información,
- los actores relevantes y
- los mecanismos de apoyo. Para el desarrollo de este modelo se involucrarán a las múltiples partes interesadas y se contemplarán experiencias internacionales al respecto. (Departamento Nacional de Planeación, 2020).

En este orden de ideas El Ministerio de Tecnologías de la Información y las Comunicaciones establecerá un procedimiento para la promoción y difusión del modelo de divulgación periódica de vulnerabilidades, con el fin de garantizar que las debilidades detectadas por un descubridor sean comunicadas en condiciones adecuadas para las partes y

a su vez atendidas y subsanadas por las entidades, propietarios u operadores de infraestructuras críticas de manera oportuna. Lo anterior, dentro de un marco de divulgación responsable (Departamento Nacional de Planeación, 2020).

Para el Ministerio de Defensa Nacional crear e implementar un sistema de intercambio de información cibernética es prioridad, con miras a facilitar la divulgación de indicadores de compromiso entre los actores que interactúan en el entorno digital a nivel nacional e internacional. Dicho sistema se articulará con el registro central único de incidentes de seguridad digital. (Departamento Nacional de Planeación, 2020)

Entre tanto el Ministerio de Tecnologías de la Información y las Comunicaciones generará un estudio para la actualización del modelo de gobernanza de la seguridad digital en Colombia, para los sectores público y privado. Con el objetivo de apoyar en el fortalecimiento de la organización de seguridad digital en el país. (Departamento Nacional de Planeación, 2020)

Por lo tanto, el Departamento Nacional de Planeación, realizará la medición de impacto de los incidentes de seguridad digital en el sector público colombiano para definir la viabilidad de inversión en las acciones de prevención y mitigación de los riesgos de seguridad digital. Esta medición comprende el levantamiento de información detallada sobre cómo las entidades invierten sus recursos para la gestión de los riegos, cómo los distribuyen para estrategias de prevención y reacción sobre incidentes de seguridad digital, qué tan consientes son de sus vulnerabilidades, o qué tanto gestionan la seguridad de la información a partir de las fuentes primarias. (Departamento Nacional de Planeación, 2020)

Finalmente, el Ministerio de Defensa Nacional en conjunto con el Ministerio de Tecnologías de la Información y las Comunicaciones elaborará un reporte anual para el coordinador nacional de seguridad digital, sobre los logros y avances de ejecución (desde las perspectivas cualitativa y cuantitativa) de los planes de fortalecimiento de las capacidades para cada una de las instancias y entidades responsables de la ciberseguridad y ciberdefensa de la Nación. Dicho reporte debe tener como objetivo fomentar la prevención en seguridad digital, la promoción de toma de decisiones y la mejora continua de la gestión y respuesta a incidentes cibernéticos a nivel nacional. (Departamento Nacional de Planeación, 2020)

Antecedentes

A manera global se puede considerar que, el mundo evidencia un constante riesgo de ser blanco de agresiones cibernéticas, no solo a nivel estatal sino también como ciudadanos, puesto que el número de ciudadanos con acceso a Internet aumenta notablemente. Es por esto, que los países latinoamericanos han dispuesto importantes recursos ´para combatir este flagelo, considerando que tiene la tasa de crecimiento más altas de usuarios de Internet, destacando así que, América Latina simboliza cerca del 10% de usuarios de Internet en el mundo, y la cantidad de usuarios ha aumentado (Lavinder, 2019).

Por lo tanto, el Banco Interamericano de Desarrollo (BID) genera un constante esfuerzo para que, los países de América Latina puedan garantizar la seguridad cibernética en la región sobre todo en la protección de los datos, pero pese a este esfuerzo los delitos cibernéticos han ido en un constante asenso.

Entendiendo la complejidad del tema es importante abordar las estadísticas de las ciber amenazas, teniendo en cuenta que de conocer los potenciales riesgos se pueden diseñar

estrategias mitiguen el impacto de dichos ataques, por lo que de acuerdo a un estudio realizado por (Poma & Vargas, 2019), se puede evidenciar los siguientes datos,

Tabla 3 Ciber amenaza Mundial al 7 de setiembre de 2019 en cuanto a infecciones locales

Puesto	País	Porcentaje
1	República del Congo	19,86%
2	Yemen	18,71%
3	Kirguistán	18,66%
4	Tayikistán	18,44%
5	Uzbekistán	18,16%
6	Camerún	18,12%
7	Guinea Ecuatorial	17,58%
8	Birmania	17,09%

(Poma & Vargas, 2019)

En la tabla No 3, se evidencia que, dentro de los ocho países con más ataques cibernéticos a sus sistemas informáticos, puntea la lista la República del Congo con un total 19,86% con referencia a los demás países, esto podría atribuirse a que este país no cuenta con personal plenamente capacitado, para sumir dichos ataques, ducho en otras palabra el esta país africano no hay expertos que puedan disminuir el riesgo generado por las ciber amenazas.

Tabla 4 Ciber amenaza Mundial al 7 de setiembre de 2019 en cuanto a Amenaza web

Puesto	País	Porcentaje
1	Albania	13,99%
2	Túnez	13,23%
3	Argelia	12,35%
4	Nepal	12,19%
5	Yibuti	11,01%
6	Filipinas	10,58%
7	Birmania	10,01%
8	Libia	9,80%

(Poma & Vargas, 2019)

En la tabla No 2 se puntualiza en los ocho países del mundo con mas ataques y amenazas web, esta desafortunada lista es liderada por Albania seguido por Túnez, por que cabe agregar que, estos países evidencian una gran debilidad en los procesos de los direccionamientos de páginas web, lo que según los expertos los deja e un punto muy vulnerable, pues sus sistemas no están completamente protegidos por softwares que permitan bloquear paginas indebidas y por consiguiente están propensos a los ataques.

Tabla 5 Ciber amenaza Mundial al 7 de setiembre de 2019 en cuanto a Ataque de redes

Puesto	País	Porcentaje
1	Etiopia	18,02%
2	Irán	14,03%
3	Costa Rica	14,12%
4	China	13,29%
5	Pakistán	12,12%
6	Indonesia	11,63%
7	Sudan	11,36%
8	Bangladés	10,93%

(Poma & Vargas, 2019)

En la tabla No 5 se enlistan los países con mas amenazas y ataques a las redes liderando la lista Etiopia y, según el informe de referencia las redes sociales son atacadas con mucha frecuencia debido a personas sin escrúpulos que hacen uso del sistema de mensajería

instantánea con el único objetivo de ser aceptados por sus potenciales víctimas, dando por hecho que si aceptan están invitaciones, pueden ser vulnerables ante cualquier virus o robo de información.

Tabla 6 Ciber amenaza Mundial al 7 de setiembre de 2019 en cuanto a Basura

Puesto	País	Porcentaje
1	China	18,25%
2	Estados Unidos de América	13,26%
3	Brasil	4,94%
4	Rusia	4,88%
5	Turquía	3,04%
6	Alemania	3,03%
7	India	2,60%
8	Singapur	2,08%

(Poma & Vargas, 2019)

En la tabla No 6 se puede ver que de los ocho países más atacado sus sistemas informáticos, es China quien encabeza la lista ocupando el primer lugar por Basura, por basura se entiende los elementos acumulables en los emails, como los spams que diariamente se remiten con la intensión de saturar el correo de la víctima.

Por lo que, se puede atribuir este fenómeno a que al poseer este país el mayor número de cibernautas tienen los requisitos para que los elementos considerados basuras se

acumulen por lo que es necesario que se tomen las medidas pertinentes, para identificar qué tipo de información es la que el usuario a diario usa, o recibe.

Tabla 7 Ciber amenaza Mundial al 7 de setiembre de 2019 en cuanto a Bonet

Puesto	País	Cantidades
1	China	6584
2	Estados Unidos de América	1867
3	South África	230
4	Corea del Sur	107
5	Reino Unido	70
6	Holanda	26
7	Canadá	17
8	Alemania	15

(Poma & Vargas, 2019)

En la tabla No 7, se hace referencia a los ocho países con más ataques a sus sistemas informáticos, China sigue ocupando el primer lugar por Bonet con 6584 unidades, según este análisis, este fenómeno se atribuye al ataque de negación de servicio desde Canadá contra páginas web. Debido a la sobredemanda de personas que hacen uso de este tipo de páginas en este país.

Tabla 8 Ciber amenaza Mundial al 7 de setiembre de 2019 en cuanto a Correo Infectado

Puesto	País	Cantidades
1	Fiyi	4,47%
2	Mónaco	3,53%
3	Grecia	2,96%
4	Moldova	2,89%
5	Emiratos Árabes	2,67%
6	Montenegro	2,41%
7	Catar	2,37%
8	Chipre	2,14%

(Poma & Vargas, 2019)

En la tabla No 8, en la lista de los ocho países más atacados por correos infectados, encabeza la lista Fiyi puesto que, de manera general dichos correos malware lo mismo, que a su vez tienen la capacidad de provocar alteraciones en los sistemas informáticos como el caso de robo de contraseñas.

Para el caso de la tabla No 9, se puntualiza en los ocho países mas atacados en Las en Vulnerabilidad, lista que encabeza las Bahamas, la vulnerabilidad se detecta por la falta de controles; es decir que existen diversidad de riesgos en los sistemas informáticos

Tabla 9 Ciber amenaza Mundial al 7 de setiembre de 2019 en cuanto a Vulnerabilidad

Puesto	País	Cantidades
1	Las Bahamas	1,08%
2	Guinea-Bisau	0,74%
3	Estados Unidos de América	0,70%
4	República del Congo	0,68%
5	Canadá	0,63%
6	Australia	0,60%
7	Alemania	0,57%
8	España	0,53%

(Poma & Vargas, 2019)

Finalmente, es importante tener en cuenta que, aunque Colombia no encabeza ninguna de estas listas donde se enumeran los ocho países más vulnerables en diferentes ciber amenazas según este mismo informe Colombia se ubica en el puesto número 40 a nivel mundial, como uno de los países más vulnerable ataques cibernéticos.

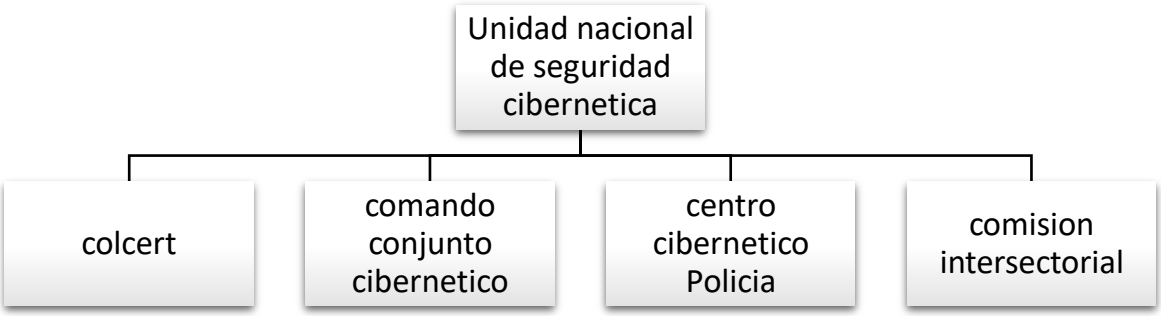
CAPÍTULO V

Lineamientos para la construcción de una política de buenas prácticas para el manejo de información

Plan de acción para la construcción de buenas prácticas en el manejo de la información

Este plan de acción lo que pretende es estar dentro de un ámbito de mejora continua con el fin de que la seguridad cibernética en Colombia cobre mayor importancia para esto se debe desarrollar el uso oficial de las TIC como parte de la política de Colombia se incrementa la competitividad en las compañías de prestación de servicios del mismo modo se debe auxiliar a las empresas locales de tecnologías de la información, con el fin de fomentar una cultura sobre estructura y desarrollo organizacional, así mismo apoyo político por parte del gobierno nacional invirtiendo en personal experto en la materia bien informado, los cuales sean influyentes e importantes en comunidades internacionales, un musculo financiero por parte del estado colombiano sólido, mejorar la eficiencia de la red, soluciones a los problemas de infraestructura digital, Para tener éxito en materia de seguridad cibernética es indispensable capacitar a los usuarios de plataformas hogareñas con el fin de establecer higiene cibernético.

Figura 2 Sinergia de la unidad nacional de seguridad cibernética colombiana fuente edición propia



En la anterior ilustración se muestra la sinergia de la unidad nacional de seguridad cibernética en Colombia mediante la cual se aplicará una estrategia siguiendo con los principios y directrices de la política integral CONPES 3701 está política, ejercida por el gobierno nacional no se deben limitar al ámbito informático, sino que necesitan extenderse a las redes comerciales, controladas por la unidad nacional de seguridad cibernética. Para ello es fundamental establecer una hoja de ruta con el propósito de Evaluar el nivel de la seguridad frente a los riegos y vulnerabilidades cibernéticos en Colombia.

Administración de la seguridad cibernética

A fin de tener una administración optima de la seguridad cibernética se debe establecer una fuerza de trabajo capacitada y disciplinada direccionada al tema administrativo y organizacional, en el marco de modernización y desarrollo de la fuerza pública crear todo tipo de mecanismo que contribuyan a instaurar una estructura de organización sólida en materia de seguridad cibernética no solo en el campo administrativo sino también en lo operacional, sus objetivos son:

- Iniciar proyectos de optimización de los recursos administrativos de la seguridad cibernética utilizando a las agencias de las mismas con la finalidad de conocer las necesidades y retroalimentar a la unidad nacional de seguridad cibernética en Colombia.
- Desarrollar proyectos propuestos a prevenir posibles riesgos organizacionales en materia administrativa y operacional.
- Promover educación y capacitación a las oficinas de las agencias de seguridad cibernética todo bajo el marco de responsabilidad social empresarial con el fin de posibilitar y conocer la legislación en materia de modelos estándares de control de calidad.
- Desarrollar un espíritu de sentido de pertenencia en la unidad nacional de seguridad cibernética y por eso contribuir a la formación vital de una institución que esté acorde a todos los marcos de trasparencia.

La administración de la seguridad cibernética juega un rol muy importante, su eficiencia y validez, es producto de la dirección, habilidades y estrategias que se utilicen todo esto dependerá del trabajo final, y permitirá medir los resultados obtenidos.

Así mismo la delimitación administrativa de la unidad nacional de ciberseguridad, delimitara cada proceso de una forma sistemática como toda ciencia, inicia paso a paso, para que el producto y el proyecto converjan en uno mismo, con el fin de estar conexo de manera adecuada con los demás procesos, que suministra la coordinación deseada.

En la estructuración de la parte administrativa es importante apoyarse en la Guía del PMBOK del Project Management Institute donde se describe el entorno integrador de la dirección de proyectos, que requiere que el Grupo de Procesos de supervisión, Monitoreo y Control y el resto de Grupos de Procesos desplieguen todo tipo de actividades uno sobre los otros de manera retributiva o mutua (Mendoza, 2014).

La combinación de la administración de la seguridad cibernética obedece a especialidades muy particulares que ayudan a determinar una representación holística porque determina características de unificación, consolidación, comunicación y actividades decisivas para que el proyecto se lleve a cabo de manera controlada, de modo que se cumpla con los requisitos o parámetros exigidos, y se pueda establecer un departamento administrado de la unidad de seguridad cibernética.

Este departamento administrativo se requiere no solo trabajar en una especialidad si no apoyarse mutuamente con los procesos de las otras áreas de conocimiento, de modo que el trabajo resulte en la entrega del alcance del producto exigido por la unidad nacional de seguridad cibernética en Colombia Los esfuerzos de cada miembro de la dirección deben llegar a tener un grupo de alto desempeño y liderazgo organizacional de tal manera que se convierta en un soporte fundamental de la Unidad de Seguridad Cibernética de Colombia.

Tomar decisiones a lo largo de cada proyecto es totalmente importante, pero para tomar ese tipo de acciones se debe estar asesorado, suponiendo que para esto hay que tener la disposición con el fin de aceptar todo tipo de recomendaciones asertivas.

Por otro lado un departamento administrativo toma relevancia si se proyecta a desarrollar un ambiente de mejoramiento continuo en la optimización de servicios y procesos, los cuales deben estar plantados desde el análisis de las diferentes perspectivas que se puedan presentar y direccionado a la sugerencia de potenciales soluciones de los problemas por la dirección de administración del riesgo del Ejército Nacional, la cual es vital en un mundo altamente competitivo ya que se debe actuar bajo estándares internacionales.

Es fundamentar tener en cuenta que un gerente de proyectos es la pieza fundamental en el engranaje empresarial porque pone en funcionamiento toda la estructura organizacional de la compañía debido a sus conocimientos y su formación personal, para así mismo poder incorporar clientes potenciales todo esto bajo una visión integradora, hace que su equipo de proyecto sea el más organizado porque evalúan contingencias, analizan riesgos, elaboran procesos todo esto bajo la supervisión, monitoria y control.

Para planificar un proyecto debe establecerse una reunión con el objetivo de unificar un argumento o criterio organizacional de tal manera que se puedan instituir grupos de trabajo con la condición de designarlos en el área de conocimiento específica, así mismo ir en una sola línea de trabajo, tener la habilidad para enfrentar cualquier cambio o reto con su equipo de proyecto.

La unidad nacional de seguridad cibernética debe Inspeccionar y actualizar las políticas, y estándares de seguridad, todo esto para Implementar un sistema de gestión de la seguridad de información (SGSI). La importancia de este organismo gubernamental es ejercer un control eficiente de los casos conocidos a nivel global e interno y los

procedimientos de respuesta a incidentes que han tenido aquellas agencias de seguridad extranjeras para un óptimo desempeño. Así mismo es importante también implementar controles de seguridad cibernética, analizar la prevención de pérdida de datos y programa de gestión de identidades y de accesos. Instaurar los procedimientos de respuesta de incidentes, con el ánimo de originar pruebas de penetración de la red.

Delimitación legal de la Unidad de Seguridad Cibernética.

Aunque la consolidación de esta una unidad encargada de la seguridad cibernética sería una entidad gubernamental, estaría subordinada al comando general de las FFMM, para lo cual necesita enmarcarse en lo parámetro de cada fuerza. De tal manera que permita la articulación de las políticas propuestas por el actual gobierno, que se ajuste a los parámetros proyectado por la institución como los son el Plan de transformación del Ejercito Nacional al 2030, el plan estratégico de las FFMM, Guía de aplicación del Plan Estratégico – GAPE 2015 – 2018 y Plan de Guerra "Espada de Honor", todo esto se encuentra soportado por la constitución política de Colombia en el artículo 217, y regidas por las Política de Defensa y Seguridad para la Nueva Colombia.

Gestión en seguridad informática

La realización, alcance y evaluación de políticas, estratégicas, planes, programas de acuerdo a la normatividad nacional y la evolución de la misma, son acciones permanentes para el conocimiento y la reducción del riesgo entorno a la seguridad informática de la fuerza pública y del estado, bajo el marco de la función pública como un fin social del Estado social de derecho contemplado en la constitución política nacional.

Así mismo la importancia de mitigar los riesgos cibernéticos para contrarrestar este problema, radica en identificar el objetivo de estudio de la norma la cual literalmente nos expresa la necesidad de instituir las directrices y mecanismos con el propósito de asignar las responsabilidades de los múltiples intervinientes sociales en el ámbito de la evaluación, prevención, identificación monitoreo e intervención constante de la manifestación en factores de riesgo cibernético, el diagnóstico de riesgo del mismo debe realizarse por un perito en seguridad cibernética.

De acuerdo con la resolución y normatividad colombiana se razona que un experto es un analista de la seguridad informática. Para que pueda determinar, así como el estudio y determinación de origen de amenazas informáticas presuntamente causadas por todo tipo de grupos de interés. La gestión de seguridad informática se define como un método para determinar, analizar, valorar y clasificar el riesgo, con la finalidad de implementar mecanismos que permitan controlarlo.

Hablar de gestión del riesgo en materia e ciberdefensa implica ahondar en un tema poco explorado, pero que requiere una parametrización inmediata que no permita que los sistemas de seguridad del Estado sean vulnerados, responsabilidad que se le atribuye las FFMM, por su misión constitucional establecida en la constitución política de Colombia de 1991.

Esto lo incluye en el plan nacional de desarrollo PND, el cual se focaliza en tres pilares fundamentales, paz, equidad y educación, pero para poder cumplir con estos tres objetivos es necesario que se garantice la seguridad nacional, desde todo punto de vista.

Conclusiones

Cabe resaltar que, Colombia muy posiblemente enfrentará amenazas y ataques de alta complejidad y sofisticación para los cuales no estará preparado, por lo que, ante el primer objetivo se puede decir que, la protección de datos personales, teniendo en cuenta la normativa existente en Colombia, radica en el sin número de ataques informáticos la página de la presidencia de la República, ha sido vulnerada Gobierno y el ministerio de defensa nacional entre otras instituciones públicas del estado dejaron fuera de servicio varias páginas la modalidad introducir códigos maliciosos otro de los casos emblemáticos de ciber amenazas en Colombia son casos como robo de identidad, robo a cuentas bancarias del mismo modo intento atentarse contra la infraestructura crítica de la nación, pero estos fueron repelidos, por lo que, dentro de su marco de gobernanza y al carecer de un marco de coordinación de políticas de ciberseguridad no puede lograr una adecuada interacción e identificación entre las diversas entidades alrededor del tema.

Por otro lado, en el segundo apartado, se puede afirmar que, dentro de los elementos relevantes para la formulación de un procedimiento que permita garantizar la gestión segura de los datos de los miembros de las Fuerzas militares, se destaca que, el Estados se mantengan actualizado en afinidad a las novedades, las cuales se encuentran en torno a la delincuencia cibernética, hacer énfasis en las políticas de seguridad integral cibernética fue la iniciativa del actual gobierno para destinar un rubro financiero dentro del presupuesto

público para crear un grupo de respuesta a emergencias cibernéticas y demás agencias de ciberdefensa del estado, así las cosas en la actualidad se encuentran en un nivel de madurez formativo y establecido, para llegar a un nivel dinámico se requieren de muchos esfuerzos lo importante es estar en el camino del éxito hacia una política que aporte a generar soluciones a los eventuales riesgo que se puedan presentar.

Así mismo, es importante tener en cuenta que, Colombia hay muchas deficiencias, en los sectores privados, públicos y claro también la densa demografía, no permite que la tecnología llegue a todos los rincones de todo el territorio nacional. Puesto que, no sólo por los ataques que se originen en el país, sino por la sumatoria de ataques que se originan globalmente indudablemente esto lleva a una sensación de desconfianza en el entorno digital.

Y, en un tercer apartando se hace la definición de los lineamientos para la construcción de una política de buenas prácticas para el manejo de información, donde se destaca el plan de acción para la construcción de buenas prácticas en el manejo de la información, así como, la delimitación legal de la Unidad de Seguridad Cibernética y finalmente la gestión en seguridad de la información, teniendo en cuenta, los potenciales riesgos en un ordenador, el número de dispositivos infectados por un sistema operativo de datos que se puede encontrar en cualquier ordenador o CPU así como los datos que han sido vulnerados por un software o programa que permite controlar y supervisar procesos de forma industrial.

Por lo que, para dar respuesta a la pregunta planteada, es importante fortalecer a través de manuales y reglamentos las líneas estratégicas integrales expuestas en el CONPES 3701 mediante las cuales determinan de manera detallada los aspectos técnicos de la ciberseguridad y la ciberdefensa.

Referencias

Aguilar, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios internacionales (Santiago) versión On-line ISSN 0719-3769*.

Álvarez, et al . (2015). *Desafíos y Nuevos Escenarios de la Seguridad Multidimensional en el Contexto Nacional, Regional y Hemisférico en el Decenio 2015-2025".* Bogota : Escuela Superior de Guerra "General Rafael Reyes Prieto".

Arellano, C. A. (2021). El derecho de protección de datos personales. *Biolex versión On-line ISSN 2007-5545versión impresa ISSN 2007-5634*.

Arimetrics. (2017). *Qué es Framework*. Obtenido de Google Ads: https://www.arimetrics.com/glosario-digital/framework

Capó, L. (2015). *Sistemas de Detección de Intrusos en Seguridad Informática.* Habana, Cuba: Ministerio de Salud Pública, Cuba.

Corrochano, et al . (2021). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. *Carta de la Organización de los Estados Americanos*.

Departamento Nacional de Planeación. (2020). *conpes 3995 Politica Nacional de Confianza y Seguridad Digital.* Bogota.

Escobar, et al. (2019). *Integridad y Seguridad en los sistemas de Bases de Datos.* FACTY.

Ferrero, et al. (2018). *Aspectos centrales de la confidencialidad en psicología.* Bogota: X Congreso Internacional de Investigación y Práctica Profesional en Psicología.

Hernández, et al . (2014). *Metodologia de la Inestigaciòn.* Mexico: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Herrán, A. I. (2017). *El derecho a la intimidad en la nueva ley orgánica de protección de datos.* Librería-Editorial Dykinson.

Lavinder, K. (2019). *Ataques Cibernéticos ¿Está preparada América Latina?* Universidad Salve Regina.

Lopez, J. (2019). *MIGRACIÓN VENEZOLANA EN COLOMBIA: UN DESAFÍO PARA LA SEGURIDAD.* Bogota : UNIVERSIDAD MILITAR NUEVA GRANADA.

Maldonado, et al. (2019). *LOS DATOS PERSONALES COMO CONTRAPRESTACIÓN ECONÓMICA: A PROPÓSITO DEL CASO GOOGLE VS CHU Y LA PROTECCIÓN DE LOS DERECHOS DEL CONSUMIDOR.* Universidad Católica San Pablo.

Mejía, M. I. (2020). *G.INF.06 Guía Técnica de Información - Gobierno del dato.* Bogota: Ministerio de Tecnologías de la Información y las Comunicaciones.

Meraz, A. I. (2018). *Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales.* Monterrey, Mexico: Instituto de Ciencias Jurídicas de Puebla, Departamento de Investigaciones.

Mieres, J. (2019). *Ataques informático Debilidades de seguridad comúnmente explotadas* . White paper.

Mok, S. C. (2010). PRIVACIDAD Y PROTECCIÓN DE DATOS: UN ANÁLISIS DE LEGISLACIÓN COMPARADA. *Diálogos Revista Electrónica de Historia*, 111-152.

Molano, D. A. (2021). *POLÍTICA DE EDUCACIÓN PARA LA FUERZA PÚBLICA 2021 – 2026: hacia una educación diferencial y de calidad.* Bogota: Ministerio de Defensa Naciona.

Mora. (2021). PRiVACiDAD Y SEGURiDAD EN iNTERNET. *INCIBE* .

Mosquera, V. (2019). *CIBERSEGURIDAD EN COLOMBIA.* Bogota : Universidad Piloto de Colombia.

Pérez, Y. (2017). *Importancia de la Ciberseguridad en Colombia.* Bogota : Universidad Piloto de Colombia. .

Poma, A. E., & Vargas, R. L. (2019). Problemática enCiberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. *SCIÉNDO*, 275-282.

Ramiro, M. A. (2015). *El derecho fundamental a la protección de datos personales en Europa.* Alcala : Universidad de Alcala .

Sheldon. (2012). eciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, 95-112.

Significados. (22015). *Significado de Vulnerabilidad*. Obtenido de Qué es Vulnerabilidad:: https://www.significados.com/vulnerabilidad/

Tamayo. (2020). Protección de la información. *INICBE* .

Urbina, M. (2011). *TRAZABILIDAD.* UCATSE: UNIVERSIDAD CATOLICA AGROPECUARIA DEL TROPICO SECO UCATSE Pbro. “Francisco Luis Espinoza Pineda”.

Vargas et, al. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad ISSN: 1390-4299*, 31-45.