PROPUESTA DE UN MODELO EN EL TRATAMIENTO DE DATOS PERSONALES PARA EL CONTROL DE ACCESO UBICADO EN EL COMANDO AÉREO DE MANTENIMIENTO CAMAN

Mayor GÓMEZ MASTRODOMENICO JUAN SEBASTIÁN

Capitán Morales Carvajal Robinson Augusto

Director de Trabajo

ESCUELA DE POSTGRADO DE LA FUERZA AÉREA COLOMBIANA

MAESTRÍA EN DIRECCIÓN GESTIÓN Y DE LA SEGURIDAD INTEGRAL

COHORTE III

2022

PROPUESTA DE UN MODELO EN EL TRATAMIENTO DE DATOS PERSONALES PARA EL CONTROL DE ACCESO UBICADO EN EL COMANDO AÉREO DE MANTENIMIENTO CAMAN

Mayor GÓMEZ MASTRODOMENICO JUAN SEBASTIÁN

Proyecto presentado para optar al título de Maestrante en Dirección y Gestión de la Seguridad Integral

Capitán Morales Carvajal Robinson Augusto

Director de Trabajo

ESCUELA DE POSTGRADO DE LA FUERZA AÉREA COLOMBIANA

MAESTRÍA EN DIRECCIÓN GESTIÓN Y DE LA SEGURIDAD INTEGRAL

COHORTE III

2022

Agradecimientos

A todas aquellas personas que la vida y Dios se ha encargado de cruzar en mi camino, a mi familia como pilar fundamental en el desarrollo de este trabajo, a mi esposa a mis hijos, a mis amigos en esta vía del Postgrado, por la cual pasamos las dificultades y las satisfacciones de ser estudiantes, algunos encontrados al principio de la Maestría otros ya al final, pero igual importantes y queridos todos para mí, de verdad nunca los olvidaré, les deseo mucho éxito en su vida profesional y personal.

Índice de Contenido

1. INTRODUCCIÓN 10

2. PLANTEAMIENTO DEL PROBLEMA ..... **¡Error! Marcador no definido.**

3. OBJETIVOS 21

3.1. Objetivo General 21

3.2. Objetivos Específicos 21

4. JUSTIFICACIÓN 22

5. ANTECEDENTES 24

6. MARCO DE REFERENCIA 40

6.1. Marco Teórico 40

Dato 44

Defensa y Seguridad integral 47

Factor humano 48

Sistemas de seguridad y factor humano 50

Delitos informáticos en Colombia 51

Metodología de gestión de riesgo a utilizar 54

6.2. Marco contextual 57

6.3. Marco normativo 63

Decreto 1797 de 2000 Reglamento de régimen disciplinarios para las fuerzas militares 64

Decreto 1799 de 2000. Por el cual se dictan las normas sobre evaluación y clasificación para el personal de Oficiales y Suboficiales de las Fuerzas Militare y se establecen otras disposiciones 64

Manual de Estado Mayor Fuerza Aérea- Manual FAC 3-05. Tercera Edición 65

Decreto no. 1428 de 2007. Por el cual se cumplían las normas de Decreto Ley 2000, Por el cual se modifica el decreto que regula las normas de carrera del personal de Oficiales y Suboficiales de las Fuerzas militares. 65

Decreto 317 de 2005 65

Ley 1581 de 2012 66

Principios rectores que rigen el tratamiento de datos personales a la luz de la ley 1581 de 2012 ..... **¡Error! Marcador no definido.**

7. PILOTAJE ..... **¡Error! Marcador no definido.**

8. METODOLOGÍA 72

Diseño de estudio 72

Tipo de estudio 73

Población y muestra 77

Fuentes primarias y secundarias 80

Instrumentos de recolección de datos 80

9. ENTREGABLES 84

10. ANÁLISIS DE RESULTADOS 85

10.1. Situación actual en protección de datos personales haciendo énfasis en las debilidades que exponen a terceros los datos personales para salvaguardar los datos. 85

10.2. Elementos que debe contener el modelo de protección de datos que ayuden a mitigar el riesgo de pérdida de la información 94

10.3. Modelo de protección de datos personales en el control de acceso que mediante formatos y procedimientos permita asegurar la integridad de la información 108

11. CONCLUSIONES 155

12. RECOMENDACIONES 158

13. REFERENCIAS BIBLIOGRÁFICAS 161

14. ANEXOS 167

Índice de Tablas

Nº	Tabla	p.p.
1	Frecuencia de delitos informáticos en Colombia	32
2	Operacionalización de las variables	56
3	Análisis de la Revisión Documental	102
4	Triangulación de la información	105
5	Ciclo De Las Etapas Del Modelo De Protección De Datos	100
6	Análisis de las Bases de Datos	101
7	Descripción de mecanismos de procesamiento de bases ……	102
	Campos que conforman la base de datos	103
8	Permisos concedidos por el propietario de la información	104
9	Información sobre el encargado del tratamiento de los datos	104
10	Transferencia Internacional/Categorización	105
11	Criterios de Categorización de la información proporcionada por	
12	el titular	105
	Artículo 18 Deberes de los Encargados de la Información	108
13	Proceso de Consultas y Solicitudes por inconformidad	111
14	Registro cronológico de consulta y quejas	114
15	Previsiones de Seguridad de la Información	115
16	Cuestionario Diagnóstico para el Cumplimiento ley 1581	123
17	Responsabilidad demostrada	129
18	Fases del proceso continuo de gestión de los riesgos	135
19	Inventario y Valoración de Activos de Información	139
20	Nivel de Restricción	140
21	Responsables	140
22	Identificación de Riesgos	141
23	Evaluación del riesgo	141
24	Descripción de Controles	142
25	Calificación del Control	143
26	Tratamiento de Riesgo	144

Índice de Figuras

Figura 1.Normas de control interno…… 58

Figura 2. Procedimientos existentes…… 59

Figura 3. Estructura organizativa…….60

Figura 4. Entrada y salida de datos……..61

Figura 5. Calidad de datos……...62

Figura 6. Control de datos……...63

Figura 7. Control de datos (continuación)……...64

Figura 8. Almacenamiento de datos ……...65

Figura 9. Tipos de datos …….66

Figura 10. Ambiente de control ……..67

Figura 11. Evaluación de riesgos…….……69

Figura 12. Actividades de control ……...70

Figura 13. Información y comunicación …….71

Figura 14. Monitoreo ……..72

Figura 15. Lineamientos gerenciales ……..……75

Figura 16. Riesgo de calor inherente …….145

Figura 17. Riesgo de calor residual……....146

Resumen

La presente investigación propone un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento, mediante un análisis documental tanto al interior como al exterior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN. En tal sentido, se estudia el marco teórico relacionado, para así identificar las prácticas, vulnerabilidades y amenazas que pueden afectar directamente el desarrollo de los procesos en referencia a la seguridad de la protección de datos en el Comando Aéreo de Mantenimiento; analizar los resultados obtenidos relacionados a la seguridad de los datos en la Unidad y proponer lineamientos en gestión del riesgo. Luego de obtenidos y discutidos los resultados, se obtuvieron conclusiones entre las que se evidencian debilidades notorias con respecto a los indicadores que tienen su origen en los postulados de la Ley 1581 de 2012, como también la interrelación de estos indicadores con los distintos elementos que configuran la gestión de la protección de los mismos, entre los cuales están la supervisión, monitoreo, el control y la información. Así, se presentan una serie de estrategias para dar cumplimiento a la propuesta específica del trabajo. Sobre la estructura del trabajo, en el primer capítulo se trató el problema de investigación, con sus objetivos y la justificación. En el siguiente apartado, se describieron los antecedentes, marco referencial y pilotaje. Seguidamente, se exploró el capitulo de la metodología con la delineación de los entregables del trabajo y del tipo de investigación; luego, se abordó el apartado de los resultados, terminando con las conclusiones y recomendaciones del estudio.

Palabras clave: protección de datos, seguridad, riesgo, estrategias.

Abstract

This research proposes a personal data protection model for access control in the security group of the Air Maintenance Command, through a documentary analysis both inside and outside the force to safeguard the sensitive information of organic and floating personnel CAMAN. In this sense, the related theoretical framework is studied, in order to identify the practices, vulnerabilities and threats that can directly affect the development of the processes in reference to the security of data protection in the Air Maintenance Command; analyze the results obtained related to data security in the Unit and propose risk management guidelines. After obtaining and discussing the results, conclusions were obtained among which notable weaknesses are evident with respect to the indicators that have their origin in the postulates of Law 1581 of 2012, as well as the interrelation of these indicators with the different elements that make up the management of their protection, among which are supervision, monitoring, control and information. Thus, a series of strategies are presented to comply with the specific proposal of the work. On the structure of the work, in the first chapter the research problem was discussed, with its objectives and justification. In the following section, the background, referential framework and piloting are described. Next, the methodology chapter was explored with the delineation of the deliverables of the work and the type of research; then, the results section was addressed, ending with the conclusions and recommendations of the study.

Keywords: data protection, security, risk, strategies.

Introducción

Los datos personales en la actualidad son tratados como un valor intangible pero que sin duda las entidades y personas que necesitan la información lo conocen, sin duda cualquier sociedad desconoce su importancia pero reconoce que es de gran importancia su regulación pues con esto se busca protegerla, hoy en día desde el momento de ingresar a un sitio web y utilizar un programa específico se está brindando datos personales que no se sabe a dónde y en manos de quien irán a parar, para esto es fundamental implementar un modelo en el tratamiento de datos personales en el control de acceso del CAMAN.

Por lo anterior, se puede identificar que en Colombia desde la Constitución Política de 1991 se incorporó la importancia de la protección de datos personales lo cual quedo registrado en el artículo 15 donde se establece la protección de derechos fundamentales tales como el derecho a la intimidad y al buen nombre, es acá donde el estado ha ordenado desplegar todas las capacidades y acciones necesarias para la adecuada recolección, tratamiento y circulación de la información de los colombianos.

Es importante recordar, que a partir de la entrada en rigor de la Ley 1581 de 2012 y donde se da un ámbito de aplicación y unas definiciones se hace necesario el cumplimiento de lo consagrado en esta ley, después de consultar información en los grupos de seguridad es evidente que carecen de un modelo en el tratamiento de datos personales, por lo cual es imperante su creación para proteger la información del personal orgánico y flotante de la base con el fin de determinar debilidades y fortalezas en el tratamiento de datos personales en el control de acceso de CAMAN, se deben analizar las posibles soluciones al problema en mención. La especialidad de seguridad y defensa ha buscado garantizar en los 92 años de existencia la seguridad de las bases, minimizando los riesgos en contra del personal e infraestructura (Jefatura de Seguridad y

Defensa, 2018), es por esto que el personal de hombres y mujeres que la conforman estudian nuevas amenazas que han mutado desde el espacio físico hasta el ciberespacio y es allí donde se introduce la importancia de la protección de datos personales en los sistemas de control de acceso.

En este sentido, debido al aumento de las formas de conexión a la internet y a un mundo globalizado donde la tecnología a determinado una facilidad para conectarnos desde cualquier aparato, los datos personales han venido tomando un gran auge, es por esto que las organizaciones deben garantizar el correcto tratamiento, garantizando los respectivos responsables de la información como lo establece el artículo 3 de la ley 1581 de 2012. Por tal razón, se hace trascendental hablar sobre la clasificación de los datos personales en el país para entender el riesgo que hay cuando se dejan los datos sin la debida protección y sin un responsable.

Por lo anterior, es importante definir varios puntos importantes en este trabajo, se inicia por la definición de la RAE donde determina que el dato viene de latín datum “lo que se da” y lo define como la información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho (RAE, 2019), por otro lado se puede decir que un dato sin un análisis especifico no significa nada, por lo que se entiende de la importancia de mantener los datos personales seguros, entendiendo que son datos que pueden manejar información sensible de las personas; por otro lado un dato personal es cualquier información que se refiera a una persona.

A título enunciativo, estos datos pueden hacer referencia a los siguientes aspectos de un ser humano: familia, transacciones financieras, salud, solvencia económica, creencias religiosas, procesos y condenas criminales, origen racial y étnico, profesión, títulos y grados académicos,

comportamiento sexual, hobbies, salarios, ideas políticas, etc. (Bruselas, 2007). Entiéndase dato personal como cualquier información concerniente a personas físicas, que tengan carácter de privado, que está ligada a su intimidad y que toque temas susceptibles de discriminación, como orientación sexual, religiosa, étnica, entre otros (Certicamara, 2013).

De esta forma, mediante un estudio de enfoque cuantitativo apoyado por una revisión documental en el control de acceso del grupo de seguridad en el CAMAN, a través de encuestas y entrevistas al personal orgánico y flotante de la Unidad se busca determinar la forma de tratamiento de datos personales, las posibles limitaciones que podemos encontrar en esta investigación es la falta de procedimientos e instructivos en este tema de protección de datos personales, teniendo en cuenta que no es el área responsable de este manejo de la información pero si quien debe ser el custodio de la misma, es acá donde radica la importancia de establecer un formular un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo , con el fin de proteger la información sensible de las personas orgánicas y flotantes de la base.

Por otro lado, a partir de la entrada en vigor de la ley estatutaria 1581 de 2012, se da designación para que a través de la Superintendencia de Industria y Comercio SIC sea la responsable de velar por el tratamiento de los datos personales en Colombia, tarea que no ha sido fácil pues teniendo en cuenta según Argüello (2015) que hoy en día existen muchas entidades que no cumplen con la normatividad vigente ordenada y donde hay un gran porcentaje de empresas privadas y públicas que aún no realizan el tratamiento de datos según la ley en mención, la recolección de datos personales debe tener una finalidad legítima y cierta, es decir, una razón de ser de esa recolección. Además, los datos recolectados deben ser pertinentes y adecuados para alcanzar dicho fin.

De igual forma, el tratamiento de los datos personales fue uno de los temas tratados durante la asamblea nacional constituyente para que se respetarán, no vulneraran o pusieran en riesgo los derechos y libertades de las Colombianas y los colombianos, cuando el Estado y las organizaciones recolectaran, almacenaran o usaran la información sobre las personas"(Remolina, 2013), por lo que se puede inferir que desde la constitución del 1991 se hizo importante para el estado dicha protección de los datos personales para los ciudadanos. Del mismo modo, la Corte Constitucional con la sentencia T-729 de 2002 unificó los principios de administración de datos personales en Colombia, estableciendo de esta manera como el primer antecedente inmediato en la ley 1266 de 2008 conocida como Habeas data en el País, siendo importante aclarar que esto inicia como protección a los usuarios en el sector financiero pero luego se desliga y se hace necesario crear una legislación especial para protección de datos personales y es acá donde nace la Ley 1581 de 2012 la cual busca salvaguardar la información de los usuarios.

Por lo tanto, con los avances de hechos en el mundo y principalmente en Colombia, las tecnologías de la información y comunicación TIC, los datos personales de los ciudadanos se han convertido en un componente primordial de las relaciones sociales y de la economía en sí misma, motivo por el cual se han convertido en el valor agregado, teniendo en cuenta que la información personal es una importante moneda del milenio. El valor monetario de esta clase de información es grande y sigue creciendo (Schaeartz, 2004).

Así, con la transformación digital que está viviendo el país se hace necesario la implementación de mecanismos que puedan garantizar la integridad de la información obtenida de las personas y esta política de tratamiento de datos personales ayuda a proteger la información sensible que se entregan en los ingresos de las Unidades. Teniendo en cuenta que Colombia es un estado de derecho, se debe garantizar los derechos fundamentales plasmados en la Carta

Magna, en esta se aclara que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre por lo que es importante que las instituciones sean garantes de hacer cumplir lo ordenado en las leyes y tratados nacionales e internacionales respectivamente.

En concordancia con lo anterior, y entendiendo que hoy en día los datos personales son tratados como una mercancía con un valor incalculable de acuerdo al objetivo del negocio, es necesario mirarlo con mayor importancia y este trabajo formular un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento desde un nivel interno hasta referentes mundiales, revisando información dentro de la fuerza en las dependencias que desde su funcionalidad deben realizarlo, en el país a nivel legal y sancionatorio y referentes regionales e internacionales para poder forjar unas bases sólidas en la protección de datos personales que genere un cumplimiento total desde la normatividad y como marco regulatorio para salvaguardar los datos personales de los funcionarios y personal flotante.

De tal manera, es importante conocer a nivel internacional como se realiza el tratamiento de datos personales, por lo anterior se realiza también una revisión de los estudios previos internacionales y nacionales, con esto se busca conocer el nivel de protección que se tiene en el país y que puede hacer falta de acuerdo a la comparación hecha, para poder tomar las buenas costumbres y aplicarlas a nivel institucional con el fin de proteger los datos personales, se debe tener cuidado con los tratamientos de datos personales que se realizan en otros países, pues cada estado es garante de manejar sus leyes de acuerdo a sus necesidades y esto puede llevar a que la información se mueva en el mercado negro de las empresas con fines comerciales o delincuenciales, es importante los tratados internacionales en relación a este tema para evitar que nuestros datos sean vendidos al mejor postor.

Consecuentemente, las recomendaciones que se deben hacer en materia de datos personales inician desde lo básico como permitir el tratamiento hasta la modificación o eliminación de nuestra información, es acá donde se deben hacer campañas con las personas flotantes y orgánicas para informarles de cómo se va hacer dicho tratamiento de datos, quien va hacer el custodio y quien los va a tratar o donde puede hacer modificaciones si así lo requiere, teniendo en cuenta que esto aun no es normal para los dueños de la información. Lo que se busca es concientizar a las personas del tratamiento que se va a realizar para que conozcan sus derechos como titular de los datos, se debe designar una persona como la encargada de la protección de datos personales dentro del control acceso.

De igual forma, es importante poder formular un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento, mediante un análisis en el interior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN, ya que las instituciones deben propender por garantizar la custodia y el tratamiento de acuerdo a la Ley.

Problema de Investigación

En el seno de la Fuerza debe laborar personal que apoye los procesos internos que se dan en cada una de las Fuerzas que la componen para cumplir la misión inherente al conjunto de principios, políticas y objetivos que tienen asignada. De tal manera, este personal militar se ve afectado por diversos factores que inciden en su eficacia, algunos de ellos son de acuerdo con la visión de Valverde et al. (2016), la alineación de los procedimientos internos de este tipo de instituciones y las reglamentaciones dadas por el Estado donde buscan garantizar la protección de los datos a los usuarios para evitar algún tipo de fraude cibernético.

En este sentido, la correcta implantación de la normativa de protección de datos y seguridad de la información en las organizaciones militares de hoy en día permite que las mismas puedan utilizar los datos con mayor inteligencia aplicada y eficiencia. Por lo tanto, los datos personales son y serán en los próximos tiempos un activo crucial y determinante para la viabilidad y años de vida de una organización. Recopilar mayores datos significativos, crear estructuras técnicas y organizativas adecuadas que permitan analizar, extraer y usar dichos datos, va a permitir a las instituciones modernas tomar decisiones más acertadas, lo que se traduce en una mayor eficiencia y mayores beneficios. Así, la Comisión Europea a través de su grupo de trabajo ha expresado que la protección de datos personales tendrá la obligación de aplicar medidas reales y eficaces que minimicen el riesgo económico y jurídico de lo que podría generar la no protección de datos (Comisión Europea, 2010).

En relación a lo anterior, de acuerdo a la definición de los controles de acceso como dispositivos que impiden o retrasan cualquier acto de intrusión que atente contra la seguridad (Bedoya, 2014) se hace imperativo identificar cuáles protocolos de protección de datos personales son aplicables en instituciones militares con el fin de mitigar el riesgo de atentados

cibernéticos que puedan generar pérdida de información para las Unidades, partiendo de la premisa que la información es uno de los activos más importantes para la fuerza.

En relación a Colombia, en la Superintendencia de Industria y Comercio se establecen unos principios básicos para el tratamiento de datos personales que se puede utilizar como guía en instituciones militares, este listado de comprobación puede tomarse como la hoja de ruta para verificar el cumplimiento de la implementación de acuerdo a los principios y deberes establecidos en la Ley; así, se debe tener en cuenta que la información personal que se recolecta es para finalidades legítimas informando al titular acerca de la finalidad con la que se va a tratar, de igual forma se cuenta con el consentimiento previo, expreso e informado donde el titular autoriza para realizar dicho tratamiento de datos.

Asumiendo esta premisa, se deben garantizar las medidas técnicas para controlar y brindar el acceso a la información personal solo a los titulares o a terceros de acuerdo a lo autorizado por la Ley; así, con estos puntos mencionados anteriormente se puede establecer la piedra angular para lograr el cumplimiento mínimo en la protección de datos personales conforme a la ley; es importante aclarar que estos temas están en constante actualización y deben ir de la mano con las recomendaciones que se establezcan a nivel interno en materia de ciberseguridad por la parte funcional.

Partiendo de lo dicho, en Colombia, el Comando Aéreo de Mantenimiento es actualmente considerado como la cuna de la logística Aeronáutica y pionero en la fabricación de aeronaves T90 CALIMA que hacen parte de la flota de aviones de la Fuerza Aérea del país. En el presente, es la Unidad más antigua de la Fuerza Aérea Colombiana y en alianza con la Corporación de la Industria Aeronáutica Colombiana CIAC, lidera procesos de mantenimiento mayor al equipo aeronáutico de la fuerza pública, potencializando las capacidades del talento humano que trabaja

con calidad, eficiencia y eficacia; mediante la definición de políticas y lineamientos que han permitido el trabajo coordinado y la gestión de estrategias de mejoramiento del conocimiento que han orientado el trabajo grupal.

De esta manera, en el Comando Aéreo de Mantenimiento, en el grupo de Seguridad y Defensa de Bases Aéreas N° 95 actualmente trabajan 13 Oficiales, 47 Suboficiales y 262 Soldados, responsables de velar por la Seguridad y la defensa de la Unidad, datos recabados de acuerdo con el Grupo de Seguridad y Defensa de Bases Aéreas de la Fuerza Aérea de Colombia (2020).

Así, dicha Unidad posee la capacidad para enfrentar la amenaza, mediante la estandarización operacional, infraestructura, equipos y armamento que brinda la sostenibilidad en el desarrollo de operaciones aéreas y cumplimiento de los fines del Estado. Así mismo, deben mantener y garantizar la seguridad de las Unidades Militares Aéreas por medio del desarrollo de operaciones de seguridad y control, utilizando entre otros, sistemas electrónicos para la seguridad, equipos de reacción, productos de seguridad, análisis de riesgo; así desarrollan operaciones especiales de apoyo a las operaciones aéreas, en donde resalta la importancia de contar con un sistema integral de Seguridad para el CAMAN que garantice la supervivencia de la Unidad.

No obstante, se han presentado dificultades en la seguridad y defensa del Comando Aéreo de Mantenimiento (CAMAN), ya que se realizó una observación directa con relación al tratamiento de datos personales relacionado con la seguridad y defensa de bases aéreas. Así, a pesar que los controles de acceso en las Unidades militares están diseñados para identificar y enrolar el personal visitante, no existe un responsable en el tratamiento de datos personales que es necesario de acuerdo con la Ley 1581 de protección de datos. También, se han presentado

eventos donde el personal que labora en esta área utiliza los datos personales para realizar llamadas y envío de mensajes a las personas que reportan información generando inconvenientes en el área y para las personas tanto residentes como visitantes, siendo efectivamente una infracción a la seguridad de la información y a la seguridad física de la base (JES, 2019).

De la misma manera, existen casos registrados donde se ha perdido información de datos personales. Consecuentemente, lo descrito anteriormente puede generar una falla, ya que la pérdida, suplantación o variación en el sistema de ingreso produce ingresos de manera ilegal a la base, por lo que se esperaría en un futuro cercano un empeoramiento de la situación ya que atentados en contra del personal e infraestructura de la institución serían entonces difíciles de evitar.

De tal forma, los síntomas anteriores conllevan a deducir que el problema actual consiste resumidamente en la falta de un modelo de protección de datos personales para el control de acceso en la unidad de seguridad del Comando Aéreo de Mantenimiento.

En efecto, el deber ser implica que se debe conocer cómo se realiza el tratamiento de los datos personales en el control acceso al Comando Aéreo de Mantenimiento (CAMAN), con la finalidad de formular un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento, mediante un análisis en el interior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN.

De igual forma, es necesario una autorización escrita explícita donde los titulares autoricen para el tratamiento de datos, es importante informar en un sitio visible en el ingreso del control acceso a la unidad sobre los derechos que le asisten a los titulares de la información indicando que está permitido el ejercicio a conocer, actualizar y rectificar los datos personales que autorizaron a recolectar, aclarar que en caso de alguna solicitud, queja y copia se tratara de

acuerdo a la ley y dentro de los términos ordenados, por último se debe informar a los titulares cuando se actualice el modelo de tratamiento de datos personales.

En resumen, teniendo en cuenta que en los controles de acceso se manejan los datos del personal orgánico y visitante a la Base, es responsabilidad de la Fuerza el manejo que se le da, es acá donde el presente trabajo trata de solucionar la problemática presentada formulando un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento, mediante un análisis en el interior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN; la anterior premisa obliga a extremar las medidas de seguridad en ciberseguridad tendientes a reducir posibles afectaciones a los sistemas de información; así, al tener sistemas robustos de seguridad se puede minimizar los intentos de ataques.

Objetivos

Objetivo General

Formular un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento, mediante un análisis en el interior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN.

Objetivos Específicos

- Describir la situación actual en protección de datos haciendo énfasis en las debilidades que exponen a terceros los datos personales para salvaguardar los mismos, basado en los postulados de la Ley 1581 de 2012.
- Establecer los elementos que debe contener el modelo de protección de datos que ayuden a mitigar el riesgo de pérdida de la información, con base en la medición de los postulados de la Ley 1581 de 2012.
- Diseñar un modelo de protección de datos personales en el control de acceso que mediante formatos y procedimientos permita asegurar la integridad de la información.

Justificación

A partir de la expedición y entrada en funcionamiento de la ley 1581 de 2012 que trata de la privacidad de los datos personales y teniendo como referencia el reporte de riesgos globales del 2020 del foro económico mundial, donde se muestra que los delitos informáticos y robo de información son los más comunes en los años 2018 y 2019, la formulación de un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento, mediante un análisis en el interior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN. Es acá, donde radica la importancia de que las instituciones cuenten con mecanismos capaces de soportar y minimizar los riesgos existentes dentro de un contexto interno y externo, teniendo en cuenta que la información es uno de los activos estratégicos más importantes para la organización, dicho de otra manera al ocurrir un evento que altere el normal desarrollo generando impacto y ocasionando una probabilidad alta de parar, se debe contar con una alta resiliencia que permita reestablecer de manera rápida el objetivo del negocio, en este punto los hombres de seguridad destacados en las unidades deben ser los primeros en tomar acciones que garanticen la seguridad de la información y el tratamiento correcto para evitar problemas por el descuido.

Así mismo, el tener una política de tratamiento de datos en el control acceso ayudara a tener una guía para la protección de la información como activo fundamental, evitando la perdida, el fraude y demás delitos que puedan incurrir las personas por mal uso de los datos, por otro lado, nos ayuda a ser garantes como institución del estado en salvaguardar la información que almacenamos de las personas que ingresen a la Unidad.

Igualmente, es importante informar a las personas orgánicas y flotantes que brindan datos personales para ingresar a la Unidad, que serán tratados de acuerdo con lo reglamentado en la ley

1581 de 2012, donde se establece unas responsabilidades para la entidad y con las cuales se deben dejar plasmadas en un formato de autorización de datos, estos se usaran exclusivamente para verificar antecedentes y así poder tomar la decisión si se autoriza el ingreso a la dependencia o no.

Por lo anterior, se hace necesario que se nombre una persona encargada de custodiar la información recolectada por la dependencia de control acceso, esta será la responsable de tratar los datos como se especifica en la ley, dando alcance a los lineamientos institucionales y brindando la integridad de los datos entregados por las personas.

De esta manera, esta política va encaminada a proteger la información brindada por las personas orgánicas y flotantes que ingresan al CAMAN, determinando responsabilidades dentro y fuera de la institución con el fin de salvaguardar los datos que se han obtenido para poder autorizar el ingreso a la BFA, es importante poder mitigar cualquier perdida de información de dato personal, público y sensibles del titular que brindo datos a través de una autorización a la institución.

Así, la importancia de esta política de tratamientos de datos personales en el CAMAN radica en minimizar el riesgo de pérdida de información obtenida por el titular a través de un ingreso a la Unidad, por lo que como institución se debe ser garante en cumplir con las normas ordenadas por el estado colombiano, de acuerdo con Garriga (2020), el principio de finalidad resulta ser el más importante pues define la finalidad y el uso de la información recolectada, aclarando para que puedan ser utilizados, esto debe ser la hoja de ruta en el tratamiento de datos personales en Colombia, lo que puede ayudar a que los datos sensibles sean tratados con el fin que se brindaron.

Antecedentes

Colombia es un estado social de derecho lo que permite definir que desde la constitución de 1991 el estado debe garantizar los derechos y deberes de los ciudadanos a través de las instituciones y autoridades, en consecuencia, se ha podido establecer antecedentes a la protección de datos personales en el país, así:

5.1. Con respecto a la Constitución de 1991, si se interpreta el Artículo 2; son metas primordiales del Estado: servir a la comunidad, auspiciar la prosperidad básica y garantizar la eficiencia y eficacia de los postulados, derechos y deberes determinados en la Constitución; así mismo proveer la colaboración de todos en las decisiones que incidan en el quehacer económico, político, administrativo y cultural de la República; defender la independencia del país, conservar la integridad del territorio y preservar la convivencia armoniosa y la vigencia de un orden de justicia. Las autoridades de la nación están instituidas para proteger a todos los individuos que residen en el país, en su vida, virtud, bienes, fe y restantes derechos y libertades, y para cerciorar la observancia de los deberes sociales del país y de los individuos.

Y con respecto al artículo 15: todos los individuos tienen derecho a su privacidad personal y familiar y a su buen nombre, y el Estado debe respetarlos. De la misma manera, tienen derecho a saber, renovar y corregir los datos que se hayan recolectado inherente a éstas en las bases de datos y en archivos de organismos públicos y privados. En la reunión, tratamiento y circulación de información se respetarán la libertad y otras garantías que consagre la Carta Magna.

De tal manera, solamente pueden ser obstaculizados o realizado su registro a través de orden judicial, en los casos y con los formulismos que normalice el estatuto. Con la finalidad de advertir la comisión de hechos terroristas, una regla estatutaria normalizará forma y

circunstancias en que las autoridades que ella indique, con basamento en importantes motivos, puedan interceptar o registrar la correspondencia y otros formatos de comunicación privada, sin precedente orden judicial, con aviso contiguo a la Procuraduría General de la Nación y control judicial siguiente dentro de las treinta y seis (36) horas sucesivas.

Consecuentemente, al comenzar cada lapso de sesiones el Gobierno rendirá reporte al Congreso sobre la utilización que se realicen de esta facultad. Los delegados que abusen de las medidas que describe este apartado incurrirán en falta muy grave, sin perjuicio de los otros compromisos que sucedan. Para efectos tributarios judiciales y para asuntos de inspección, control e intervención del Estado, podrá requerir la exposición de libros contables y demás escritos privados, en los señalamientos respectivos de la normativa.

De tal manera, dentro de los avances para lograr proteger los datos de los ciudadanos, el estado a través de la ley 1266 de 2008 establece la protección de los datos personales en especial los financieros y crediticios que fueron denominados como habeas data.

5.2. De igual manera, la Corte Constitucional recordó que la sentencia C-748 de 2011 señaló que la recolección de datos personales por parte de las autoridades públicas no puede convertirse en un escenario de abuso del poder informático. “Pueden solicitar datos personales a los ciudadanos, incluso con carácter obligatorio, pero esos datos deben ser los estrictamente necesarios para el cumplimiento de la función específica”.

Para poder cumplir el marco normativo se hace imperativo que apliquemos lo dispuesto en el CONPES 3701, donde se establecen unas normas de protección en ciberdefensa y ciberseguridad (CONPES 3701, 2011), teniendo en cuenta que los datos personales que vamos a tratar los debemos cuidar y proteger para que esta información vital para el personal interno y externo a la BFA no sean de conocimiento público de acuerdo a la clasificación de la

información, recordando que somos en este momento los responsables del tratamiento de dicha información.

Teniendo como marco normativo la ley 1581 de 2012 y 1377 de 2013, donde se establece la protección de datos personales y el tratamiento de los datos respectivamente, se relaciona la forma en que se debe tratar los datos de cada persona y ordena a la SIC ser la garante de la información y la responsable en sancionar a las empresas que no cumplan con la ley.

Este modelo está definido dentro del sector de tecnología como el área a realizar el estudio, pues es allí, donde se puede determinar que los datos personales son el activo más importante en el control de acceso dentro de una BFA, pues de esto depende el buen nombre de la institución, los datos personales deben ser siempre una prioridad para el personal que tiene a cargo el tratamiento de los datos personales esto de acuerdo a lo consagrado en el decreto 1377 de 2013 artículo 6 donde dice que se deberá cumplir lo siguiente:

Comunicar al titular que por tratarse de datos sensibles no es necesario delegar su procesamiento. Igual, avisar al titular de forma manifiesta y previa, además de los requisitos formulados, de la autorización para la agrupación de otro tipo de dato personal, cuáles de los datos que serán objeto de procesamiento son sensibles y la finalidad del tratamiento, así como conseguir su consentimiento deliberado. (Decreto1377, 2013).

En lo referente a lo que expone Remolina (2013) “El tratamiento de los datos personales fue uno de los temas que se propuso, analizó y aprobó en la Asamblea Nacional Constituyente para que se respetaran, no vulneraran o pusieran en riesgo los derechos y libertades de las colombianas y los colombianos, cuando el Estado y las organizaciones recolectaran, almacenaran o usaran la información sobre las personas” (p.14).

Se debe realizar un estudio de sitio en una base específica, donde se analice que aspectos se deben implementar para poder garantizar la protección de datos, desde su recolección, y tratamiento teniendo en cuenta el reporte del forum economic world en su informe de riesgos globales 2020 donde muestra en condiciones de probabilidad que los ataques cibernéticos siguen estando dentro de los más nombrados durante los años 2018 y 2019 (Global risks report, 2020) por lo que se hace indispensable desarrollar una política para protección de datos personales.

En el capítulo 26 del decreto reglamentario 1074 de 2015, se establece las reglamentaciones para la creación del registro nacional de base de datos y deja encargado de esta función a la Superintendencia de industria y comercio, con esto se logra poder centralizar la información de las bases de datos a nivel nacional y tener un responsable en el tratamiento.

Con estos antecedentes, es propio decir que el estado a través de sus instituciones ha buscado garantizar los derechos fundamentales establecidos en la constitución, por ende, es necesario que las personas hagan valer los deberes que a la luz de la ley de protección de datos personales ha establecido para tal fin, la evolución en los sistemas ha llevado a que los delitos informáticos aumenten drásticamente sin que la víctima y el delincuente estén cerca físicamente pues ahora los ciberdelincuentes pueden estar en otro lugar del planeta ingresar a una red extrae la información valiosa para la organización y se roba millones de datos sensibles que pueden llevar a la quiebra inmediata a una empresa.

Ley 1581 de 2012

Dentro de la estructura normativa de la Ley 1581 de 2012, el legislador desarrolló ocho principios rectores, los cuales fueron expuestos en el artículo cuarto de la mencionada ley. En estos se plantearon de manera específica los lineamientos y las bases para efectuar un correcto tratamiento de datos personales. Por lo tanto, los mismos serán eje central y guía práctica para

ejecutar de manera idónea una buena política de tratamiento de datos personales, pues a través de estos principios se plantean las bases de aplicación de la norma.

Así los definió el autor Remolina (2013) “aquellos postulados generales que, incluidos o no formalmente en el ordenamiento jurídico, sirven de base o de razón de ser de enunciados normativos particulares del derecho del debido tratamiento de datos personales” (p.177).

En relación al Principio de legalidad en materia de Tratamiento de datos: Este principio resulta ser el más importante en el tratamiento de datos personales, pues el mismo refiere que todo el proceso de recolección y circulación de datos debe hacerse de acuerdo a las normas vigentes para este proceso.

Es decir, los datos personales no podrán ser recolectados bajo modalidades fraudulentas o con engaños. Todo el proceso de tratamiento de datos debe encontrarse acorde a los lineamientos legales previstos para tal fin, ir en contravía de lo ya establecido haría de la recolección o el uso del dato una práctica ilícita.

Así, los datos sólo podrán ser recabados y tratados de buena fe, con estricto respeto por la Ley y los derechos de las personas y de conformidad a lo previsto en las presentes directrices. Es así, que dicho principio se encuentra directamente relacionado con todos los demás, pues su aplicación debe estar inmersa en todas las actividades que se tengan que desarrollar en el marco de protección de datos.

En relación al Principio de Finalidad: Este principio está ligado con el objetivo o la razón para la cual fue recolectado dicho dato. De ahí que los datos recolectados no pueden tener una destinación o uso contrario al autorizado. La Unión Europea en su Reglamento General de Datos Personales en su artículo 5° así ha definido este principio “Los datos personales será recogidos

con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (…)" (RGDP, art.5).

Luego, aquellos usuarios que recolecten datos personales deben tener en claro que el uso de los mismos debe tener un fin específico, ir en contravía de ello, demostraría una conducta ilegal, pues se sobrepasan los límites autorizados para su destinación. "Esto significa que no podrán solicitarse ni registrarse más datos que los estrictamente necesarios para llevar a cabo la finalidad de que se trate, aunque fuesen susceptibles de serlo para cumplir objetivos futuros" (Observatorio Iberoamericano de Protección de Datos, 2013).

Por lo tanto, este principio lo que "busca es evitar que se recolecten datos para hacer con ellos lo que sea y delimita los usos que el responsable, encargado o usuarios pueden dar a la información en comento" (Remolina, 2013, p.182).

Principio de Libertad: Este principio va directamente relacionado con el consentimiento del titular o dueño de la información. Tal y como se expone en el artículo 4° literal c) "El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular.

Así, los datos personales no pueden ser emanados o hechos públicos sin previa autorización, o en ausencia de mandato normativo o judicial que releve el consentimiento" (Ley 1581, 2012). Se tiene entonces que el principio de libertad en relación con la protección al derecho a la intimidad está directamente ligado a que "los datos personales de un individuo solo pueden ser revelados con su consentimiento expreso o tácito…" (Bautista, 2015, p. 31).

Es por ello, que el consentimiento del titular debe verse expreso en una autorización, documento que para efectos del tratamiento de datos personales juega un papel importante, pues a través de este, el titular otorga su permiso para que sus datos personales sean destinados para una labor en específico. Con ello lo que se busca es "legitimar el tratamiento de datos

personales" (Remolina, 2013, p.191). Por lo tanto, el consentimiento del titular debe ser libre de tal manera que éste pueda tener claridad sobre el uso y tratamiento que va a recibir sus datos.

Así lo expresó, el Parlamento Europeo en su reglamento: El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. (Reglamento Europeo, Considerando 32). Vale la pena aclarar entonces que la autorización debe ser expresa, clara y en la misma debe delimitarse la finalidad y la temporalidad del tratamiento de dichos datos.

En cuanto al Principio de Veracidad o Calidad: Este principio está directamente relacionado con la realidad y actualidad del titular. Es decir que la información debe ser real, exacta y actualizada. La imparcialidad de dicha información viola notoriamente el derecho de habeas data y buen nombre de los titulares, pues claramente todos aquellos datos incorrectos, incoherentes, o desactualizados pueden arrojar información que no corresponde al titular. "Los datos deberán mantenerse exactos, completos y puestos al día, respondiendo a la verdadera situación de la persona a la que se refieran" (Viega, 2010, p. 4).

En relación al Principio de transparencia: Interpretando el artículo 4° de la Ley 1581 de 2012 literal e, señala que en el tratamiento debe protegerse el derecho del titular a conseguir de la autoridad del tratamiento o del encargado, en toda situación y sin limitaciones, datos inherentes a la existencia de información que le competen (Ley 1581, 2012, art. 4). Se tiene entonces que la definición de este principio va directamente relacionada con el derecho que tiene todo titular de conocer sus datos personales.

Quiere ello decir entonces, que la persona tendrá acceso a toda la información relacionada con el tratamiento y la política de protección que actualmente se desarrolla y de la cual están siendo beneficiados sus datos personales. Se debe entonces, "garantizar al titular, cuando lo requiera y sin restricciones, el derecho a obtener información acerca de la existencia de datos que le conciernan por parte del responsable del tratamiento de sus datos". En ese sentido, en aras de dar aplicación y materializar el principio de transparencia, la Corte Constitucional señaló que el principio de transparencia debe entonces "permitir a cualquier ciudadano establecer con exactitud quiénes son los responsables y encargados del tratamiento de sus datos" (Rojas, 2014, p.7).

En cuanto al Principio de acceso y circulación restringida: Este principio se encuentra incorporado en el artículo 4 de la ley 1581 de 2012 literal f), el cual señala que el tratamiento se sujeta a las limitaciones que son secuela de la naturaleza de la información personal, de las reglamentaciones de la normativa y la Constitución. Consecuentemente, el tratamiento solamente podrá efectuarse por individuos autorizados por el Titular y/o por los sujetos previstos en la normativa; la información personal, excepto los datos públicos, no pueden ser aprovechables en Internet u otros medios de difusión o comunicación en masa, salvo que dicho acceso se pueda controlar en forma técnica para ofrecer un discernimiento restringido solamente a los Titulares o terceros que sean autorizados de acuerdo a la normativa **(**Ley 1581, 2012, art. 4°).

En ese orden de ideas, se observa que el legislador limitó el acceso y la circulación de dichos datos a todas aquellas personas autorizadas para tal fin. En efecto, el presente principio, busca generar controles de seguridad en lo que respecta al acceso de los datos. No sobra poner de presente, que estos datos no serán de naturaleza pública.

Así, quienes efectúen el tratamiento de datos personales tendrán que tener ciertas restricciones para ello, el acceso y tratamiento solo estará en cabeza de aquellos que se encuentren autorizados para tal fin (responsables - encargados). De lo contrario, no es correcto que se tenga acceso a los datos de manera deliberada.

Por otro lado, respecto a la circulación de dicha información, la misma también tendrá que verse limitada. Es decir que el envío o transferencia de dichos datos, también será condicionada. No puede entonces, convertirse en una red de tráfico de datos sin ejercer los respectivos controles y restricciones de seguridad. Por lo tanto, los datos serán suministrados única y exclusivamente a las personas autorizadas para ello, que, para el caso en particular, las mismas se encuentran definidas en la Ley 1581 de 2012 en su artículo 13. Luego entonces, suministrar datos personales de manera irresponsable a personas no autorizadas pone en riesgo la privacidad y la integridad de la persona.

En relación al Principio de Seguridad: Tal y como se ha explicado durante el trascurso del presente escrito, los datos personales son un activo de suma importancia. Luego entonces, el cúmulo de datos personales suministran información relevante que hacen parte de la órbita de la privacidad y la intimidad de una persona.

En razón a ello, y a la magnitud de información que los datos personales proporcionan, los mismos deben gozar de una protección especial en lo que respecta a su circulación, administración, manipulación y en general en lo que respecta al tratamiento de estos. Por lo tanto, los estándares de seguridad deben ser altísimos, y las políticas desarrolladas en materia de protección deben por tanto garantizar la calidad de la información.

Por lo tanto, este principio busca que se adopten las medidas de seguridad necesarias y efectivas en el proceso de tratamiento de datos personales. Todo ello en aras de mitigar el riesgo

en eventos como pérdidas de información, adulteración de la misma, desactualización en la información administrada, entre otros; riesgos que podrían poner en peligro la calidad de la información.

Por lo tanto, es deber de los sujetos intervinientes, controlar que la información administrada goce de total seguridad, para lo cual tendrán que implementar técnicas especializadas en seguridad informática, planes de contingencia, planes de identificación de riesgos y en general adoptar todas las estrategias posibles con las cuales se permita adoptar un plan completo de seguridad que permita tener total confiabilidad sobre los datos recolectados en el proceso de tratamiento de datos.

Así mismo, el Principio de Confidencialidad: Lo que busca este principio es conservar la discreción en la difusión de dicha información. Por lo tanto, aquellas personas que intervienen en el proceso de tratamiento de datos personales están en la obligación de guardar total confidencialidad en el suministro de la información manejada. Quiere ello decir, que las personas intervinientes, no podrán revelar o suministrar la información que es o ha sido de su conocimiento con ocasión a su actividad o a su gestión dentro del proceso de tratamiento.

Así lo manifestó, la Agencia Española de Protección de Datos en su artículo Estándares Internacionales sobre Protección de Datos Personales y Privacidad - Resolución de Madrid: “La persona responsable y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal deberán respetar la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el interesado o, en su caso, con la persona responsable” (Agencia Española de Protección de Datos, 2009).

Luego entonces, lo que se pretende con la adopción de dicho principio, es evitar poner en riesgo la información. Claramente el principio de confidencialidad se encuentra directamente

relacionado con el secreto profesional, pues quien ejerce una labor dentro del tratamiento de datos personales, no podrá divulgar la información que ha conocido con ocasión al ejercicio de sus funciones.

5.3. En relación a los estudios internacionales y locales recientes; se debe reseñar lo documentado por El Banco Mundial en su informe Supply Chain Security Guide (Donner y Cornelis, 2009), en donde identifica y categoriza los problemas de seguridad de datos en dos tipos: actos terroristas y actos criminales. Dentro de la primera categoría, se agrupan todas aquellas acciones terroristas que consideran el uso de medios de transporte (incluyendo el contenedor) como arma o dispositivo de contención de elementos explosivos, radioactivos o contaminantes.

En la segunda categoría, se agrupan los actos delictivos como el tráfico ilegal de bienes o personas, así como el robo de la carga o del vehículo. A medida que el tiempo ha pasado, ha sido posible evidenciar que el tratamiento de datos lo conformen diferentes ámbitos como lo son: información, recursos económicos y bienes, con una integración significativa entre los usuarios y los proveedores del servicio a lo largo del territorio.

Es por ello, que de esta manera la seguridad de los datos puede ser la más vulnerable a los diferentes riesgos, debido a los diferentes actores que intervienen en el proceso, y es así como se debe centrar en un análisis de la seguridad en todos los tramos en los que se mueva (aéreo, terrestre, marítimo), pues debe considerarse que la seguridad de los datos debe ser tan segura como lo es el eslabón más débil.

5.4. Así mismo, Argüello (2015) presentó una investigación titulada “Análisis de la seguridad de los datos en Madecentro Colombia SA”. Este trabajo tuvo como objetivo diseñar un sistema de gestión de datos e información y lograr así un mejoramiento en el proceso de la

seguridad de datos de la empresa, garantizar niveles óptimos de confiabilidad y veracidad en la información de la comercializadora.

Sobre este aspecto, el informe expuso inicialmente una descripción de los conceptos de gestión de información e indicadores de control, fundamentados en la clasificación de información según los diferentes tipos de datos y haciendo uso de material actualizado sobre el tema. Así, se planteó el estudio enmarcado en una investigación descriptiva con diseño de campo no experimental.

En resumen, el autor concluyó que existen fallas notorias en la seguridad de los subsistemas de información y seguridad por lo que se recomendó diseñar un sistema en dicha comercializadora y lograr así un mejoramiento en la gestión de datos; del mismo modo, el aporte que provee esta investigación es facilitar el desarrollo de un modelo ya que sirve como ejemplo el cual hace posible la ejecución de una investigación con categoría de trabajo de grado.

5.5. Del mismo modo, Pereira (2015) realizó una tesis cuyo objetivo general estuvo centrado en diseñar un modelo de referencia para el dimensionamiento de riesgos operacionales en el tratamiento de datos aeronáutica colombiana; para lo cual un modelo funcional de aplicación empresarial que permite dimensionar los riesgos implícitos en los procesos operacionales en la gestión de datos identificando y gerenciando los riesgos asociados en las operaciones empresariales, con el levantamiento de datos en la fuente e integrando los resultados obtenidos mediante procesos de conocimiento enmarcados en los conceptos de seguridad de información, de forma que se agregue valor a los procesos intraempresariales en la aeronáutica privada de Colombia.

Partiendo del estudio del funcionamiento de la gestión de datos, el resultado final de este estudio presenta un modelo aplicado para las Empresas del sector aeronáutico privado, donde se

puede detectar y administrar los riesgos en la seguridad e la información, así como unas recomendaciones alrededor de los procesos gerenciales y operativos que deben estar presentes en toda gestión de datos; constituyendo así un importante aporte para el estudio en curso.

5.6. Dentro de esta misma perspectiva, Celemín (2015) elaboró un artículo de investigación cuyo objetivo general fue el fortalecimiento de la logística militar como estrategia en su desarrollo ante el postconflicto en Colombia. Para eso, estudió la estructura de la logística militar en Colombia mediante un análisis documental que evidencia la importancia del tratamiento de datos en la misma como estrategia vital para poder llegar en el momento exacto con eficiencia y eficacia a los desplazados y/o víctimas de los grupos al margen de la ley.

Entre los resultados encontrados, se evidencia que la logística militar cuenta con equipamiento para apoyar las tropas en el campo de combate, pero no cuenta con un sistema de seguridad para el control del equipamiento adecuado para poder responder ante las situaciones que el postconflicto requiere de unas Fuerzas Militares en transformación. Así, la temática tiene relación con la investigación en curso ya que se toma como referencia la base teórica en donde se exponen los diferentes subsistemas de seguridad de información en el área militar.

5.7. Bajo esta perspectiva, Álvarez (2016) realizó una investigación cuyo propósito fue analizar el sistema de control de seguridad basado en el informe COSO para la gestión de la protección de datos en la policía de Bucaramanga. Este trabajo se basó en un estudio de campo, no experimental, con apoyo bibliográfico. Se tomó como población las cinco (5) personas que pertenecen a la división administrativo/contable, en este sentido la muestra quedó conformada por el total de la población.

Igualmente, como técnicas, se seleccionaron la entrevista, la encuesta y la observación directa, aplicando el cuestionario, previamente los datos fueron organizados y tabulados, para su

posterior tratamiento estadístico, de lo cual se detectó la necesidad de establecer un sistema de control de seguridad basado en el informe COSO para el área de inventario y producción de las fuerzas policiales, implementando los cinco elementos que componen el mismo y así poder detectar en el momento preciso cualquier irregularidad o error en la seguridad del inventario y los registros productivos. En analogía con la presente investigación, la relación está basada en que ambas indagan sobre lineamientos gerenciales de control que ayudan a salvaguardar la información de una organización.

5.8. Así mismo, Reynoso (2017), desarrolló un artículo de investigación cuya problemática se fundamentó en el análisis del tratamiento de datos dentro del ejército en Colombia ya que constituye una generación natural de principios competitivos en la empresa. Igual, la selección del caso de estudio según el autor se basó en dos criterios: (a) la accesibilidad a información y apertura de la organización y (b) la importancia de la entidad dentro del sector militar; siendo la administración castrense el área disciplinar en donde se llevó a cabo el estudio.

Consecuentemente, la metodología utilizada por Reynoso (2017) se basó en un paradigma cualitativo con enfoque documental y método descriptivo, con aplicación de tiempo tres (3) meses, en donde la técnica de recolección de información fue la revisión bibliográfica que permitió identificar la existencia de dimensiones y tipologías culturales elaboradas bajo un contexto en donde esperó conocer cómo era el tratamiento de la información en una organización castrense.

De acuerdo a los resultados encontrados, se dedujo la importancia del tratamiento de datos dentro de una empresa militar, en donde se aborda directamente las estrategias utilizadas para el mejoramiento del mismo en este tipo de organizaciones y la incidencia que tienen en la

prestación de los servicios militares, por lo cual constituyen un aporte importante a tomar en cuenta.

5.9. Siguiendo este orden de ideas, Ceballos (2017) apunta a un estudio "Diseño de un Sistema de Control de la información para Empresas Ferreteras del Departamento del Valle del Cauca". La citada investigación tuvo como objetivo general diseñar un sistema de control de gestión a las empresas ferreteras de dicho Departamento, por ello, se planteó una investigación descriptiva con diseño de campo no experimental; como instrumento de recolección de datos se aplicó un cuestionario con un total de diecisiete (17) preguntas que dieron respuesta a las interrogantes de la investigación y a las variables.

En efecto, los datos recolectados fueron plasmados mediante la construcción de tablas y gráficos utilizando estadística descriptiva. Una vez presentados y analizados los resultados, se observó la necesidad de profundizar los controles y adoptar procesos que ayuden a garantizar la custodia del material por ser éste el más extenso de los activos. Para esto, la gerencia necesita información oportuna y enfocar su atención sobre todas las áreas críticas identificadas. Así, el aporte para la presente investigación, es que ambas se enfocan en diseñar una mejora para evitar el riesgo del material en la entidad.

5.10. En esta misma perspectiva, Perea y Sánchez (2018), elaboraron un artículo cuyo objetivo principal fue el diseño de un modelo de transferencia de la metodología de referencia de operaciones para la gestión de la información de la Fuerza Aérea Colombiana. Así, la investigación se basó a través de cuatro fases metodológicas: análisis preliminar, diagnóstico situacional, desarrollo y cierre; las cuales permitieron diseñar una propuesta conforme a las necesidades de la organización para el desarrollo de las operaciones aéreas en todo el territorio nacional.

5.11. Seguidamente, se presenta el trabajo de Puello Rincón (2016), en donde realizó una investigación enfocada en la policía nacional; así, aborda de manera novedosa el análisis del nivel de protección presente en las herramientas creadas para proteger al uso indebido de datos personales por medio de nuevas tecnologías de la información y las comunicaciones para la policía de Colombia.

Después de la identificación del proyecto, la formulación del problema a tratar y los objetivos a cumplir, se expuso el marco referencial, compuesto en el espacio internacional por el antecedente teórico encontrado en investigaciones previas que han indagado acerca de los mecanismos de protección de datos personales, y en el espacio nacional, los estudios del nivel de protección que otorga la norma sustancial, en especial la ley 1266 de 2008, enfocada en la policía nacional.

De acuerdo a los resultados obtenidos, la propuesta de gestión para la Fuerza Aérea Colombiana, en su proceso de tratamiento de información, permitió establecer claramente cuáles son los procesos que se manejan a nivel del tratamiento de datos, así como establecer unos indicadores de gestión claros con unas mediciones que permita hacer seguimiento al desempeño en el control de la información.

Así mismo, la exploración de estudios previos permitió encontrar similitudes en diversos estudios que proponen también un modelo de protección de datos, e igualmente enriqueció el trabajo al señalarse diferencias, limitaciones y diferentes teorías de variados autores; mismos que serán de provecho a lo largo del desarrollo de los objetivos. En síntesis, el estudio señalado guarda relación con el propio ya que busca mediante el uso de técnicas y métodos reconocidos la optimización de la gestión de la información en la fuerza aérea.

Marco Referencial

Marco Teórico

Teorías Relacionadas a la Protección de Datos Personales

Actualmente no existe una uniformidad real en la descripción y definición del concepto de privacidad, debido a su carácter elusivo y multifacético que puede adaptarse a diferentes explicaciones. Privacidad es un término antiguo, pero recientemente codificado, reconocido por primera vez por los jueces estadounidenses Warren y Brandies, quienes, en un artículo publicado en la revista jurídica Harvard Law Review, identificaron este concepto con el "derecho a ser dejado en paz".

Antes de eso, la intimidad y la privacidad de datos no se percibían como conceptos que necesitaban ser protegidos: así como a partir de la Revolución Industrial nació el derecho a la libertad de expresión y asociación, el derecho al voto y muchos otros derechos civiles consecuencias de nuevas necesidades. de la sociedad que estaba cambiando, así nace también el derecho a la privacidad, cuando las personas comenzaron a sentir la necesidad de dividir la esfera de la vida privada de la pública (Moore, 2012).

El artículo se considera de suma importancia, ya que marcó un punto de inflexión para el reconocimiento de este nuevo derecho, que hasta entonces no tenía una definición precisa, sólo el derecho a la propiedad y a la vida fueron detallados y considerados durante mucho tiempo los pilares fundamentales de los estilos de vida de cada individuo. Era hora de un sentido más preciso de la privacidad de cualquier persona, con el fin de limitar la invasión, especialmente por parte del estado.

De la definición dada por Warren y Brandies se pasa a otra teoría, formulada en 1967 por Alan Westin, quien pensaba en la privacidad como control de la información (Moore, 2012), es

decir, como el poder de tener pleno control y gestión de toda la información relativa a la persona. Esta teoría ha encontrado muchos seguidores gracias a su carácter innovador; otros juristas como como Frederik Schauer y Richard Posner han identificado el derecho a la privacidad con la posibilidad de comprobar los hechos y la información relacionada con su propia vida (Kühn, 2016).

Ahora bien, a pesar de que muchos expertos han defendido el predominio de esta visión de la privacidad, con la evolución y expansión de Internet más allá del ámbito militar desde finales de los 90, estas teorías ya no eran viables de manera concreta porque ya no era posible tener control de la información cuando los datos pueden fluir a una velocidad impensable a través de medios que no existían antes.

Desde este mismo punto de vista, William Parent en 1983 buscó dar un tono un poco diferente a los autores anteriores. En su pensamiento, la privacidad de datos es vista como la condición en la cual la información personal no registrada no esté en posesión o sea conocida por otros (Decew, 2002). La información es relevante a los hechos, y por lo tanto corresponde a los individuos elegir revelar o no.

De esta manera, siempre se ha subrayado que la definición de privacidad de datos tiene un valor moral para personas que aprecian la libertad y la individualidad, pero existe un derecho moral a ello (Decew, 2002). Incluso Richard B. Posner, dio un pensamiento absolutamente en línea con el de Westin, afirmando que la privacidad es el control sobre cuándo y por quién las diferentes partes de nosotros mismos pueden ser "sentidas" por otros.

Del mismo modo, para Parker, la privacidad de información se traduce en una especie de control más marcado de la información personal; así, la privacidad de datos se traduce en una

especie de control aún más fuerte de la información personal, limitando el acceso a los extraños no solo a la información personal sino también al propio cuerpo (Moore, 2008).

Así mismo, algunos autores como R. Gavison y N. Morenham han definido la privacidad de datos como una inaccesibilidad, centrándose en la protección de la intimidad como condición de la soledad (Carolan, 2011). El punto débil de esta teoría es que no puede ser aplicada uniformemente a todas las situaciones y especialmente no toma cuenta de los diversos matices de la vida, ya que es una teoría que asume la privacidad total o su total ausencia, y para tenerla el único medio es el aislamiento, voluntario o forzado, en una ermita o en una isla desierta, eliminando así todas las interacciones sociales (Carolan, 2011).

Como argumenta Carolan (2011), la privacidad de datos es de hecho un concepto relacional más que solipsista, la vida social está a nuestro alrededor. y es difícil, casi imposible salir; está en la capacidad de cada individuo para mejorar la administración en esta área equilibrando lo que debe permanecer privado con lo que puede ser en el dominio publico.

Sobre esta perspectiva, otra característica nueva que se está introduciendo gracias al crecimiento de la web está subrayada por Decew (2002), quien dijo que mientras en el pasado las violaciones de la privacidad en Internet eran en su mayoría de carácter físico (seguimiento de correo, vigilancia, búsquedas), ahora se llevan a cabo mayoritariamente de manera indirecta y de manera oculta, donde la persona interesada no puede entender que está controlada (ataques cibernéticos, malware, recolección de big-data, cookies) .

De la misma manera, En 1960, William Prosser, creyendo que la definición de privacidad de Warren y Brandies era demasiado vaga, ha tratado de aclarar sistemáticamente esta nueva normativa, alegando que hay cuatro diferentes tipos de contenido en los intereses de privacidad (Prosser, 1960).

Consecuentemente, el autor ha tratado de definir estas cuatro áreas, que eran: intrusión en la soledad de una persona; declaraciones públicas de hechos privados embarazosos; tergiversar a otras personas públicamente; apropiación de la semejanza de otro en beneficio de otros. Así, el punto focal de la discusión de Prosser es que destaca que la definición de Warren y Brandies era demasiado limitada.

En el ámbito social, numerosos autores y juristas han salido en forma negativa sobre la privacidad de datos. Algunos científicos sociales han expresado definir la privacidad como una obsesión enfermiza de la sociedad liberal contemporánea (Schafer, 2002).

Así mismo, Paul Halmos creía que un exceso de privacidad podía encabezar una especie de alienación de sociedad, lo que él llama "desocialización" (Schafer, 2002). Todos aquellos que fueron críticos con el concepto de privacidad caen en la categoría que se llama "reduccionista" porque creen que la privacidad no existe como un concepto en sí mismo, sino que es más bien una derivación de otros derechos como el derecho a propiedad y que no vale la pena considerar la privacidad como una idea independiente (Decew, 2002).

En este sentido, una de las reduccionistas teóricas más importantes fue Judith J. Thompson, quien analizó los casos de violación de la privacidad, sostuvo que era posible encuadrarlos todos en el contexto de la violación de la propiedad privada (Decew, 2002). Thompson estaba firmemente convencida de su idea, tanto que utilizó palabras que no dejaban sombras en su forma de pensar, como definir la privacidad como un "interés parasitario" para enfatizar la naturaleza de la privacidad de datos como una derivación de otros derechos.

Analizando lo anterior, si bien es innegable que el derecho a la privacidad resulta del derecho más amplio a la propiedad de datos, no se puede aceptar esta teoría como demasiado vaga; un punto de vista en la línea del pensamiento de Judith Thompson, pero revisado en menor

grado es de Russell Brown, quien delinea un enfoque alternativo argumentando que la privacidad tiene valor, pero es un concepto demasiado confuso y engorroso para ser utilizado con eficacia. La crítica que se traslada a esta visión se refiere a la cuestión de si la exclusividad no logra proteger adecuadamente el pleno rango de intereses cubiertos por la privacidad (Carolan, 2011).

Por lo tanto, el concepto de privacidad de datos aún está en desarrollo y construcción, muchos autores solo han delineado algunos aspectos de este derecho tan amplio y vago a la vez; con reciente innovaciones tecnológicas, que han tenido lugar a una velocidad asombrosa, se observa aún más claramente lo que diferentes autores ya habían visto en el pasado reciente, es decir, que la privacidad es un concepto inútil, por lo que definitivamente se debe aceptar el hecho de que la sociedad moderna ha ido más allá de este derecho.

Gestión de la Seguridad

De acuerdo a la Ley 1581 de 2012; se trata de las actividades y prácticas sistemáticas y coordinadas por medio de las cuales una organización maneja de manera óptima sus riesgos y las amenazas e impactos potenciales asociados derivados de ellos Así, se busca como resultado o logro específico de seguridad requerido, cumplir con la política de gestión de seguridad, así como evitar la resistencia a actos intencionales, sin autorización, diseñados para causar perjuicio o daño.

Dato

Es un antecedente necesario para llegar al conocimiento exacto de algo o para producir las consecuencias legítimas de un hecho (Ley 1581 de 2012). La naturaleza de los datos resulta ser indispensable al momento de dar un correcto tratamiento, pues no todos los datos pueden ser tratados de la misma manera.

En ese sentido, lo manifestó Remolina (2013), en su artículo Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica "la protección de datos personales se amplía a cualquier naturaleza de información sobre la persona (privada, sensible, semiprivada y pública), lo cual implica que toda clase de dato personal debe ser tratado debidamente" (p.6). En ese sentido, se han efectuado diversas clasificaciones de los datos. Sin embargo, actualmente en Colombia de acuerdo a los parámetros legales previstos en la Ley 1266 de 2008, 1581 de 2012 y los preceptos constitucionales, se ha elaborado una clasificación general, en la que encontramos los Datos públicos, privados, semiprivados, sensibles.

Dato público. La Ley 1266 de 2012 lo define como el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos que están contenidos en herramientas públicas, sentencias de tipo judicial adecuadamente ejecutadas que no sean sometidas a reserva y los concernientes al estado civil de los individuos (Ley 1266, 2008, art.3 literal f).

Datos personales. La Ley 1581 de 2012 ha señalado que el Dato personal es "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables". (Ley 1581, 2012, art.3 literal c).

La Ley 1266 de 2012 define que es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente normativa se hace referencia a un dato, se presume que hace referencia a la utilización del individuo. Los datos personales pueden ser públicos, semiprivados o privados, (Ley 1266, 2008, art.3 literal e).

Ahora bien, según la comisión europea en su RGPD define el dato personal como cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal (RGPD, 2018).

Según la SIC, el dato personal es cualquier información que pueda ser relacionada con una persona. En España la RLOPD define un dato de carácter personal es cualquier información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables

Tratamiento de datos personales. Según Álvarez (2018), se dice que son operaciones y procedimientos técnicos de carácter automatizado o no automatizado que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, supresión, secciones o comunicaciones de datos, consultas, utilización, interconexiones y transferencias. Es decir, el tratamiento de los datos permite prácticamente todo. En Colombia, la Ley 1581 de 2012 ha señalado que el tratamiento es "Cualquier operación o grupo de actividades sobre datos del sujeto, tales como la recolección, acopio, utilización, circulación o eliminación (Ley 1581, 2012, art.3 literal g).

Datos sensibles. Están definidos como los datos que afectan la intimidad del titular de los datos personales ya que pueden revelar su origen racial étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos concernientes a la salud, a la vida sexual, y los datos biométricos (Ley 1581, 2012, titulo III art.5).

Dato semiprivado. La Ley 1266 de 2012 indica que Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo discernimiento o comprensión pueda involucrar

no solamente al titular sino a cierto conjunto de individuos o a la sociedad, como el elemento de información financiera y crediticia de procedimientos comerciales o de servicios inherente al Título IV de la normativa (Ley 1266, 2008, art.3 literal g).

Dato privado. La Ley 1266 de 2012 define Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular, (Ley 1266, 2008, art.3 literal h). Teniendo en cuenta que se ha evolucionado hoy en día a través de la necesidad de incursionar en la protección de datos personales en un mundo donde a partir de un click en un navegador se puede estar en contacto con alguien al otro lado del planeta, se hace indispensable poder analizar otros países que están a la vanguardia en temas de información y ciberseguridad para poder establecer dentro de una sana comparación el nivel en el que se encuentra el estado como máximo ente regulador en la sociedad.

Por tal motivo, se revisará contenido de los Estados Unidos, Europa, Centro América y Suramérica dentro de un mundo globalizado y liderado por las mayores potencias, es importante recordar que si puedes controlar la información se puede lograr desestabilizar un país, se puede buscar una persona perdida, se puede vender un artículo y un sin número de cosas más, en razón a lo anterior se debe verificar la información que reenviamos ya que puede ser información falsa o sensible y puede ayudar con un delito.

Defensa y Seguridad Integral

Según Guédez (1998), la defensa integral es el conjunto de sistemas, métodos, medidas y acciones de defensa, cualesquiera sean su naturaleza e intensidad, que en forma activa formule, coordine y ejecute el Estado con la participación de las instituciones públicas y privadas, y las personas naturales y jurídicas, nacionales o extranjeras, con el objeto de salvaguardar la

independencia, la libertad, la democracia, la soberanía, la integridad territorial y el desarrollo integral de la Nación.

Igualmente, desde la visión de Guédez (1998), la seguridad de la nación está fundamentada en el desarrollo integral, y es la condición, estado o situación que garantiza el goce y ejercicio de los derechos y garantías en los ámbitos económico, social, político, cultural, geográfico, ambiental y militar de los principios y valores constitucionales por la población, las instituciones y cada una de las personas que conforman el Estado y la sociedad, con proyección generacional, dentro de un sistema democrático, participativo y protagónico, libre de amenazas a su sobrevivencia, su soberanía y a la integridad de su territorio y demás espacios geográficos.

De acuerdo a lo anterior, en relación a los sistemas de seguridad y defensa integral militares, el direccionamiento organizacional básico está constituido por las normas y procedimientos de seguridad. No obstante, esas normas y procedimientos muchas veces no son no son actualizadas y en muchas ocasiones obstaculizan la labor administrativa de quienes trabajan en la organización militar; llevando esto a desarrollar la burocracia dentro de la misma.

Así, el direccionamiento organizacional en el contexto militar, se puede ubicar según Guédez (1998) como un estilo gerencial en el cual, quien ejerce sus funciones se ampara en la seguridad de una normativa estable e inflexible; es el estilo gerencial que precisa de la norma, los antecedentes, los controles, la consulta y la orden por escrito de sus superiores para tomar decisiones.

Factor Humano

Sobre este aspecto, se consideran: desempeño laboral y comunicación organizacional, los cuales se explican a continuación.

Desempeño Laboral. Se entiende por desempeño laboral el rendimiento laboral y la actuación que manifiesta el trabajador al efectuar las funciones y tareas principales que exige su cargo en el contexto laboral específico de actuación, lo cual permite demostrar su idoneidad. En este sentido, tanto la comunicación, como el manejo de conflicto y el ambiente laboral son variables importantes a tomar en cuenta en procura de lograr la eficacia del individuo en su puesto de trabajo.

Así, la comunicación es un valor agregado en las organizaciones, en donde es más importante la forma en que se transmite el mensaje que el contenido de ese mensaje. De acuerdo a Lyon et al. (2014), en la conducta asertiva en la organización primero se actúa y después se va hacia los sentimientos, ya que lo más importante es lograr la productividad y el logro de los objetivos organizacionales, diferenciándose así de la conducta a nivel familiar, en donde los sentimientos van de primero.

Comunicación organizacional. Es un mensaje, una noticia, una información, un significado cualquiera. Es un puente que permite a ese algo pasar de una persona a otra o de una organización a otra. En este sentido Chiavenato (2001) define: “Es la transmisión de una persona a otra, de una organización a otra, el fenómeno mediante el cual un emisor influye y aclara algo a un receptor, o el proceso mediante el cual se intercambia, se comprende y se comparte información entre dos o más personas, con la intención de influir en comportamiento” (p. 521). En síntesis, las organizaciones pueden llegar a tener un alto grado de calidad en sus comunicaciones mediante una rica mezcla de canales que faciliten las oportunidades para que la información circule tanto en Dirección ascendente como descendente u horizontal.

Sistemas de Seguridad y Factor Humano

La gestión en seguridad aérea en la Fuerza Aérea, está delineada bajo la Política Institucional número cinco (5), Principio número cuatro (4), Objetivo Institucional número 1 (uno), buscando fortalecer la Supervisión, Prevención de Accidentes, Administración de Riesgos Operacionales, Líneas de Investigación y Recuperación de Personal, a través de la optimización permanente de los procesos esenciales. El origen de la nueva aproximación para la Gestión en Seguridad Aérea es la comprensión del talento humano aplicado, que se ve convertido en productividad e innovación para la conservación de la capacidad operativa de la Fuerza.

Así mismo, la línea de investigación de accidentes ha reformado y reforzado el sistema de clasificación e informe nuevas formas de operación, que producen recomendaciones y operaciones de corrección para fortalecer el "PREVAC". Toda la dirección de Seguridad Aérea está encaminada en el Plan Estratégico Funcional, con diferentes visiones que conforman el mapa de estrategias en la siguiente manera: visión de efectos concentrada en la reducción de accidentes: igual, visualización de usuarios orientada a satisfacer las necesidades de seguridad de las áreas funcionales; visión de procesos orientada a la exploración, innovación y beneficio de prevención, investigación y recuperación de talento humano; perspectiva de crecimiento y aprendizaje organizacional encauzada a las competencias del personal especialista en Seguridad Aérea.

De la misma forma, entre los lineamientos de seguridad se prevé diseñar e implementar un sistema de defensa integrado, flexible y sostenible: la fuerza aérea seguirá comprometida en la salvaguarda de los intereses políticos, económicos y sociales de la nación y continuará el proceso de fortalecimiento de sus capacidades. Sin embargo, dada la naturaleza multidimensional de la seguridad internacional, se avanzará en el diseño e implementación de un

sistema disuasivo de defensa creíble, integrado, y operable también para cumplir con los propósitos de seguridad interna.

Por lo tanto, la fuerza aérea promoverá una estrategia de diplomacia para la seguridad mediante cooperación con base en experiencias exitosas y negociación de acuerdos para el desarrollo de estrategias coordinadas de seguridad; así como el implementar un programa de ciberseguridad y ciberdefensa.

Delitos Informáticos en Colombia

Resulta de gran importancia el tratamiento de datos los cuales terminan siendo el activo vital para cualquier institución hoy en día, a continuación se muestra en la tabla 1 la frecuencia de los delitos informáticos en Colombia, los cuales se han ido incrementando en más del doble cada año lo que demuestra que no estamos exentos de que nos pase, que sería de la Fuerza donde se filtre la información de los residentes de una Base, o de las personas que flotantes, esto en manos criminales podría generar extorsión mediante llamadas, terrorismo que afectarían la buena imagen.

Tabla 1

Frecuencia de delitos informáticos en Colombia

Delito	*2017*	*2018*	*2019*
– Artículo 269E: USO DE SOFTWARE MALICIOSO.	668	2199	1530
– Artículo 269F: VIOLACIÓN DE DATOS PERSONALES.	721	1173	625
– Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.	269	695	439

Nota. Información obtenida del sistema virtual de la Policía Nacional de Colombia (2020).

De acuerdo a la información obtenida del servicio de registro de ciberincidentes, disponible en el CAI virtual de la Policía Nacional de Colombia, se puede observar que en los dos últimos años y en lo corrido del año 2019, existe una tendencia al aumento de la realización de actividades delictivas relacionadas con el uso de las herramientas informáticas, es decir, de acuerdo a lo estipulado en la ley 1273 de 2009, en la cual se incluye en el Código Penal una serie de delitos informáticos, relacionado directamente con la protección de la información y de los datos, se evidencia que hay un crecimiento en la comisión de delitos informáticos en especial el delito del articulo 269E, uso de software malicioso, que refiere al uso de malware, ransomware, trojanos, entre otros; con el objetivo de dañar o evitar el uso de la información o de los datos de un particular.

Así, los delitos informáticos son más frecuentes de lo que se cree y demuestra que es pertinente, fortalecer las estrategias por parte de la institución en lo referente a la seguridad informática, puesto que, a pesar de que existe un documento CONPES 3701 y la Ley 1581 de 2012, es necesario incentivar y potencializar la capacitación y aplicación de políticas que permitan asesorar y proteger a los integrantes de la Fuerza y el personal visitante respecto al tratamiento de datos, se puede observar que el delito sustitución de portales web para apropiarse de información personal está aumentando progresivamente por lo que es necesario que se analice este tema y teniendo en cuenta el trabajo actual se puede afirmar que se debe enfocar esfuerzos en lograr mantener la calidad de la información contando con una ciberseguridad y una ciberdefensa bien establecidas que ayuden a mitigar los riesgos anteriormente mencionados.

Ahora bien, para poder garantizar los lineamientos dispuestos en la Ley 1581de 2012, se dieron unos parámetros a través de unos principios que se deben seguir en la protección de datos personales en Colombia los cuales se nombran para conocimiento y aplicación en el modelo: el

principio de legalidad el cual se relaciona en temas de tratamiento de datos, el principio de finalidad obedece a la finalidad legitima de acuerdo con la Constitución y la Ley constituyéndose de obligatoriedad por lo cual debe ser informada a titular de los datos, el principio de libertad nombra que solo se podrá tratar los datos siempre y cuando se tenga un consentimiento, previo, expreso e informado por el titular por lo que se ordena que no es posible obtener ni divulgar los datos sin previa autorización.

De tal forma, este principio es muy importante al momento de recolectar información en el control de acceso y será fundamental analizar dicho procedimiento, el principio de veracidad o calidad trata que la información recolectada debe ser veraz, completa, exacta, actualizada, comprobable y comprensible y prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan al error por lo que se puede deducir que no se debe informar de los datos personales al titular de manera incompleta o parcial pues puede modificar el contenido y el fin con el que se obtuvo.

Así mismo, el principio de transparencia habla acerca de garantizar en cualquier momento sin restricciones la información cuando el titular la solicite, el principio de acceso y circulación restringida nombra que no se podrá tener la información en internet u otros medios de divulgación o comunicación masiva, el principio de seguridad nombra unos requisitos técnicos humanas y administrativas para otorgar seguridad a la información con el fin de evitar adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento en este principio se debe enfatizar el modelo que se está desarrollando para obtener y brindar dicha seguridad a los datos personales obtenidos y autorizados por el titular.

Así, el principio de confidencialidad relaciona que las personas que intervengan en el tratamiento de datos personales deben garantizar la reserva de la información inclusive después

de finalizada su relación laboral que comprende el tratamiento es importante tener procedimientos internos dentro del control acceso que garanticen lo anteriormente enunciado con el fin de proteger la información siendo este el valor intangible más valioso de la institución.

Metodología de Gestión de Riesgo a Utilizar

Debido al mundo económico integrado que existe hoy en día se ha creado la necesidad de integrar metodologías y conceptos en todos los niveles de las diversas áreas administrativas y operativas con el fin de ser competitivos y responder a las nuevas exigencias empresariales, surge así un nuevo concepto de gestión donde se brinda una estructura común que agrupa los elementos del control interno para la gestión del riesgo en diferentes áreas, entre éstas la protección de los datos conocida como metodología COSO. Así, el Committee of Sponsoring Organizations of The Treadway Commission (COSO); es una iniciativa de 5 dimensiones para la gestión del riesgo dentro de las organizaciones, que puede ser aplicado a la seguridad de los datos y que se complementa con los postulados principales de la Ley 1581 de 2012.

De esta forma, según la metodología COSO, existen indicadores que inciden en la gestión administrativa y que deben ser tomadas en cuenta por toda organización según Mantilla (2013), de acuerdo a las características administrativas, operacionales y de tamaño de dichas instituciones; los componentes son: Ambiente de Control, Evaluación de Riesgo, Actividades de Supervisión, Información y Comunicación, Monitoreo**.**

Ambiente de Control. De acuerdo a Mantilla (2013), se refiere a la actitud y compromiso los altos mandos para establecer una atmósfera propicia para la implantación y ejecución de las operaciones de la organización en forma controlada. Es importante destacar que, si la alta Dirección considera que el control es importante, el resto de las personas que

conforman la organización lo sentirán y responderán acatando responsable y conscientemente las políticas, normas y procedimientos establecidos.

En esta perspectiva, un ambiente de control fuerte en el tratamiento de datos en el ámbito militar se puede reflejar en la existencia de sistemas de comunicación de políticas, normas y procedimientos formalizados y de políticas de manejo de personal para el talento humano involucrado en la protección de los datos, disposición del alto mando para disponer de sistemas de información confiables y participación de la Dirección en la elaboración de las estrategias relacionadas con la seguridad en la gestión de datos.

Evaluación del Riesgo. Los riesgos afectan la marcha de las organizaciones. Su nivel de detección e impacto es variable. Por ello, según la visión de Mantilla (2013), su evaluación muchas veces excede el ámbito de gestión de la información. Este componente implica realizar un diagnóstico y análisis del ámbito interno y externo de una organización, que sirva de base para el proceso de toma de decisiones.

De tal forma, algunos factores que pueden ocasionar la aparición de riesgos son; cambios en el ambiente operativo: cuando se incorporan nuevos procedimientos para realizar las actividades administrativas; personal nuevo: el personal nuevo puede tener diferentes enfoques o entendimiento de la gestión de la protección de datos.

Igualmente, están las nuevas tecnologías: requiere readaptación del personal e implementación de nuevos procedimientos, lo que puede traer consigo el incumplimiento o mala interpretación de alguna norma o procedimiento en el trabajo. Reestructuras Orgánicas: pueden estar acompañadas por reducciones de personal y cambios en la supervisión y segregación de funciones que pueden cambiar el riesgo relacionado con la gestión de la seguridad de los datos.

Actividades de Supervisión. Las actividades de supervisión de acuerdo a Mantilla (2013), son las políticas, normas y procedimientos que ayudan a asegurar que se tomen las acciones necesarias para el logro de los objetivos organizacionales. Algunas de ellas se describen a continuación. En primer lugar, la asignación de responsabilidades: se refiere a que las personas que conforman la organización sepan a quienes y en qué momento deben rendir cuentas de su labor y a quienes pedirles cuenta de su cumplimiento. Separación adecuada de funciones: esto significa, asignar a diferentes personas las responsabilidades y mantener la custodia de la protección de los datos con el propósito de reducir la oportunidad para que alguien pueda perpetrar y esconder errores o irregularidades en el cumplimiento de sus deberes.

De la misma forma, controles físicos: esta actividad abarca la seguridad física de los datos, esto incluye: su salvaguarda física y digital, como instalaciones aseguradas sobre el acceso a los registros (hardware); autorización para el acceso a los programas de computación y archivos de datos (software).

Información y Comunicación. Este componente está relacionado según la visión de Mantilla (2013) al flujo de comunicación que se da entre los diferentes niveles de la organización. Esta comunicación se da por medio de la información que luego se convertirá en conocimiento por el personal. La información pertinente permite una adecuada gestión de la protección de los datos.

Monitoreo. Es el proceso que de acuerdo a Mantilla (2013) consiste básicamente en cómo se valora la calidad del desempeño del personal en el tiempo. Es realizada por medio de actividades tales como: evaluaciones separadas o combinación de las dos. El monitoreo incluye actividades regulares de administración y supervisión y tras acciones personales realizadas en el cumplimiento de sus obligaciones.

Marco Conceptual

Modelo de Información

Entendido como los lineamientos y protocolos que deben seguirse para asegurar los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, así como de saber qué datos están siendo tanto retenidos como usados y de corregir las inexactitudes.

Tipos de Modelos de Información

Relacional. Aunque tiene un enfoque "más antiguo", el modelo de base de datos más común que todavía se usa en la actualidad es el relacional, que almacena los datos en registros de formato fijo y organiza los datos en tablas con filas y columnas. El tipo más básico de modelo de datos tiene dos elementos: medidas y dimensiones. Las medidas son valores numéricos, como cantidades e ingresos, que se utilizan en cálculos matemáticos como la suma o el promedio. Las dimensiones pueden ser de texto o numéricas (Maki, 2005).

Dimensional. Menos rígido y estructurado, el enfoque dimensional favorece una estructura de datos contextuales que está más relacionada con el uso o contexto comercial. Esta estructura de base de datos está optimizada para consultas en línea y almacenamiento de datos. Los elementos de datos críticos, como la cantidad de una transacción, por ejemplo, se denominan "hechos" y van acompañados de información de referencia denominada "dimensiones", ya sea la identificación del producto, el precio unitario o la fecha de la transacción. Una tabla de hechos es una tabla principal en un modelo dimensional (Maki, 2005).

Igualmente, Entity-Rich (ER): un modelo ER representa una estructura de datos comerciales en forma gráfica que contiene cuadros de varias formas para representar actividades, funciones o "entidades" y líneas para representar asociaciones, dependencias o "relaciones". Luego, el modelo ER se utiliza para crear una base de datos relacional en la que cada fila

representa una entidad y los campos de esa fila contienen atributos. Como en todas las bases de datos relacionales, los elementos de datos "clave" se utilizan para vincular las tablas (Maki, 2005).

Control de Acceso y Procedimientos para Asegurar la Integridad de la Información y Elementos que Debe Tener el Modelo de Protección de Datos

El control de acceso es una técnica de seguridad que regula quién o qué puede ver o utilizar recursos en un entorno informático. Es un concepto fundamental en seguridad que minimiza el riesgo para la empresa u organización. Hay dos tipos de control de acceso: físico y lógico. El control de acceso físico limita el acceso a campus, edificios, salas y activos físicos de TI. El control de acceso lógico limita las conexiones a las redes informáticas, los archivos del sistema y los datos (Garriga, 2004).

Para proteger una instalación, las organizaciones utilizan sistemas de control de acceso electrónico que se basan en las credenciales de los usuarios, lectores de tarjetas de acceso, auditorías e informes para rastrear el acceso de los empleados a ubicaciones comerciales restringidas y áreas de propiedad, como centros de datos. Algunos de estos sistemas incorporan paneles de control de acceso para restringir la entrada a habitaciones y edificios, así como alarmas y capacidades de bloqueo para evitar operaciones o accesos no autorizados.

Los sistemas de control de acceso realizan la autenticación de identificación y la autorización de usuarios y entidades mediante la evaluación de las credenciales de inicio de sesión requeridas que pueden incluir contraseñas, números de identificación personal (PIN), escaneos biométricos, tokens de seguridad u otros factores de autenticación. La autenticación multifactor (MFA) que requiere dos o más factores de autenticación, suele ser una parte

importante de una defensa en capas para proteger los sistemas de control de acceso (Garriga, 2004).

El objetivo del control de acceso es minimizar el riesgo de seguridad del acceso no autorizado a los sistemas físicos y lógicos. El control de acceso es un componente fundamental de los programas de cumplimiento de seguridad que garantiza que la tecnología de seguridad y las políticas de control de acceso estén implementadas para proteger la información confidencial, como los datos de los usuarios. La mayoría de las organizaciones cuentan con infraestructura y procedimientos que limitan el acceso a redes, sistemas informáticos, aplicaciones, archivos y datos confidenciales, como información de identificación personal (PII) y propiedad intelectual.

Los sistemas de control de acceso son complejos y pueden ser difíciles de administrar en entornos de TI dinámicos que involucran sistemas locales y servicios en la nube. Después de algunas infracciones de alto perfil, los proveedores de tecnología han pasado de los sistemas de inicio de sesión único (SSO) a la gestión de acceso unificado, que ofrece controles de acceso para entornos locales y en la nube (Garriga, 2004).

Autoridad de Control Interesada

Es aquel responsable que incide en la utilización de datos personales originado por: a) El responsable o autoridad de la utilización está enfocada en el territorio del estado miembro de esa responsabilidad de control. b) Los participantes o interesados que residen en el estado miembro de esa responsabilidad de control se ven básicamente impactados o es posible que se vean bastante impactados por el tratamiento.

Datos Personales

Todos los datos sobre un individuo reconocido (el involucrado); se considerará individuo identificable a toda persona cuya tipificación pueda establecerse, directa o indirectamente,

mediante un identificador que pueden ser: el número de identificación, elementos de ubicación, un denominador en línea o distintos factores que determinan la denominación física, fisiológica, genética, psíquica, económica, cultural o social de dicho individuo.

Elaboración de Perfiles

Cualquier manera de forma de llevar en forma automatizada la información personal que consiste en usar los datos de la persona para valorar aspectos específicos de un individuo, concretamente para revisar o interpretar elementos concernientes al provecho en la labor, contexto económico, salud, particularidades personales, beneficios, fiabilidad, comportamiento, localización o movimientos de dicho individuo.

Fondo de Seguridad. El concepto está estipulado en la Ley 399 de 1997 como una cuenta especial sin personería jurídica, cuyo objetivo es financiar gastos destinados a fortalecer la seguridad, por lo que se constituye en una herramienta vital dado que su alimentación se da por el 5% de los contratos de obra.

Fuerza Pública. Según las Constitución Política de Colombia, la fuerza pública, está constituida exclusivamente el Ejército Nacional, Armada Nacional y la Fuerza Aérea, establecidas para la defensa de la soberanía, la independencia, la integridad, la integridad del territorio nacional y del orden constitucional.

Normas Corporativas Vinculantes. Los lineamientos de protección de datos personales obtenidas por una autoridad de la utilización señalada en la localidad de un estado para transferencias o un grupo de transferencias de datos personales a un autorizado en uno o más países terceros, dentro de un conjunto empresarial o una unión de compañías relacionadas a una actividad económica similar.

Orden Público. Se define como el orden externo de la calle en cuanto a condición elemental para el libre y pacifico ejercicio de los derechos.

Operación de Seguridad y Defensa. Según la Directriz área funcional para la ejecución de seguridad y defensa, Fuerza Aérea Colombiana, 2018, es el conjunto de acciones encaminadas a mantener la vanguardia y la iniciativa en medidas de prevención de seguridad. Es así, la ejecución de todas las actividades que conllevan a proteger los activos que se tienen en las bases aéreas, se vigilan a través de estos medios.

Responsable del Tratamiento o Responsable. El individuo o persona jurídica, autoridad pública, servicio u otro órgano que, solo o junto con otros, establezca los fines y formas del tratamiento; si el derecho de la Unión o de los estados miembros estipula los medios y fines del tratamiento, el autorizado del tratamiento o los criterios específicos para su nombramiento podrá determinarlos el derecho de la Unión o de los estados miembros.

Tratamiento. Se refiere a actividades como la recopilación, el almacenamiento, el uso, la transferencia y la divulgación de datos personales. Todas las actividades que involucren datos personales, desde la planificación del procesamiento hasta la eliminación de datos, constituyen procesamiento de datos de este tipo. Así, todos los datos relativos a una persona identificada o identificable son datos de carácter personal. La información como nombres, números de teléfono, datos de ubicación e información sobre las enfermedades congénitas de los abuelos del individuo son datos personales.

Violación de la Seguridad de los Datos Personales. Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Marco Contextual

Al respecto, en el Comando Aéreo de Mantenimiento, en el grupo de Seguridad y Defensa de Bases Aéreas N° 95 actualmente trabajan 13 Oficiales, 47 Suboficiales y 262 Soldados, responsables de velar por la Seguridad y la defensa de la Unidad, datos recabados de acuerdo con el Manual Oficial del Comando Aéreo de Mantenimiento de la Especialidad de Seguridad y Defensa de Bases Aéreas de la Fuerza Aérea de Colombia (2020).

En este sentido, la Fuerza Aérea Colombiana dentro de sus especialidades cuenta con la Especialidad de Seguridad y Defensa de Bases Aéreas que está constituida por talento humano capacitado y entrenado para prevenir, disuadir y reaccionar ante eventos que amenacen la integridad del personal, las aeronaves y la infraestructura del poder aeroespacial del país. Así, posee la capacidad para enfrentar la amenaza, mediante la estandarización operacional, infraestructura, equipos y armamento que brinda la sostenibilidad en el desarrollo de operaciones aéreas y cumplimiento de los fines del estado.

Así mismo, deben mantener y garantizar la seguridad de las Unidades Militares Aéreas por medio del desarrollo de operaciones de seguridad y control, utilizando entre otros, sistemas electrónicos para la seguridad, equipos de reacción, productos de seguridad, análisis de riesgo; así desarrollan operaciones especiales de apoyo a las operaciones aéreas, en donde resalta la importancia de contar con un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento, mediante un análisis documental en el interior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN.

Igualmente, la Fuerza Aérea Colombiana emplea un sin número de campañas y actividades encaminadas a brindar bienestar al personal de Oficiales, Suboficiales y Soldados, lo

anterior con el fin de que todo este personal que allí labora se encuentre motivado y presto a desarrollar las diferentes actividades. De igual modo, los tiempos son cambiantes y surgen nuevas tendencias de administración de personal y de cómo a este personal se le pueden generar estrategias o mecanismos para que sean eficientes en lo que hacen y lo más importante que lo hagan bien y oportunamente.

Marco Normativo

En el marco legal se presentan las leyes y normas que rigen la protección de datos en Colombia. En primer lugar, la Constitución Política de Colombia en el Artículo 216 indica que La fuerza pública está conformada de manera exclusiva por las Fuerzas Militares y la Policía Nacional. Así, los ciudadanos de Colombia deben tomar las armas cuando las eventualidades de tipo público lo requieran para ejercer defensa inherente a la independencia del país y sus instituciones públicas. La normativa establecerá las circunstancias que en cualquier momento exoneren del servicio militar y los privilegios por la prestación de dicho servicio (Const., 1991, art. 216).

Así, interpretando a la Constitución Política de Colombia en el Artículo 217, la Nación dispondrá para su defensa Fuerzas militares indelebles formadas por el Ejército, la Armada y la Fuerza Aérea. La función de las Fuerzas Militares será primordialmente la defensa de la soberanía, la independencia, la integridad de la República y del orden bajo la Constitución. Así, el Estatuto establecerá el sistema de reemplazos en las Fuerzas Militares, así también los ascensos, derechos y responsabilidades de sus integrantes y el régimen de carrera, prestaciones y de disciplina, que les es oportuno (Const. 1991, art. 217).

Igualmente, el Código de Comercio en el Articulo 1787 “Por razones de seguridad aérea la autoridad competente podrá realizar las verificaciones que sean necesarias en los viajeros, tripulaciones, aeronaves y cosas transportadas”. (Código de comercio, 1971, art 1787).

Cabe resaltar, que en el Plan Estratégico del Comando Aéreo de Mantenimiento el Grupo de Seguridad y Defensa de Bases Aéreas de la Fuerza Aérea de Colombia (2019), se destaca la necesidad que la Fuerza Aérea Colombiana, y específicamente el Comando Aéreo de Mantenimiento debe realizar el diseño de estrategias administrativas que mejoren el control en referencia a la Seguridad desde cada uno de los procesos que se desarrollan a través de la gestión a corto, mediano y largo plazo, ya que así se pueden reducir los índices de robo o vulneraciones, reflejando la transparencia en los trámites de contratación o compra de bienes y servicios para las operaciones logísticas del CAMAN.

Así también, la Fuerza Aérea, cuenta con leyes que si bien no orientan el tema de familia constituyen un marco acerca de los lineamentos y disposiciones legales que rigen a los uniformados, y que se detallan de forma cronológica a continuación.

Decreto 1797 de 2000: Reglamento de Régimen Disciplinario para las Fuerzas Militares

Art 14: Las disposiciones de este reglamento se aplican a las y los oficiales, suboficiales y soldados en servicio activo, así como los prisioneros de guerra.

Decreto 1799 de 2000

Por el cual se dictan las normas sobre evaluación y clasificación para el personal de Oficiales y Suboficiales de las Fuerzas Militare y se establecen otras disposiciones. Art. 1: A través del cual se determinan "las normas, criterios, técnicas y procedimientos generales para la evaluación y clasificación de Oficiales y Suboficiales al servicio de las Fuerzas Militares, con excepción de los oficiales generales y de insignia".

Manual de Estado Mayor Fuerza Aérea- Manual FAC 3-05. Tercera Edición

Art.1: La finalidad es constituirse como un documento de consulta del comandante y del personal que se desempeña en los procesos de toma de decisiones y en las funciones propias del planteamiento y la solución de problemas de la Fuerza Aérea.

Decreto 317 de 2005

Por el cual se dictan normas para la adjudicación, uso y mantenimiento de alojamiento militar de la Fuerza Aérea Colombiana.

Decreto No. 1428 de 2007

Por el cual se cumplían las normas de Decreto Ley 2000, Por el cual se modifica el decreto que regula las normas de carrera del personal de Oficiales y Suboficiales de las Fuerzas militares. Art. 1: Las fuerzas Militares de la Republica de Colombia son las organizaciones destinadas a la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional. Están constituidas por el Ejército, la Armada y la Fuerza Aérea.

Ley 1266 es del 2008 en la Protección de los Datos Personales

La Ley Estatutaria 1266 de 2008 (Ley 1266) regula el tratamiento de datos financieros, registros crediticios e información comercial recabada en Colombia o en el extranjero. La citada normativa define términos generales sobre habeas data y establece tanto bases como principios de procesamiento de datos, derechos de los interesados, obligaciones del responsable del tratamiento y normas específicas de los datos financieros.

De tal forma, la Ley 1266 establece las normas y condiciones aplicables a fuentes de datos para compartir información con operadores de datos y para que dicho operador gestione y comparta la información con los usuarios. Sin perjuicio de ello, la ley privilegia el tratamiento

con fines de gestión de información financiera, crediticia, comercial y de servicios, considerando que esto beneficia al sector financiero y crediticio como una actividad de interés público.

Ley 1581 de 2012

Los datos personales en Colombia revisten gran importancia, pues estos resultan ser un componente significativo para la identificación de una persona. Así lo ha sostenido la Superintendencia de Industria y Comercio en su Guía Sobre la Protección de datos personales "Cuando se habla de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. En esa medida, ante la necesidad de un tratamiento especial de los datos personales, nace en Colombia la Ley 1581 de 2012, en la cual se incluyó todas las disposiciones generales en materia de protección de datos personales y se emitieron lineamientos respecto a la recolección, manejo y circulación de todos los datos que fueran incluidos en las diferentes bases de datos.

Así las cosas, teniendo en cuenta el gran universo que abarca los datos personales, resulta importante analizar más a fondo cada uno de los parámetros establecidos en materia de protección de datos, pues ante la constante globalización respecto a las nuevas tecnologías, los datos personales se convierten en un activo de cada persona y, por lo tanto, merecen una política integral sobre el uso y la destinación de los mismos. Esto con el fin de atender al principio de responsabilidad demostrada.

De tal forma, conocer los fundamentos de la Ley Estatutaria 1581 de 2012 y los lineamientos que esta propone respecto a las condiciones de seguridad a las cuales deben sujetarse los datos personales, permite que, como dueños de la información, cada persona haga respetar el buen uso y la correcta destinación de sus datos y de esta manera prevenir los daños derivados de un uso inadecuado de los datos personales.

Sin embargo, si bien la norma desarrolla y abarca en su totalidad todos los lineamientos necesarios, que deben ser tenidos en cuenta para crear políticas efectivas en materia de tratamiento de datos personales, con el fin de prevenir conductas inadecuadas en este proceso, la misma es carente frente a la regulación relacionada con las responsabilidades por los daños y/o perjuicios que puede acarrear un tratamiento de datos deficiente.

Así pues, la norma destinó un Título para regular todo lo relacionado a los mecanismos de vigilancia y sanción, en donde, se enuncian los tipos de sanciones frente al incumplimiento de los deberes por parte de los Responsables o Encargados del tratamiento de datos. Es decir, se estructura un modelo sancionatorio. No obstante, frente al directo afectado, que para el caso en particular resultan ser los titulares de la información, no se reguló un resarcimiento frente a los posibles daños a los que se vieron inmersos estos, aun cuando la norma protege de manera especial al dueño de dicho activo. Es decir, se evidencia un vacío normativo, pues la Ley Estatutaria no regula de manera directa los aspectos relacionados a la reparación del perjuicio causado.

El ordenamiento, a través de la promulgación de dicha norma estructuró políticas efectivas en pro de velar por el respeto y la protección a los datos personales, empero dejó de lado regular un tema relevante como lo es la Responsabilidad Civil y la reparación de daños. Un cambio relevante que ha implementado el Derecho Privado en estos temas (Woolcot et al., 2018).

Con todo ello, vale la pena resaltar los avances que se lograron con la expedición de dicha norma, pues la misma, obligó que todo el tratamiento de datos personales estuviera directamente relacionado con la protección de garantías constitucionales. Así mismo, obligó a todas las empresas que recolectan datos y en general para todos aquellos sujetos que administran

estas bases, estructurar políticas de seguridad que se encuentren acorde a los lineamientos legales y evite de esta manera el riesgo que puede generar para los derechos y libertades de una persona el manejo inadecuado de los datos.

Ley 1377 de 2013 y Normativas Posteriores

El Decreto 1377 de 2013 (Decreto 1377), es una pieza de regulación secundaria relacionada con la Ley 1581 de 2012 que establece requisitos para las bases de datos personales y domésticas relacionadas a la autorización del uso y recolección de datos personales, limitaciones al procesamiento de datos, procesamiento de bases de datos y avisos de privacidad, entre otros. Este Decreto también requiere que los controladores y procesadores adopten una política de privacidad y un aviso de privacidad. Luego, surgen el Decreto 886 de 2014 (Decreto 886) y Decreto 090 de 2018 (Decreto 090) emitido por el Ministerio de Comercio, Industria y Turismo, así como la Resolución 090 de2 018 emitida por la Superintendencia de Industria y Comercio, que regula el Registro Nacional de Bases de Datos y fija plazos para el registro de las bases de datos existentes en Colombia.

Análisis Jurisprudencial de los Cambios Sucedidos en la Protección de los Datos, Principalmente a Partir de la Puesta en Vigencia de la Ley 1581 de 2012

En los últimos años, las sentencias judiciales han abordado otros temas, como el tratamiento de datos personales en las redes sociales. Por ejemplo, la sentencia T-260 de 2012 decidió el caso de un padre que creó una cuenta de Facebook para su hija de 4 años. En este caso la Corte declaró que se había vulnerado el principio de libertad en el tratamiento de los datos personales. Por tanto, dado que la menor no tenía conocimiento de la creación de la cuenta en Facebook, el Juzgado consideró que se había vulnerado su derecho a la protección de datos, y ordenó a su padre que eliminara la cuenta (Puello Rincón, 2016).

Posteriormente, el Tribunal revisó el caso de una acreedora que decidió denunciar públicamente a su deudor moroso en Facebook. En sentencia T-050 de 2016 la Corte decidió que el mensaje publicado en Facebook vulneró el derecho a la privacidad de la deudora morosa, no solo porque expuso parte de sus datos personales, sino también porque la deudora no dio autorización para que dicha información fuera revelada. Si bien el derecho que finalmente se protegió en esta sentencia fue el derecho a la intimidad, el razonamiento del Tribunal tuvo especialmente en cuenta el derecho a la protección de datos del deudor implicado (Puello Rincón 2016).

De tal manera, la posición de la Corte no ha sido tan clara en cuanto a los datos personales difundidos por los medios de comunicación. En las sentencias que se han adoptado recientemente sobre datos personales publicados en medios de comunicación, la Corte ha abordado el problema como un conflicto entre el derecho a la libertad de expresión y acceso a la información, por un lado, y el derecho al honor y al buen nombre. de la persona involucrada, por otro lado. Por tanto, no ha mencionado el derecho de hábeas data, ni ha declarado que el derecho de hábeas data no es aplicable al caso, pues la discusión se centra en la información periodística difundida por los medios de comunicación en ejercicio de la libertad de expresión, y no en información recabada en bases de datos (T-040 de 2013).

En relación con la labor de la autoridad de protección de datos, en Colombia, el Ministerio Público es la autoridad nacional encargada de controlar el correcto manejo de las bases de datos públicas. Cuando se trata de bases de datos privadas, la Superintendencia de Industria y Comercio (Superintendencia de Industria y Comercio, 'SIC') es la autoridad colombiana de protección de datos (Reynoso, 2017).

Respecto a esto último, hay tres pronunciamientos que vale la pena mencionar. El 24 de noviembre de 2014, la SIC publicó un concepto legal que establece que el tratamiento de datos personales en las redes sociales no se encuentra dentro del alcance de la Ley 1581 de 2012 (régimen jurídico general aplicable al tratamiento de datos personales), ya que en estos casos la recolección, uso, circulación, almacenamiento o supresión de datos personales no se realiza dentro del territorio colombiano (ya que las redes sociales están domiciliadas en el extranjero). No obstante, el 3 de marzo de 2016, la SIC revisó su posición, argumentando que el tratamiento de datos personales se realiza en territorio colombiano no sólo cuando el recolector de datos tiene su domicilio en Colombia, sino también cuando para llevar a cabo la recolección, uso, circulación o almacenamiento de los datos personales utiliza "medios que se encuentren en el territorio colombiano (Reynoso, 2017)

Finalmente, y en ejercicio de su obligación legal de garantizar la adecuada protección de nuestros datos en la transferencia internacional de información (artículos 21 y 26 de la Ley 1581 de 2012), la SIC emitió la Circular Externa 005 del 10 de agosto de 2017, mediante la cual definió los estándares para la transferencia internacional de datos. La Circular establece una lista de países que Colombia considera que tienen un nivel adecuado de protección de datos, entre los que se encuentran los países de la Unión Europea (que han sido aprobados como adecuados por la Comisión Europea), México, República de Corea, Costa Rica, Serbia, Perú, Noruega, Islandia y Estados Unidos.

Sin embargo, la SIC no explica por qué estos países se consideran adecuados y, sobre todo, cómo justifica la inclusión de Estados Unidos, que ha sido criticado por Human Rights Watch por no ofrecer a los extranjeros las mismas garantías que tienen sus nacionales (Reynoso, 2017). Además, no define cómo se mantendrá la adecuación de estos países (ya que las leyes

cambian con el tiempo), ni cómo se evaluará el nivel de protección de otros países en el futuro. Por último, y contrariamente al modelo europeo, la Circular no prevé un procedimiento para impugnar las decisiones de “adecuación de la protección de datos” (Reynoso, 2017).

En relación a los ejemplos de violaciones de datos; en 2014 se conoció que una red de individuos logró acceder ilegalmente a la base de datos que maneja la Unidad para la Atención y Reparación Integral a las Víctimas. Se informó que estas personas lograron acceder a la base de datos utilizando códigos de autorización que se les habían filtrado. Estos datos se vendían para permitir que personas sin escrúpulos se hicieran pasar por víctimas reales, acelerar el pago de indemnizaciones a determinados demandantes o conocer los datos personales de los denunciantes, entre otros delitos (Villalba, 2018).

Igualmente, el 16 de febrero de 2016, la periodista Vicky Dávila, directora de la emisora de radio "La Fm", divulgó una grabación en la que aparece un viceministro colombiano manteniendo una conversación de carácter sexual con un policía. Según el periodista, quien alegó haber sido intervenido por la Policía, esta grabación forma parte de los registros que evidenciarían la relación del viceministro con una red de prostitución que opera dentro de la Policía. Este escándalo terminó tanto en la renuncia del viceministro como en el despido del periodista (Villalba, 2018). Del mismo modo, el 3 de abril de 2016 se filtraron 11,5 millones de documentos de la firma de abogados panameña Mossack Fonseca & Co., que detallan información financiera de más de 214.488 entidades off-shore, exponiendo a cientos de colombianos (Villalba, 2018).

Metodología

Diseño de Estudio

Este estudio fue elaborado bajo el diseño de una investigación de campo debido a que se tomaron datos provenientes de la realidad. Al respecto, dicha actividad consistió en la recolección de información concerniente a elementos de protección de datos personales relacionados al control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento. Consecuentemente, los datos fueron recogidos directamente del sitio en donde ocurrieron los hechos, en este caso la sede física del Comando Aéreo de Mantenimiento en el Grupo de Seguridad y Defensa de Bases Aéreas y más específicamente en el control de acceso a la Unidad.

También, la investigación se enmarca en el paradigma cuantitativo con apoyo bibliográfico. En cuanto al enfoque de las investigaciones cuantitativas, Hurtado y Toro (1998), señalan que los estudios bajo este paradigma "son aquellos que predominantemente, tienden a usar instrumentos y comparaciones que proporcionan datos cuyo estudio requiere el uso de modelos matemáticos y de la estadística" (p.11). Con referencia a lo anterior, la presente investigación es cuantitativa ya que requiere de un instrumento para medir datos estadísticos.

Así mismo, el trabajo se apoya en una revisión documental, en relación a la cual Bavaresco (2001) señala que constituye prácticamente la exploración que da inicio a casi todas las demás, cuanto permite un conocimiento previo con el soporte documental bibliográfico vinculante al tema de estudio. En la presente investigación, las fuentes primarias que sirvieron a la investigación estuvo constituida por las relaciones estadísticas y datos aportados por el Comando Aéreo de Mantenimiento de la Especialidad de Seguridad y Defensa de Bases Aéreas

de la Fuerza Aérea de Colombia (2020), plasmadas en el Manual del Plan Estratégico de la Unidad.

Así mismo, las fuentes secundarias que sirvieron a la investigación estuvo constituida por diferentes libros y material de internet que sirvió para dar respuesta a los antecedentes, bases teóricas, bases legales y conceptuales.

Tipo de Estudio

Con respecto al presente proyecto, constituye una investigación de tipo no experimental y descriptiva. Así, Hurtado y Toro (1998) señalan que, en las investigaciones no experimentales, "el investigador no tiene control sobre las variables independientes porque los hechos no pueden ser intrínsecamente manipulables" (p.26); en el presente trabajo los cambios en la variable independiente ya ocurrieron y el investigador no tiene la capacidad de influir sobre las variables y sus efectos. En el caso de la presente investigación, la variable independiente se refiere al control de acceso en el grupo de seguridad, mientras que la variable dependiente lo constituye la protección de datos personales.

De igual forma, Sabino (2011) considera un estudio descriptivo como aquellos que se proponen conocer grupos homogéneos de fenómenos utilizando criterios sistemáticos que permitan poner de manifiesto su estructura o comportamiento; por lo tanto, no se ocupan de la verificación de hipótesis sino de la descripción de hechos a partir de un criterio o modelo teórico definido previamente. Con referencia a lo anterior, el trabajo es descriptivo ya que busca características de situaciones específicas, comprende la descripción, registro, análisis e interpretación de la naturaleza actual y los factores que influyen en el entorno estudiado.

Diseño Metodológico para la Propuesta de la Investigación

Para el diseño metodológico de la propuesta de investigación se seguirá un modelo basado en el ciclo PHVA, lo cual se explica a continuación.

Modelo

Es una representación de un sistema. Consiste en conceptos utilizados para ayudar a las personas a conocer, comprender o simular un tema. De tal manera, los modelos conceptuales suelen ser abstracciones de cosas del mundo real, ya sean físicas o sociales. Igualmente, los estudios semánticos son relevantes para varias etapas de formación de conceptos; la semántica se trata básicamente de conceptos, el significado que los seres pensantes dan a varios elementos de su experiencia (Villalba, 2018).

En relación a los tipos de modelos; los modelos conceptuales varían en tipo desde los más concretos, como la imagen mental de un objeto físico familiar, hasta la generalidad formal y la abstracción de los modelos matemáticos que no aparecen en la mente como una imagen. Los modelos conceptuales también varían en términos del alcance del tema que representan. Un modelo puede, por ejemplo, representar una sola cosa e incluso dominios muy amplios de la materia, como el universo físico; así, la variedad y alcance de los modelos conceptuales se debe a la variedad de propósitos que se tiene (Villalba, 2018).

Modelo PHVA

La serie de normas internacionales mundial para la implementación de sistemas de gestión de calidad y ambiental son la Serie ISO 9000; surgidas con la finalidad de contrarrestar las necesidades de mejora en la calidad de los productos y procesos en la organización (Remolina, 2013). En ese sentido, el continuo énfasis de la calidad da norma ISO 9001 como modelo mundial para los sistemas de gestión de la calidad. Frente a su desarrollo la Norma ISO

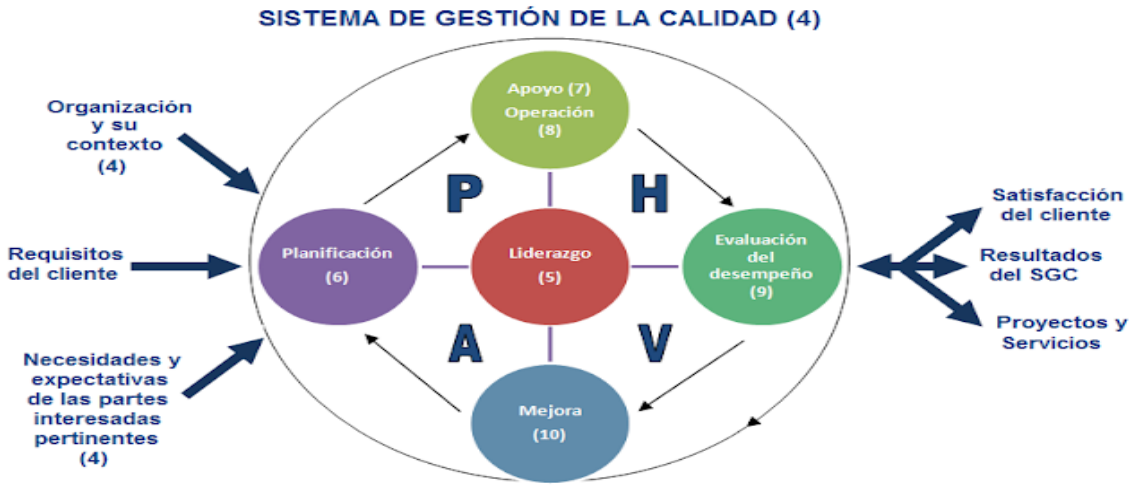
9001 se revisó los años 1994, 2000, y 2008; en el año 2015 la ISO, publico la versión más reciente de esta norma, estableciendo los parámetros y requisitos para que los sistemas de gestión de la calidad puedan ser implementados por cualquier organización.

En ese aspecto, Cruz y Ruiz (2016) indican que la última ISO 9001 orienta a demostrar la capacidad de satisfacer las necesidades y expectativas de los usuarios y demás partes interesadas, y posteriormente aspirar al logro de la excelencia. Teniendo en cuenta lo anterior, los sistemas de Sistema de Gestión de Calidad (SGC) basado en la norma ISO 9001, proporciona una base sólida para la construcción de un programa de gestión total.

En la figura siguiente, se establece la estructura de la Norma ISO 9001:2015 con relación al ciclo PHVA: Planificar – Hacer – Verificar – Actuar. El ciclo PHVA pretende de manera sistemática armonizar los procesos planteados y desarrollar sus resultados como una opción de aprendizaje y mejora de las numerosas variables de calidad.

Figura 1

Estructura de la Norma ISO 9001:2015 con relación al ciclo PHVA



Nota. Tomado de ISO 9001 (2015). Sistemas de Gestión de la Calidad. Requisitos. Colombia: ICONTEC.

Es importante indicar que, la norma ISO 9001:2015 establece 10 ítems. Los tres primeros tratan respectivamente del objeto y campo de aplicación, referencias normativas y términos y definiciones. Los ítems restantes (4 al 10) especifican los requisitos generales a los cuales la empresa debe dar cumplimiento, para establecer, implementar y mantener el sistema de gestión con el fin de satisfacer las expectativas del cliente. La tabla siguiente destaca los aportes de los ítems 4 al 10, dentro de la norma ISO 9001:2015.

Tabla 2

Requisitos numerales cuatro al diez de la Norma ISO 9001:2015

Numeral	Descripción
4. Contexto de la Organización	Incluye los requisitos generales como de información documentada. Se incluyen 2 sub-ítems enfocados al contexto de la organización, para identificar los factores tanto internos como externos que podrían afectar la organización positiva o negativamente; considerando herramientas como la Matriz DOFA y el Diagrama causa efecto.
4. Liderazgo	Debe asegurarse que el Sistema de Gestión de la Calidad (SGC) y sus requisitos están integrados en los procesos de la organización y de que la política y los objetivos están alineados con la dirección estratégica de la misma. En este se debe incluir toda aquella evidencia de que la dirección de la empresa mantiene un máximo compromiso y liderazgo para el cumplimiento de los requisitos exigidos SGC. La dirección deberá estar verificando el cumplimiento estos objetivos, para así determinar acciones de mejora.
6. Planificación	Esta numeral se enfoca en cómo la organización planea acciones para abordar los riesgos y oportunidades a nivel interno y externo, así como la planificación de objetivos de calidad y fines necesarios para cumplirlos.
7. Apoyo	Establece los criterios para que la organización, determine y proporcione los recursos para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Calidad. También hace relación al control de acceso a la información documentada que refleja la importancia de la seguridad de la información.

8. Operación	Este numeral hace énfasis en que la organización debe tener pleno conocimiento de los requisitos del cliente relacionados con el servicio, para posteriormente obtener retroalimentación del cliente acerca de sus opiniones, quejas y sugerencias. Por tanto, se concentra en las acciones para la planificación, implementación y control de procesos para la provisión de productos y servicios.
9. Evaluación	En este numeral se mide y evalúa el SGC para asegurar que sea efectivo y que ayude a mejorar de manera continua los procesos en la organización. De igual manera, señala los procesos de auditoría interna y de revisión por parte de la gerencia.
10. Mejora	Dependiendo del resultado de la evaluación del desempeño, la organización debe tomar acciones correctivas para mejorar la eficacia del sistema para así controlar y corregir las no conformidades que se puedan presentar para entrar en un proceso de mejora continua. Buscando oportunidades de mejora para cumplir los requisitos del cliente y aumentar la satisfacción del cliente.

Nota. Elaboración propia tomada de (ISO 9001, 2015). Sistemas de Gestión de la Calidad. Requisitos. Colombia: ICONTEC.

Población y Muestra

Se entiende por población, según Hernández Sampieri et al. (2012) “cualquier conjunto de elementos de los que se quiere conocer o investigar alguna o algunas de sus características” (p.196). Para efectos del estudio, la población de interés estará estructurada por todo el personal militar perteneciente al Comando Aéreo de Mantenimiento de la Especialidad de Seguridad y Defensa de Bases Aéreas de la Fuerza Aérea de Colombia; conformada por 322 oficiales y suboficiales.

Con respecto a la muestra, Arias (2012) señala, que “es un subconjunto representativo y finito que se extrae de la población accesible” (p.34). En este sentido, una muestra representativa es aquella que por su tamaño y características similares a las del conjunto, permiten hacer inferencias o generalizar los resultados al resto de la población con un margen de error conocido.

Así, se considera para la investigación, una muestra representativa y aleatoria de la población conformada por miembros del grupo de seguridad de la Unidad: oficiales (05), suboficiales (10), personal civil (10) y soldados (10); logrando impactar a las personas que brindan datos al control acceso; así mismo se tendrán las personas residentes (10) y flotantes (5); para un total de 50 individuos.

Pilotaje

Para dar cumplimiento al primer objetivo, diagnóstico de la situación actual en protección de datos haciendo énfasis en las debilidades que exponen a terceros los datos personales para salvaguardar los datos en el control acceso del CAMAN; la misma se logró mediante una investigación de campo ya que se tomaron los datos provenientes de la realidad y se relacionaron con la dimensión 1 de la operacionalización de las variables, basado en los postulados de la Ley 1581 de 2012; dando así respuesta a dicho objetivo.

Así mismo, el segundo objetivo referido a establecer los elementos que debe contener el modelo de protección de datos que ayuden a mitigar el riesgo de pérdida de la información en el control acceso del CAMAN; la misma se logró mediante una investigación de campo ya que se tomaron los datos provenientes de la realidad y se relacionaron con la dimensión 2 de la operacionalización de las variables, basado en los postulados de la Ley 1581 de 2012; dando así respuesta a dicho objetivo.

Partiendo de lo anterior, en el proceso de validación del instrumento se consideró pertinente la puesta a prueba de la encuesta a fin de evaluar su correcto diseño, es decir, estimar que tan efectivos será en el acopio de datos, a la hora de aplicarlo. En este sentido, se juzgó pertinente un tipo de valoración, probar la claridad expositiva de las preguntas en la encuesta.

Al respecto, Hernández Sampieri et al. (2012), señala que la validez “Se refiere al grado en que un instrumento realmente mide la variable que pretende medir” (p.243). A través de la validación, se trata de determinar hasta dónde los ítems de un instrumento son representativos de dominio o universo de contenido de la propiedad que se desea medir.

En este estudio, el instrumento fue sometido a la validez de contenido. Para ello, se seleccionó un experto en la temática, quién juzgó cada ítem por su adecuación con los objetivos y la teoría, por su congruencia y claridad en la redacción; con la finalidad de asegurar que reúnen condiciones para su aplicación. Realizadas las correcciones sugeridas por el juez, se procedió a elaborar el instrumento definitivo.

Posteriormente, se tabularon los datos recolectados para luego organizarlos y presentarlos en gráficos que visualizaron los porcentajes obtenidos utilizando la estadística descriptiva, para luego interpretarlos y responder de esa forma al objetivo relacionado.

Seguidamente, en cuanto al tercer objetivo referido a diseñar un modelo de protección de datos personales en el control de acceso que mediante formatos y procedimientos permita asegurar la integridad de la información del control acceso del CAMAN; éste se logró mediante la exploración teórica, en donde el autor de la presente investigación interpreta los resultados obtenidos en los anteriores objetivos respaldado por información documental; presentando así lineamientos gerenciales y operativos inherentes en la protección de datos personales basados en la Ley 1581 de 2012; para permitir asegurar la integridad de la información.

Así mismo, el trabajo se apoya en una revisión bibliográfica, en relación a la cual Bavaresco (2001) señala que constituye prácticamente la exploración que da inicio a casi todas las demás, cuanto permite un conocimiento previo con el soporte documental bibliográfico

vinculante al tema de estudio. En la presente investigación, dicha revisión bibliográfica estuvo constituida por fuentes primarias y secundarias que se explican a continuación.

Fuentes Primarias y Secundarias

Como fuentes primarias se tuvo las personas a las que se les aplicó el instrumento de recolección de datos; dicho instrumento se refiere al cuestionario diseñado para describir la situación y el establecimiento de los elementos relacionados a la protección de datos que ayuden a mitigar el riesgo de pérdida de la información. Así mismo, se incluyó el análisis jurisprudencial de la Ley 1581 de 2012, mediante el análisis de diferentes sentencias.

Así mismo, las fuentes secundarias estarán conformadas por los documentos que sirvieron como base para el marco teórico y para la investigación en general, constituidos principalmente por la Ley 1581 de 2012. Consecuentemente, dicha investigación arrojó como resultado las características y fundamentos de los principales principios y postulados que permiten diseñar el modelo de protección de datos personales en el control de acceso de CAMAN.

Instrumentos de Recolección de Datos

Dado que el estudio se enmarca en una investigación de campo y la misma basa su accionar en la recopilación de datos primarios obtenidos directamente de la realidad, se utilizará el instrumento conocido como encuesta, en este caso dirigido al personal militar de la organización y cuyo contenido es basado en los postulados de la Ley 1581 de 2012.

Sobre el asunto, una encuesta es un método de investigación utilizado para recopilar datos de un grupo predefinido de encuestados para obtener información y puntos de vista sobre varios temas de interés. Pueden tener múltiples propósitos y los investigadores pueden llevarlo a cabo de muchas maneras según la metodología elegida y el objetivo del estudio (Balestrini, 2015).

Igualmente, con la encuesta, los datos generalmente se obtienen mediante el uso de procedimientos estandarizados para garantizar que cada encuestado pueda responder las preguntas en igualdad de condiciones para evitar opiniones sesgadas que puedan influir en el resultado de la investigación o el estudio. El proceso implica pedir información a las personas a través de un cuestionario, que puede ser en línea o fuera de línea (Balestrini, 2015).

De esta forma, se utilizó un tipo de encuesta denominado cuestionario, que aporta información sobre un tema de interés, y puede ser presentada en un formato donde el encuestador realiza preguntas puntuales al encuestado, seleccionando sólo lo que indican las mismas, sin permitir hablar de otros puntos que no contemple el instrumento (Arias, 2012). Partiendo de lo anterior, dicho cuestionario estuvo estructurado en base a opciones cerradas (Si, NO) las cuales según Arias (2012) “establecen previamente las opciones de respuestas que puede elegir el encuestado” (p.72); a fin de recabar información relacionada con los veinticuatro (24) ítems del cuestionario aplicado.

En relación a la validación del instrumento, la pertinencia y congruencia de las preguntas fueron revisadas mediante el juicio de expertos, en donde un profesional en el área evaluó cada ítem del instrumento mediante un formato predeterminado (ver anexos). Partiendo de lo anterior, la variable del estudio es: formular un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento CAMAN; entendida como los lineamientos y protocolos que deben seguirse para asegurar los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, así como de saber qué datos están siendo tanto retenidos como usados y de corregir las inexactitudes. Igualmente, las dimensiones dele estudio fueron: situación actual en protección de datos personales; elementos de protección; modelo de protección de datos.

Desde este punto de vista, la variable principal de la investigación está delineada por el objetivo general de la investigación presente que fue abordado mediante el diseño de un modelo de protección de datos luego de realizado el diagnóstico y detectado los elementos que intervienen, lo cual tiene relación directa con los indicadores especificados en la operacionalización de las variables.

De acuerdo a lo anterior, se propone la siguiente tabla de operacionalización de la variable, de manera de visualizar las dimensiones e indicadores que la componen. Así, se propone el cuestionario (ver anexo 1) a aplicar en el trabajo para el abordaje del problema identificado, tomando como base el sistema de variables diseñado, el cual se visualiza en la tabla siguiente (ver tabla 3) y está basado en los principales postulados de la Ley 1581 de 2012.

Tabla 3

Operacionalización de la Variable

VARIABLE	DIMENSIONES	INDICADORES	Cuestionario Ítems
Modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento, mediante un análisis documental tanto al interior como al exterior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante.	Situación actual en protección de datos personales	- Normas de control interno	1
		- Procedimientos existentes	2
		- Estructura organizativa	3
		- Entrada y salida de datos	4,5
		- Calidad de datos	6
		- Control de datos	7,8
		- Almacenamiento	9
	Elementos de Protección de datos	- Tipos de datos	10,11,12,13
		- Ambiente de control	14,15
		- Evaluación de riesgos	16,17
		- Actividades de control	18,19,20

	- Información y comunicación	21,22
	- Monitoreo	23,24

Nota. Investigación propia.

Determinadas la variable de la investigación, las dimensiones e indicadores respectivos, se procede seguidamente a definir los principales resultados que derivarán de los diferentes objetivos que dan sentido a la investigación presente.

Entregables

Los entregables de la investigación parten de los lineamientos derivados de la necesidad previamente determinada, según los resultados obtenidos y discutidos anteriormente, los cuales evidencian aspectos por mejorar en la protección de datos personales para el control de acceso en la seguridad física del CAMAN.

Consecuentemente, se aspira entregar un modelo basado en la teoría del método COSO y en los principales postulados de la Ley 1581 de 2012, que contribuya a la mejora de la seguridad en el control de acceso del CAMAN, mediante una serie tanto de políticas (etapa gerencial) como de procedimientos (etapa operativa) que contribuirán con una mejor gestión. Igualmente, al emprenderse el mejoramiento continuo antes señalado, la organización estará en capacidad de satisfacer las necesidades y expectativas de su personal.

Análisis de Resultados

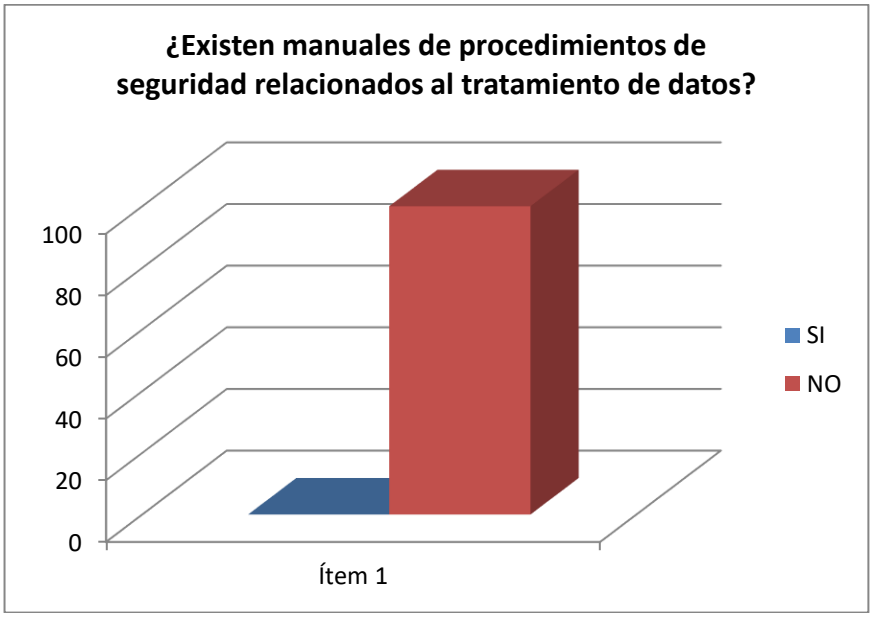
A continuación, se visualizan los resultados inherentes a la aplicación del cuestionario relativo al personal involucrado, mediante la interpretación de datos cuantitativos presentados a través de gráficos usando la hoja electrónica de cálculo Microsoft Excel. Así, se da respuesta a los objetivos uno y dos de la investigación.

Situación Actual en Protección de Datos Personales Haciendo Énfasis en las Debilidades que Exponen a Terceros los Datos Personales para Salvaguardar los Datos

De acuerdo con lo revisado en el marco de referencia y las herramientas utilizadas en esta metodología, se da cumplimiento al objetivo No. 1, toda vez que se visualizan los resultados inherentes a la dimensión diagnóstico, mediante la interpretación de datos cuantitativos presentados a través de gráficos usando la hoja electrónica de cálculo Microsoft Excel.

Figura 2

Análisis del indicador: Normas de control interno



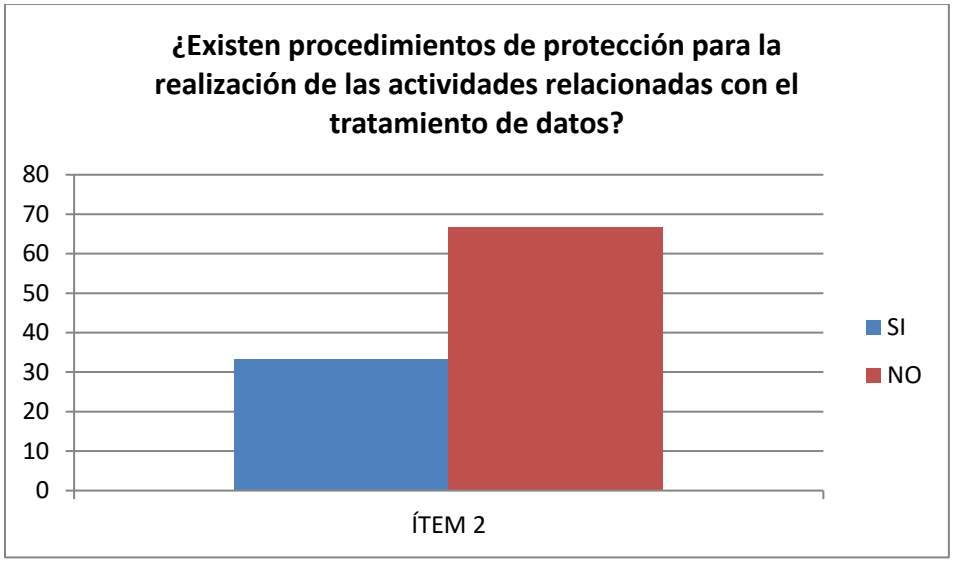
Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

En relación al ítem 1, un 100% del personal asegura que la Unidad no cuenta con un manual descriptivo de los procedimientos de seguridad. Así, en lo que se refiere a los manuales, de acuerdo con Guédez (2002), los mismos ayudan a establecer la descripción de las actividades basadas en la planificación, especificando también las responsabilidades y funciones estratégicas de cada cargo.

De allí, que la organización presenta debilidad en este indicador ya que no se establecen los procedimientos específicos de control interno según los objetivos institucionales, de tal forma que en el proceso se garantice la seguridad para un efectivo tratamiento de los datos.

Figura 3

Análisis del indicador: Procedimientos existentes



Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

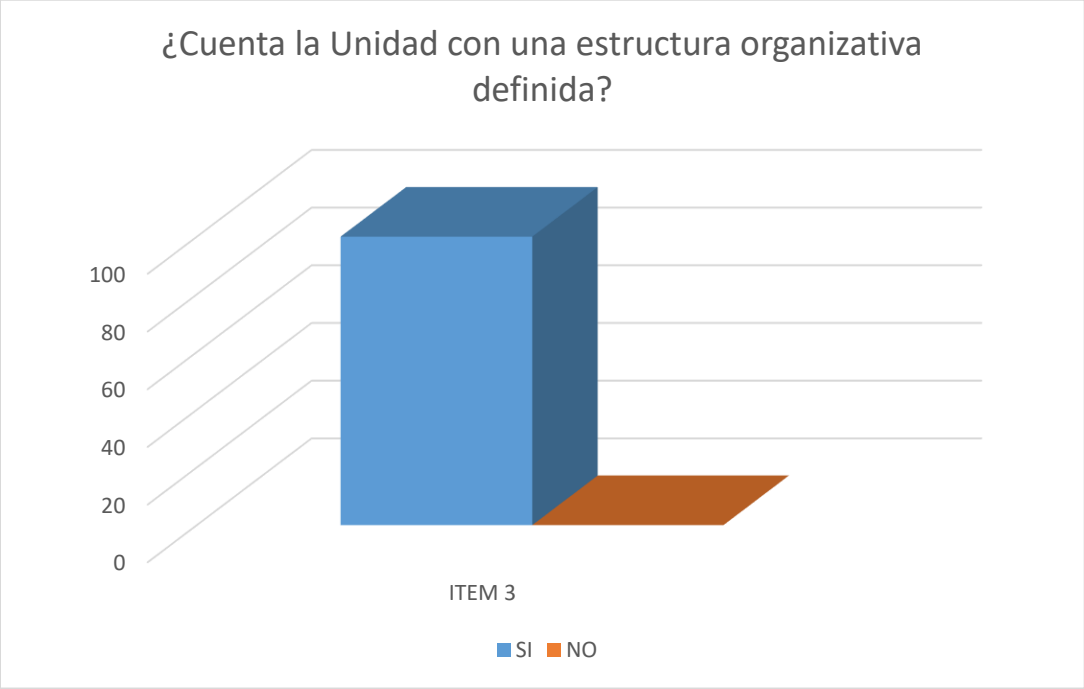
Al analizar la figura 3, el ítem 2 refleja que el 66,67% de los encuestados piensan que no existen procedimientos de protección para el tratamiento de los datos, mientras que el otro 33,33% piensa que sí existen. Al respecto, los procedimientos contribuyen a que exista una estructura formal de protección de la información en la Unidad, de tal forma que estén definidas

las responsabilidades y las actividades diversas como la descarga y carga de datos, actualización de información de las personas, entre otras actividades inherentes a la gestión de los datos.

Por lo tanto, existe una debilidad en el área descrita ya que a pesar que la Unidad tiene definida ciertas normativas para los procesos de seguridad, éstas no se cumplen o no se toman en cuenta, lo que impide tener una referencia para realizar las actividades inherentes, según reflejan los resultados.

Figura 4

Análisis del indicador: Estructura organizativa



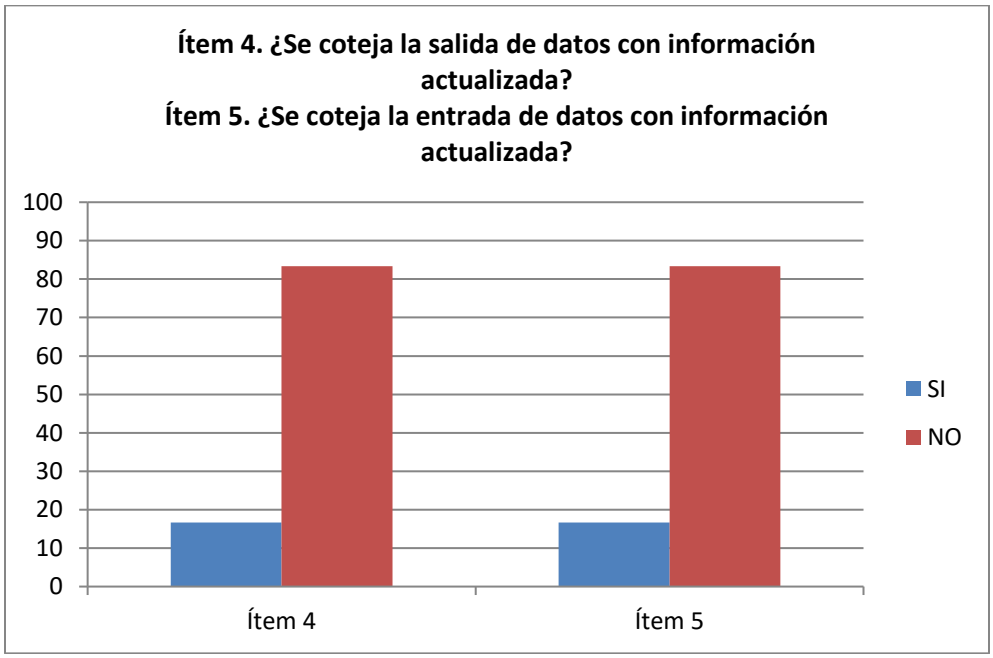
Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

En relación al ítem 3; en el gráfico 4 se indica que el 100% de los sujetos encuestados piensa que la Unidad cuenta con una estructura organizativa. Bajo estas consideraciones, es claro que en la Unidad existe una formalidad de cargos definida, ésta se cumple o y es conocida por los efectivos, lo cual permite inferir una fortaleza en la estructura organizativa, ya que se tienen los conocimientos generales acerca de las responsabilidades y funciones del personal en el área y

se conocen los grados de jerarquía que posee cada efectivo de acuerdo al cargo que desempeñan en la organización.

Figura 5

Análisis del indicador: Entrada y salida de datos



Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

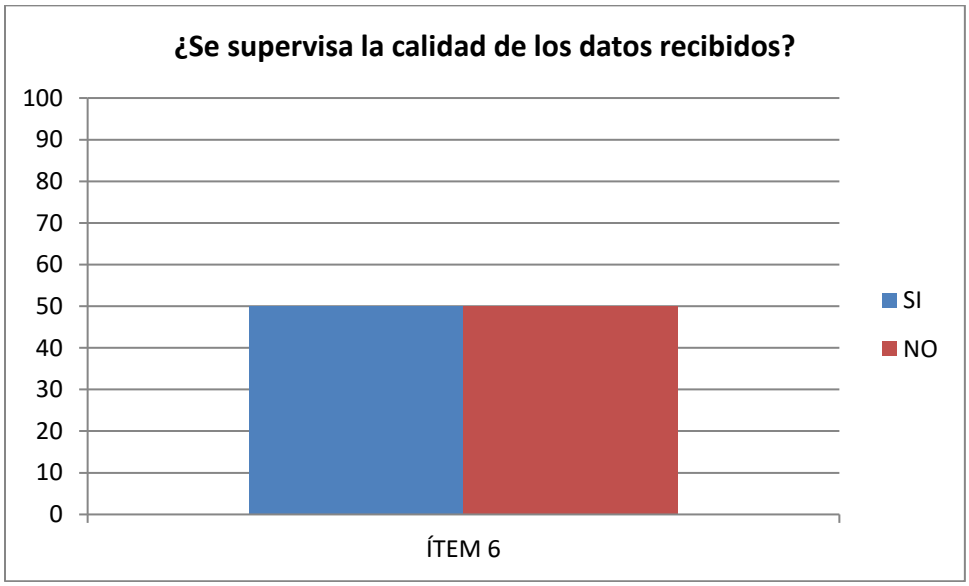
Al analizar la figura 5; se observa que en el ítem 4 el 16,67% respondió que sí se coteja oportunamente la salida de datos con información actualizada, mientras que el restante 83,33% opina que no. Con respecto al ítem 5, el 16,67% piensa que sí se coteja oportunamente la entrada de datos con información actualizada, mientras que el 83,33% opina lo contrario.

Así, como lo señala Pereira (2015), una de las principales actividades para la seguridad militar lo constituye la entrada y salida de datos, por lo que gestionar y controlar adecuadamente este ciclo en el tratamiento de datos es uno de los procesos más determinantes a la hora de conseguir el éxito dentro de la entidad castrense. Por lo tanto, existe una desorganización visible en dicho ciclo, lo que revela que puede existir una ausencia de interrelación adecuada entre la

información generada internamente y la actualización que necesitan otras unidades o personas externamente.

Figura 6

Análisis del indicador: Calidad de los datos



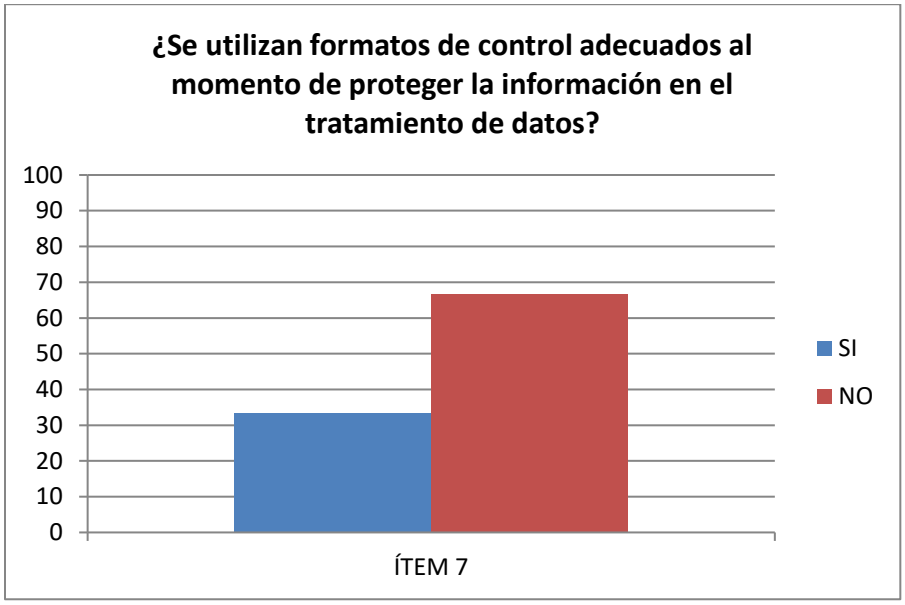
Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad

Al analizar la figura 6, se observa en el ítem 6 que el 50% respondió que se supervisa oportunamente la calidad de los datos que se reciben, mientras que un 50% opinó lo contrario. Así, Ojeda (2008) señala que la calidad es la veracidad de la información que se recibe por lo que una supervisión en el proceso permite chequear debidamente la información que van a formar parte del proceso de tratamiento de datos, así como aquella que llegue desactualizada.

En base a los resultados obtenidos, a pesar que la actividad de supervisión existe, se visualiza que ésta no se cumple como deber ser o presenta fallas, lo cual es una debilidad para la organización ya que no se controla debidamente la calidad, debido a la informalidad con que se ejecuta.

Figura 7.

Análisis del indicador: Control de datos



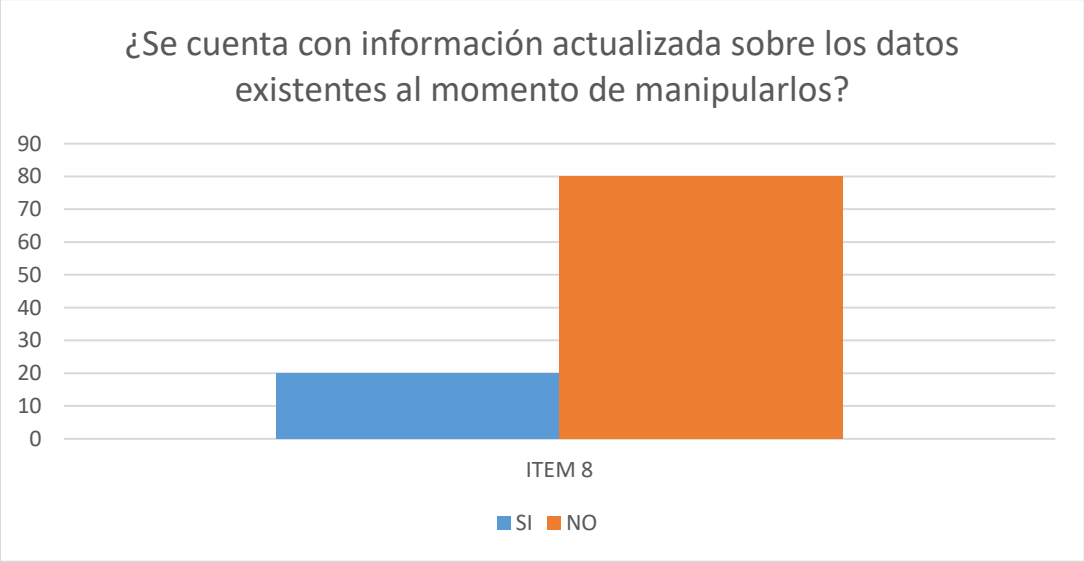
Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

En relación el ítem 7 de la figura 7, el 33,33% de los sujetos encuestados indican que se utilizan formatos de control adecuados al momento de proteger la información en el tratamiento de datos, mientras que el 66,67% opina que dichos formatos no se generan. En el proceso de seguridad es importante establecer un método de control que debe ser registrado en la base de datos que se utilice y que permita manipular los datos de acuerdo a la información de personal interno y externo, en los formatos de control adecuados.

En este sentido, se visualiza en primer término que no existe un método de control, además en segundo término al no existir precisión en los formatos de control correspondientes al movimiento de información no se puede determinar la fiabilidad de los datos, a fin de valorar los riesgos a los que se exponen; constituyendo ambas premisas debilidades en el área descrita.

Figura 8

Análisis del indicador: Control de datos (continuación)

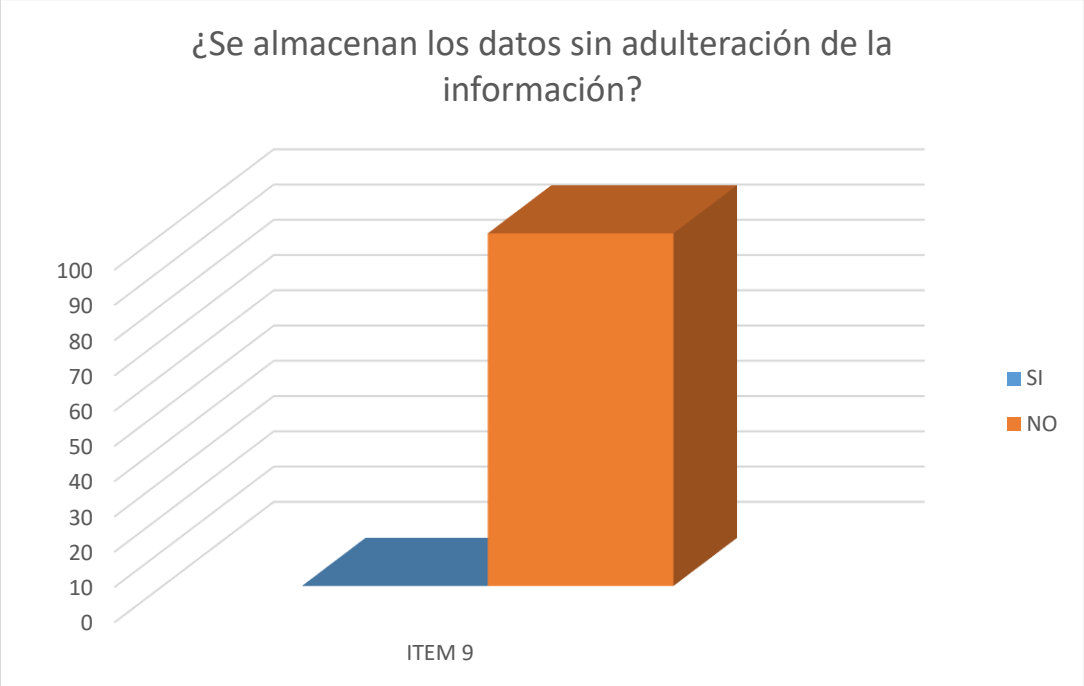


Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad

Con respecto a la figura 8, en el ítem 8 el 20% de los encuestados señalan que se cuenta con información actualizada sobre los datos existentes al momento de manipularlos, mientras que un 80% creen lo contrario. En este sentido, la información de los datos es muy importante mantenerla actualizada ya que apoya la toma de decisión en el área. Igual, se denota que la Unidad a pesar de contar con un sistema de información administrativo, muchas veces no se mantienen datos oportunos y confiables que resulten de interés a los diferentes niveles; por lo cual, constituye una debilidad para el control de datos.

Figura 9

Análisis del indicador: Almacenamiento de datos

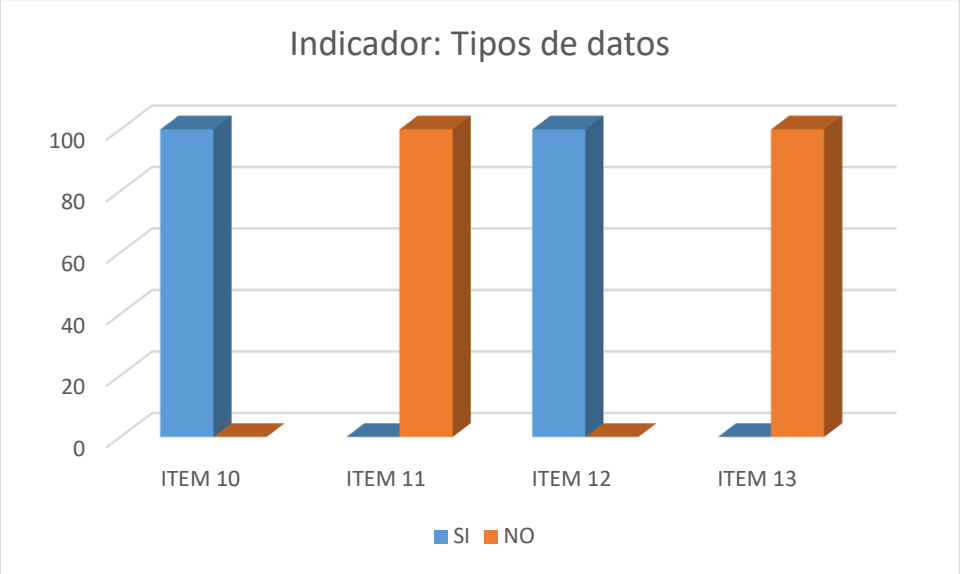


Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad

En cuanto al ítem 9 de la figura 9; el 100% coincidió en que no se mantiene un nivel adecuado de almacenamiento sin adulteración o fallas en la información registrada. Según Celemín (2015), es importante organizar los datos de tal manera que no se presenten inconsistencias y sean de fácil acceso. De acuerdo a lo descrito, existe una debilidad organizacional ya que en la información almacenada no existen los niveles mínimos que impidan las incongruencias, fallas, corrupción de datos y que garanticen la seguridad de los mismos.

Figura 10

Análisis del indicador: Tipos de datos



Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

En relación al ítem 10 de la figura 10, el 100% de los encuestados consideran que sí se da un buen tratamiento a los datos públicos. Igual, en el ítem 12, el 100% de los sujetos consideran que sí se le da el tratamiento adecuado a los datos semiprivados.

Así mismo, sobre el ítem 11 de la figura 9, el 100% de los encuestados piensa que no se actualiza en forma oportuna la información relacionada con datos privados, mientras que en relación al ítem 13, el 100% de los trabajadores opinan que no se actualiza en forma oportuna la información relacionada con datos sensibles.

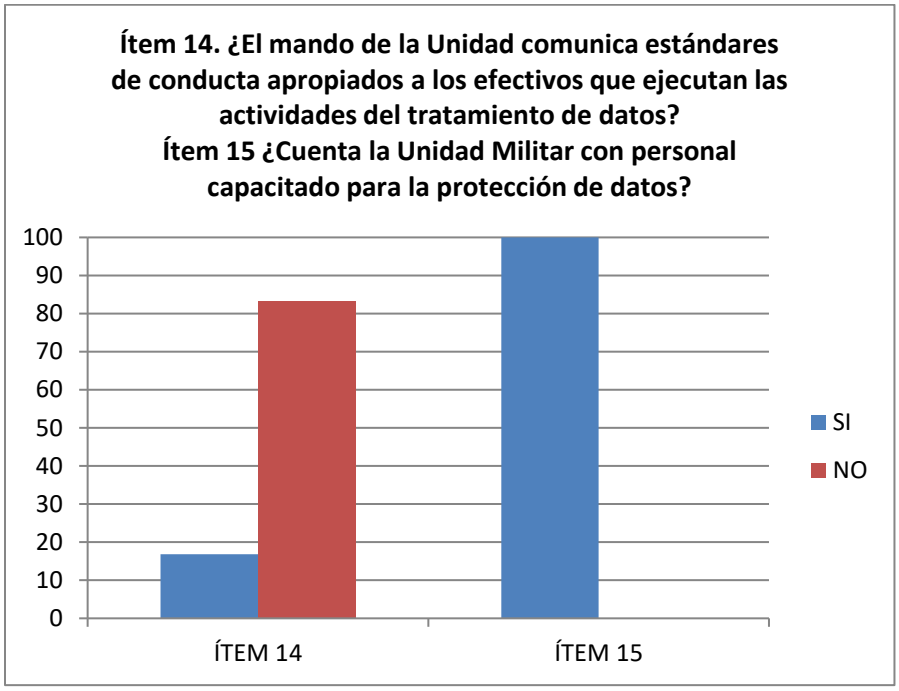
Al respecto, según Marín (2016) los ajustes relacionados a la información de los diferentes tipos de datos deben realizarse en forma oportuna y generar la actualización respectiva, evitando así errores y omisiones. Así, se percibe que la institución posiblemente no le esté dando el tratamiento adecuado tanto a los datos privados como a los sensibles.

Elementos que Debe Contener el Modelo de Protección de Datos que Ayuden a Mitigar el Riesgo de Pérdida de la Información

De acuerdo con lo revisado en el marco de referencia y las herramientas utilizadas en esta metodología, se da cumplimiento al objetivo No. 2, toda vez que se visualizan los resultados inherentes a la dimensión de elementos de protección de datos, mediante la interpretación de datos cuantitativos presentados a través de gráficos usando la hoja electrónica de cálculo Excel.

Figura 11

Análisis del indicador: Ambiente de control



Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

De acuerdo a la figura 11; en el ítem 14 los efectivos señalan en un 16,67% que el mando de la Unidad comunica estándares de conducta apropiados al personal que ejecuta las actividades del tratamiento de datos, mientras un 83,33% piensa que esto no sucede; en referencia al ítem 15

el 100% de los encuestados consideran que sí cuenta la Unidad con personal capacitado para llevar a cabo el proceso de protección de los datos.

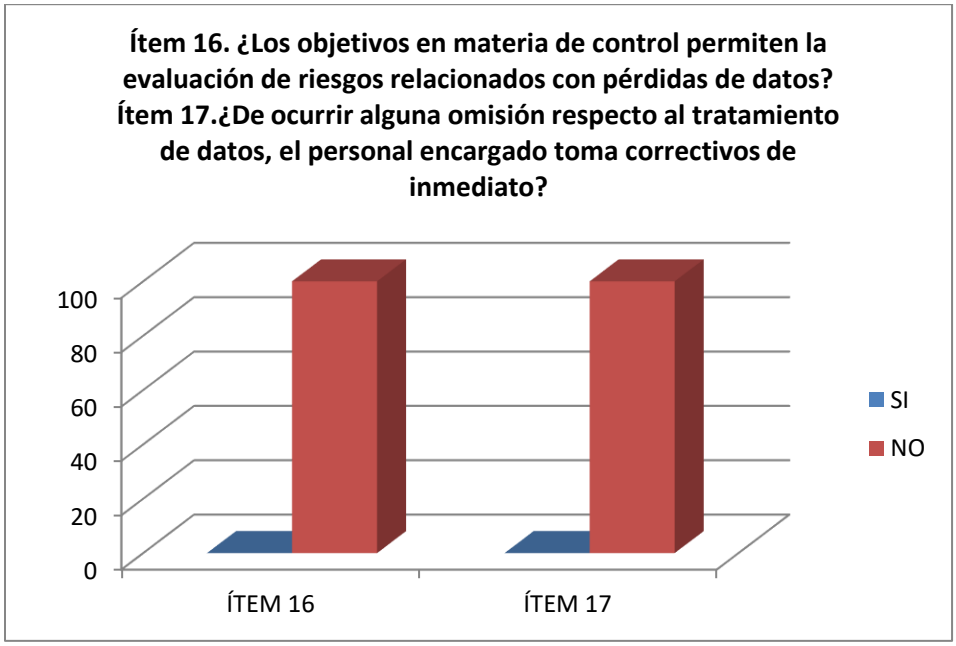
Al respecto, los estándares de conductas guían a la organización en comportamientos, actividades y decisiones para la consecución de sus objetivos, por lo que existe una debilidad en la comunicación que impide que el personal pueda reportar las irregularidades que se presenten a los mandos superiores.

Igualmente, contar con personal con los conocimientos esperados para ejercer sus funciones es importante ya que constituye una ventaja competitiva que le permitirá a la organización poder trabajar en equipo para corregir fallas existentes en el área de la seguridad y protección de los datos.

De esta forma, la Unidad muestra una fortaleza importante en este campo ya que se visualiza un grupo de efectivos capaces de llevar a cabo sus labores, por lo que se puede emprender planes para aprovechar ese talento y a la vez satisfacer los requerimientos de éstos en cuanto a formación y estabilidad, asumiendo entonces un rol competitivo en el ramo. Así, para lograr los objetivos propuestos el mando superior debe realizar diferentes actividades al momento de selección, capacitación, rotación y promoción del personal.

Figura 12

Análisis del indicador: Evaluación de riesgos



Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

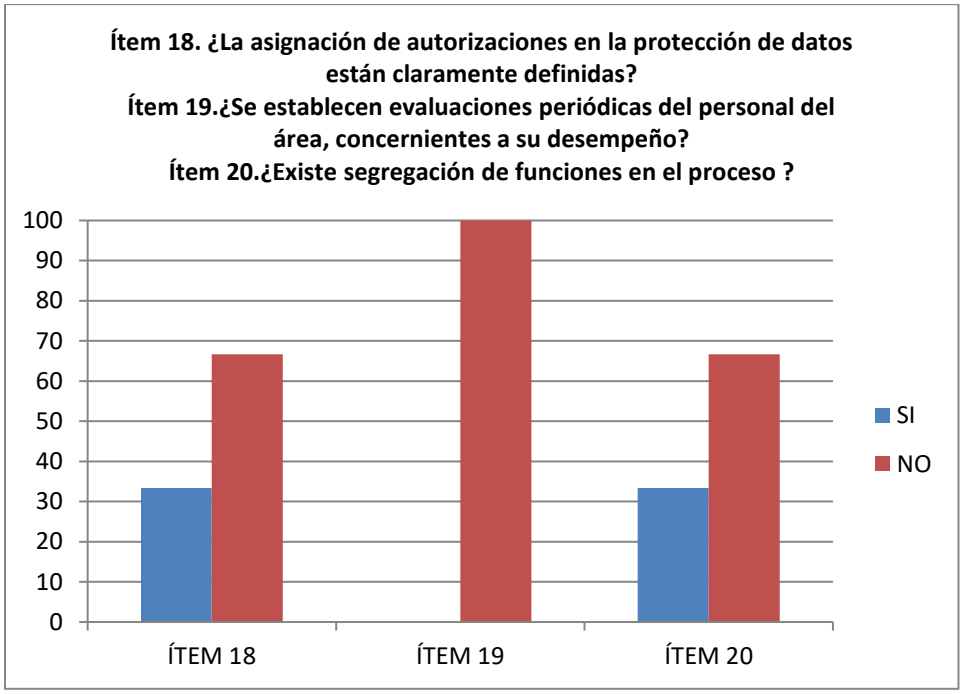
En relación a la figura 12; en el ítem 16 se denota que el 100% de los entrevistados señalan que los objetivos en materia de protección de los datos no permiten la evaluación de riesgos relacionados con pérdidas, mientras igual en el ítem 17, el 100% de los sujetos coinciden que, de ocurrir alguna omisión respecto al proceso del tratamiento de la información, el personal encargado no toma correctivos de forma inmediata.

En este sentido, Celemín (2015) señala que la implementación de políticas de control relacionadas con la evaluación de riesgos, contribuyen a guiar, orientar y encaminar a la fuerza de trabajo para que desarrolle adecuadamente sus funciones. Sin embargo, se presenta una debilidad debido a la ausencia de dichas políticas de dirección, lo que acarrea posibilidades de ausencia, fraudes y pérdidas en la gestión de los datos.

Así mismo, Marín (2016) sostiene que la verificación de objetivos como parte de la evaluación de riesgos en la gestión de datos es fundamental para confirmar que los procesos, procedimientos y actividades se cumplen, por lo que se infiere que existe una debilidad en el área ya que no se corrigen desviaciones a tiempo para encauzar dichas actividades nuevamente hacia los objetivos propuestos.

Figura 13

Análisis del indicador: Actividades de control



Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

En cuanto a la figura 13; el ítem 18 señala que el 33,33% de los encuestados opinan que la asignación de autorizaciones en el proceso de protección de datos está claramente definida, mientras que el otro 66,67% señalan que las mismas no están bien definidas. En cuanto al ítem 19, el 100% cree que no se establecen evaluaciones periódicas del personal del área concernientes a su desempeño; mientras que en el ítem 20 un 33,33% del personal visualiza que

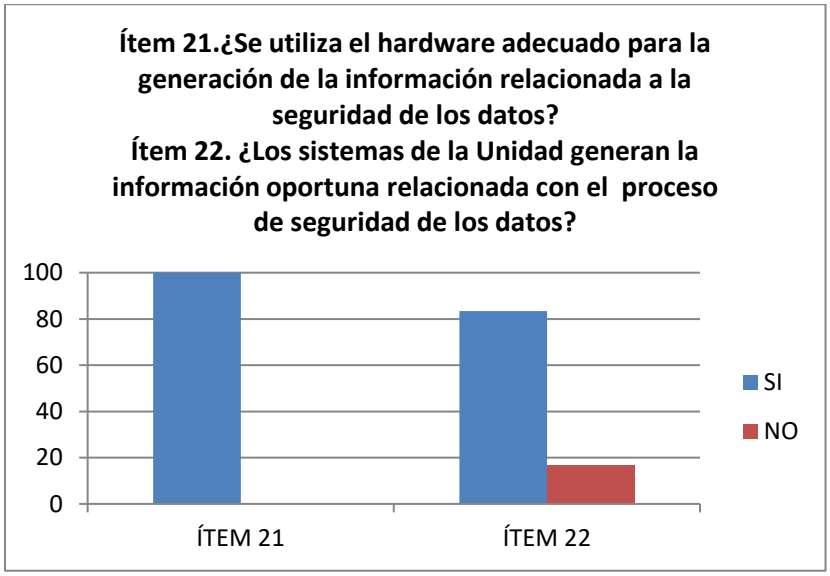
sí existe segregación de funciones en el proceso relacionado con el tratamiento de la información, al contrario de un 66,67% que piensa lo contrario.

En efecto, como lo señala Chopra y Meindl (2008) las autorizaciones promueven el control en las operaciones de control interno con el objetivo de obtener datos seguros, oportunos y confiables. De esta manera, existe una debilidad ya que no se establecen controles adecuados en los diferentes procesos del área lo cual puede traer como consecuencia que no se obtenga la información relacionada en forma oportuna.

De la misma forma, en cuanto a la evaluación de personal, ésta es importante ya que permite la corrección oportuna de desviaciones encontradas, por lo que existe una debilidad al respecto. Finalmente, en cuanto a la segregación o separación de funciones; de acuerdo con Méndez (2002) toda entidad castrense debe establecer la descripción de las actividades basadas en la planificación, especificando también las responsabilidades y funciones estratégicas de cada cargo. De allí, que la organización presenta debilidad en este indicador al no establecer responsabilidades del área de tal forma que en el proceso se garantice la seguridad en el tratamiento de los datos.

Figura 14

Análisis del indicador: Información y comunicación



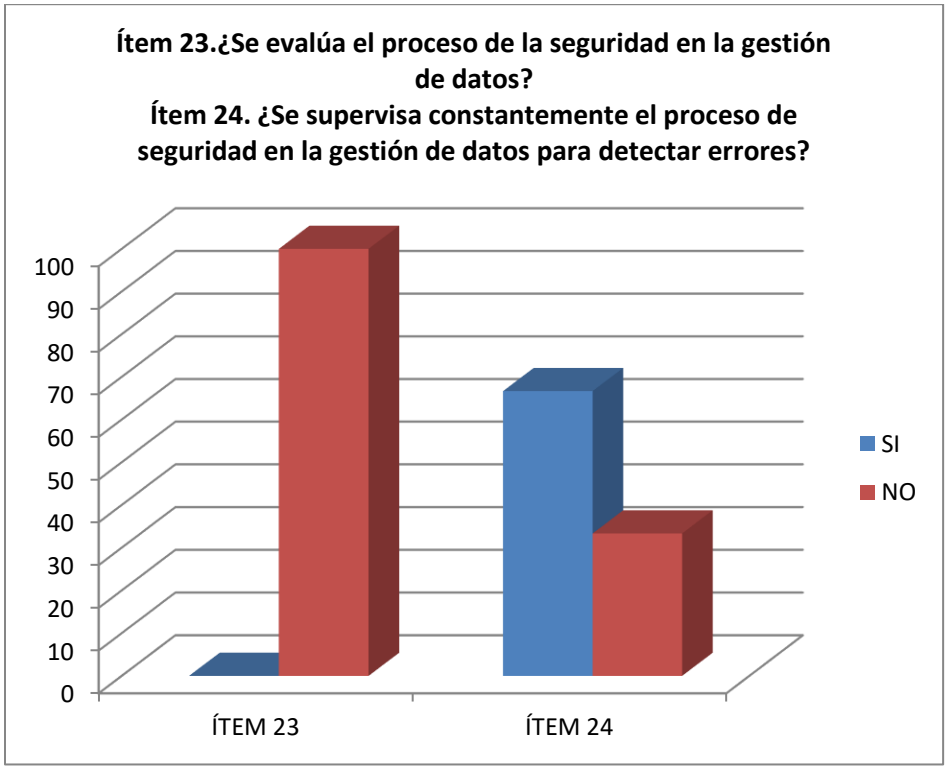
Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

De acuerdo a la figura 14; en el ítem 21 el 100% del personal encuestado coincidió en que se utiliza el hardware adecuado para la generación de la información relacionada al proceso de la seguridad de los datos; mientras en el ítem 22, el 83,33% piensa que los sistemas de la organización castrense sí generan la información oportuna relacionada con el proceso, mientras que un 16,67% opina que no se genera dicha información.

En esta perspectiva, la información es necesaria para que la entidad lleve a cabo las responsabilidades inherentes a la gestión de datos que apoyan el cumplimiento de los objetivos. Por lo tanto, se determina que a pesar que la Unidad cuenta con el hardware y software necesario para el procesamiento de datos, los mismos no se aprovechan al máximo para generar reportes en forma oportuna y apoyar a la administración en el nivel de seguridad esperado.

Figura 15

Análisis del Indicador: Monitoreo



Nota. Elaborado con la información obtenida del instrumento aplicado al personal de la Unidad.

Al revisar la información obtenida de la figura 15; con respecto al ítem 23 el 100% de los efectivos señala que no se evalúa el proceso relacionado a la seguridad en la gestión de los datos, mientras que en el ítem 24 se denota que el 66,67% de los individuos a los que se les aplicó el cuestionario consideran que se supervisa constantemente dicho proceso para detectar errores, mientras que el restante 33,33% opina lo contrario.

De acuerdo a los resultados encontrados, se visualiza que las actividades de monitoreo y supervisión son llevadas a cabo a través de evaluaciones continuas, permitiendo determinar la calidad de las actividades de los diferentes procesos del área. Así, a pesar que la supervisión existe, no se realiza una evaluación de los resultados obtenidos, constituyendo entonces una debilidad del proceso que debe ser afrontada.

Tabla 4

Análisis de la Revisión Documental

Categoría Pregunta	Documento que trata el tema	Observaciones u aportes del investigador
1.¿Existen manuales de procedimientos de seguridad relacionados al tratamiento de datos?	Galvis Cano (2012)	Existen manuales pero no en el área de seguridad integral militar en Colombia
2.¿Existen procedimientos de protección para la realización de las actividades relacionadas con el tratamiento de datos?	Documento CONPES 3701 (2011)	El aporte directo de esta investigación es seguir la Ley 1581 de 2012
3. ¿Cuenta la Unidad con una estructura organizativa definida?	Chopra y Meindl (2008)	El aporte directo de esta investigación es la asignación de responsabilidades y funciones según el modelo COSO y la Ley 1581 de 2012
4. ¿Se coteja la salida de datos con información actualizada?	Galvis Cano (2012)	El aporte directo de esta investigación es la gestión y control adecuado de la salida de datos por ser uno de los procesos más determinantes a la hora de conseguir el éxito dentro de la entidad castrense.
5. ¿Se coteja la entrada de datos con información actualizada?	Celemín (2015)	El aporte directo de esta investigación es la gestión y control adecuado de la entrada de datos por ser uno de los procesos más determinantes a la hora de conseguir el éxito dentro de la entidad castrense.
6. ¿Se supervisa la calidad de los datos recibidos?	Documento CONPES 3701 (2011)	El aporte directo de esta investigación es que la información que va a formar parte del proceso de tratamiento de datos, no llegue a ser desactualizada.
7. ¿Se utilizan formatos de control adecuados al momento de proteger la información en el tratamiento de datos?	Chopra y Meindl (2008)	El aporte directo de esta investigación es que un método de control debe ser registrado en la base de datos para que se utilice y que así permita manipular los datos

		de acuerdo a la información de personal interno y externo.
8. ¿Se cuenta con información actualizada sobre los datos existentes al momento de manipularlos?	Documento CONPES 3701 (2011)	El aporte directo de esta investigación es resaltar el apoyo en la toma de decisión en el área
9. ¿Se almacenan los datos sin adulteración de la información?	Garriga (2004)	El aporte directo de esta investigación es proteger los datos para evitar incongruencias, fallas, corrupción de datos.
10. ¿Se le da un tratamiento adecuado a los datos públicos?	Marín (2016)	El aporte directo de esta investigación es generar la actualización respectiva, evitando así errores y omisiones.
11. ¿Se le da un tratamiento adecuado a los datos privados?	Marín (2016)	El aporte directo de esta investigación es generar la actualización respectiva, evitando así errores y omisiones.
12. ¿Se le da un tratamiento adecuado a los datos semiprivados?	Celemín (2015)	El aporte directo de esta investigación es actualizar en forma oportuna la información relacionada con datos sensibles.
13. ¿Se le da un tratamiento adecuado a los datos sensibles?	Celemín (2015)	El aporte directo de esta investigación es actualizar en forma oportuna la información relacionada con datos sensibles.
14.¿El mando de la Unidad comunica estándares de conducta apropiados a los efectivos que ejecutan las actividades relacionadas al tratamiento de datos?	Maki (2005)	Aporte de la investigación: importancia de reportar las irregularidades que se presenten a los mandos superiores.
15. ¿ Cuenta la Unidad Militar con personal capacitado para la protección de datos?	Maki (2005)	Aporte de la investigación: contar con personal con los conocimientos esperados para ejercer sus funciones es importante ya que constituye una ventaja competitiva que le permitirá a la organización poder trabajar en equipo
16. ¿Los objetivos en materia de control permiten la evaluación de	Maki (2005)	Aporte de la investigación: encaminar a la fuerza de

riesgos relacionados con pérdidas de datos?		trabajo para que desarrolle adecuadamente sus funciones
17.¿De ocurrir alguna omisión respecto al tratamiento de datos, el personal encargado toma correctivos de inmediato?	Mantilla (2013)	Aporte de la investigación: importancia de la retroalimentación en la corrección de desviaciones
18. ¿ La asignación de autorizaciones en la protección de datos están claramente definidas?	Méndez (2002)	Aporte de la investigación: la no observancia puede traer como consecuencia que no se obtenga la información relacionada en forma oportuna.
19. ¿Se establecen evaluaciones periódicas del personal del área, concernientes a su desempeño??	Méndez (2002)	Aporte de la investigación: debe establecer la descripción de las actividades basadas en la planificación, especificando también las responsabilidades y funciones estratégicas de cada cargo.
20. ¿Existe segregación de funciones en el proceso relacionado con la protección de datos?	Mantilla (2013)	Aporte de la investigación: debe establecer la descripción de las actividades basadas en la planificación, especificando también las responsabilidades y funciones estratégicas de cada cargo.
21. ¿Se utiliza el hardware adecuado para la generación de la información relacionada a la seguridad de los datos?	Reynoso (2017)	Aporte de la investigación: relevancia del hardware adecuado para la generación de la información relacionada al proceso de la seguridad de los datos
22. ¿ Los sistemas de la Unidad generan la información oportuna relacionada con el proceso de seguridad de los datos?	Mantilla (2013)	Aporte de la investigación: relevancia del software adecuado para la generación de la información relacionada al proceso de la seguridad de los datos
23. ¿Se evalúa el proceso de la protección de datos?	Pereira (2015)	Aporte de la investigación: supervisa constantemente dicho proceso
24. ¿Se supervisa constantemente el proceso de seguridad en la gestión de datos para detectar errores?	Pereira (2015)	Aporte de la investigación: supervisa constantemente dicho proceso

Nota. Investigación propia.

Triangulación de la Información que se Obtuvo de la Revisión Documental, con la Información que se Consiguió con la Encuesta

Tabla 5

Triangulación de la información

Categoría Pregunta	Resultados encuesta	Información documental	Triangulación de la información
1.¿Existen manuales de procedimientos de seguridad relacionados al tratamiento de datos?	No se establecen los procedimientos específicos de control interno según los objetivos institucionales	Existen manuales pero no en el área de seguridad integral militar en Colombia	Debilidad en este indicador, por lo que se darán lineamientos para la creación de manuales
2.¿Existen procedimientos de protección para la realización de las actividades relacionadas con el tratamiento de datos?	Estos no se cumplen o no se toman en cuenta, lo que impide tener una referencia para realizar las actividades inherentes, según reflejan los resultados.	El aporte directo de esta investigación es seguir la Ley 1581 de 2012	Se presenta una debilidad por lo que se debe crear un modelo de protección de datos basado en la Ley 1581 de 2012
3. ¿Cuenta la Unidad con una estructura organizativa definida?	Existe una formalidad de cargos definida, ésta se cumple o y es conocida por los efectivos	Resulta relevante la asignación de responsabilidades y funciones según el modelo COSO y la Ley 1581 de 2012	Existe una fortaleza en la estructura organizativa
4. ¿Se coteja la salida de datos con información actualizada?	No se coteja oportunamente la salida de datos con información actualizada	Resulta muy importante la gestión y control adecuado de la salida de datos por ser uno de los procesos más determinantes a la hora de conseguir el éxito dentro de la entidad castrense.	Existe una desorganización visible en dicho ciclo, lo que revela que puede existir una ausencia de interrelación adecuada entre la información generada internamente y la actualización que necesitan otras unidades o personas externamente.
5.¿Se coteja la entrada de datos con información actualizada?	No se coteja oportunamente la entrada de datos con información actualizada	Resulta muy importante la gestión y control adecuado de la entrada de datos por ser uno de los procesos más	Existe una desorganización visible en dicho ciclo, lo que revela que puede existir una ausencia de

		determinantes a la hora de conseguir el éxito dentro de la entidad castrense.	interrelación adecuada entre la información
6. ¿Se supervisa la calidad de los datos recibidos?	A pesar que la actividad de supervisión existe, se visualiza que ésta no se cumple como deber ser o presenta fallas	La información que va a formar parte del proceso de tratamiento de datos, no debe estar desactualizada.	Debilidad para la organización ya que no se controla debidamente la calidad, debido a la informalidad con que se ejecuta.
7. ¿Se utilizan formatos de control adecuados al momento de proteger la información en el tratamiento de datos?	No existe un método de control, además en segundo término al no existir precisión en los formatos de control correspondientes	Un método de control debe ser registrado en la base de datos para que se utilice y que así permita manipular los datos de acuerdo a la información de personal interno y externo.	Se debe determinar la fiabilidad de los datos, a fin de valorar los riesgos a los que se exponen; constituyendo ambas premisas debilidades en el área descrita.
8. ¿Se cuenta con información actualizada sobre los datos existentes al momento de manipularlos?	No se cuenta con información actualizada sobre los datos existentes al momento de manipularlos	Resulta importante el apoyo en la toma de decisión en el área	Se deben mantener datos oportunos y confiables que resulten de interés a los diferentes niveles; por lo cual, constituye una debilidad para el control de datos.
9. ¿Se almacenan los datos sin adulteración de la información?	No se mantiene un nivel adecuado de almacenamiento sin adulteración o fallas en la información registrada	Se debe proteger los datos para evitar incongruencias, fallas, corrupción de datos.	Existe una debilidad organizacional
10. ¿Se le da un tratamiento adecuado a los datos públicos?	Sí se da un buen tratamiento a los datos públicos	Para la protección de los datos se debe generar la actualización respectiva, evitando así errores y omisiones.	Se percibe que la institución le está dando el tratamiento adecuado tanto a los datos semiprivados como a los públicos
11. ¿Se le da un tratamiento adecuado a los datos privados?	No se actualiza en forma oportuna la información relacionada con datos privados	Para la protección de los datos se debe generar la actualización respectiva, evitando	Se percibe que la institución posiblemente no le esté dando el tratamiento adecuado tanto a los

		así errores y omisiones..	datos privados como a los sensibles
12. ¿Se le da un tratamiento adecuado a los datos semiprivados?	Sí se le da el tratamiento adecuado a los datos semiprivados.	Es relevante actualizar en forma oportuna la información relacionada con datos sensibles.	Se percibe que la institución le está dando el tratamiento adecuado tanto a los datos semiprivados como a los públicos
13. ¿Se le da un tratamiento adecuado a los datos sensibles?	No se actualiza en forma oportuna la información relacionada con datos sensibles	Es relevante actualizar en forma oportuna la información relacionada con datos sensibles.	Se percibe que la institución posiblemente no le esté dando el tratamiento adecuado tanto a los datos privados como a los sensibles
14.¿El mando de la Unidad comunica estándares de conducta apropiados a los efectivos que ejecutan las actividades relacionadas al tratamiento de datos?	No se comunican estándares de conducta apropiados al personal que ejecuta las actividades del tratamiento de datos	Lo mandos intermedios deben reportar las irregularidades que se presenten a los mandos superiores.	Existe una debilidad en la comunicación que impide que el personal pueda reportar las irregularidades que se presenten a los mandos superiores.
15.¿Cuenta la Unidad Militar con personal capacitado para la protección de datos?	Sí se cuenta con personal capacitado para la protección de datos	Contar con personal con los conocimientos esperados para ejercer sus funciones es importante ya que constituye una ventaja competitiva que le permitirá a la organización poder trabajar en equipo	Se visualiza una fortaleza importante en este campo ya que se visualiza un grupo de efectivos capaces de llevar a cabo sus labores, por lo que se puede emprender planes para aprovechar ese talento
16. ¿Los objetivos en materia de control permiten la evaluación de riesgos relacionados con pérdidas de datos?	Los objetivos en materia de protección de los datos no permiten la evaluación de riesgos relacionados con pérdidas	Resulta relevante encaminar a la fuerza de trabajo para que desarrolle adecuadamente sus funciones	Existe una debilidad en materia de evaluación de riesgos relacionados con pérdidas
17.¿De ocurrir alguna omisión	De ocurrir alguna omisión respecto al	Resulta de importancia la	Se infiere que existe una debilidad en el área

respecto al tratamiento de datos, el personal encargado toma correctivos de inmediato?	proceso del tratamiento de la información, el personal encargado no toma correctivos de forma inmediata.	retroalimentación en la corrección de desviaciones	ya que no se corrigen desviaciones a tiempo para encauzar dichas actividades nuevamente hacia los objetivos propuestos.
18.¿La asignación de autorizaciones en la protección de datos están claramente definidas?	La asignación de autorizaciones en el proceso de protección de datos no está claramente definida	La no observancia de autorizaciones puede traer como consecuencia que no se obtenga la información relacionada en forma oportuna.	Existe una debilidad ya que no se establecen controles adecuados en los diferentes procesos del área lo cual puede traer como consecuencia que no se obtenga la información relacionada en forma oportuna.
19. ¿Se establecen evaluaciones periódicas del personal del área, concernientes a su desempeño?	No se establecen evaluaciones periódicas del personal del área concernientes a su desempeño;	Se debe establecer la descripción de las actividades basadas en la planificación, especificando también las responsabilidades y funciones estratégicas de cada cargo.	Existe una debilidad en las evaluaciones permanentes para la protección de datos
20.¿Existe segregación de funciones en el proceso relacionado con la protección de datos?	No existe segregación de funciones en el proceso relacionado con el tratamiento de la información.	Se debe establecer la descripción de las actividades basadas en la planificación, especificando también las responsabilidades y funciones estratégicas de cada cargo.	Se presenta debilidad en este indicador al no establecer responsabilidades del área de tal forma que en el proceso se garantice la seguridad en el tratamiento de los datos.
21. ¿Se utiliza el hardware adecuado para la generación de la información relacionada a la seguridad de los datos?	Sí existe el hardware adecuado para la generación de la información relacionada al proceso de la seguridad de los datos	Es importante el hardware adecuado para la generación de la información relacionada al proceso de la seguridad de los datos	Se determina que a pesar que la Unidad cuenta con el hardware y software necesario para el procesamiento de datos, los mismos no se aprovechan al máximo para generar reportes en forma oportuna y apoyar a la administración en el

			nivel de seguridad esperado.
22. ¿ Los sistemas de la Unidad generan la información oportuna relacionada con el proceso de seguridad de los datos?	Sí existe el software adecuado para la generación de la información relacionada al proceso de la seguridad de los datos	Es relevante el software adecuado para la generación de la información relacionada al proceso de la seguridad de los datos	Se determina que a pesar que la Unidad cuenta con el hardware y software necesario para el procesamiento de datos, los mismos no se aprovechan al máximo para generar reportes en forma oportuna y apoyar a la administración en el nivel de seguridad esperado.
23. ¿Se evalúa el proceso de la protección de datos?	No se evalúa el proceso de la protección de datos	Se debe supervisar constantemente el proceso de protección de datos para detectar errores	No se realiza una evaluación de los resultados obtenidos, constituyendo entonces una debilidad del proceso que debe ser afrontada.
24. ¿Se supervisa constantemente el proceso de seguridad en la gestión de datos para detectar errores?		Se debe supervisar constantemente el proceso de protección de datos para detectar errores	Las actividades de monitoreo y supervisión son llevadas a cabo a través de evaluaciones continuas, permitiendo determinar la calidad de las actividades de los diferentes procesos del área.

Nota. Investigación propia.

Modelo de Protección de Datos Personales en el Control de Acceso que Mediante Procedimientos Permita Asegurar la Integridad de la Información

Ciclo de las Etapas del Modelo de Protección de Datos

El modelo de protección de datos personales está estructurado en 5 fases o etapas, la descripción de cada una de éstas quedará plasmada en una guía que servirá como referencia para evaluar el adecuado cumplimiento de los principios establecidos en la Ley 1581 de 2012 tal como se muestra en la tabla visualizada a continuación.

Tabla 6

Ciclo De Las Etapas Del Modelo De Protección De Datos

Orden	Denominación
Etapa 1	Análisis situacional (Diagnóstico)
Etapa 2	Planeación
Etapa 3	Ejecución
Etapa 4	Análisis de riesgos
Etapa 5	Evaluación de gestión

Nota. Investigación propia.

Igualmente, se visualiza en la figura siguiente las etapas del modelo. En primer lugar, la fase de diagnóstico junto a la fase de planeación; en donde se identifican, clasificar validan e implementan los deberes. Consecuentemente, para llevar a cabo estas dos etapas se requiere investigar acerca de los procesos involucrados en los servicios prestados en la institución a fin de determinar si estos cumplen con el manejo adecuado de los datos

Seguidamente, se presenta la fase de ejecución; en donde se le da cumplimiento a la ley 158. Luego, está la fase de análisis de riesgo; se identifican las características de los riesgos que podrían tener mayor impacto. Por último, la fase de evaluación y mejora continua; trata la planeación y ejecución de auditorías internas o externas para validar el cumplimiento de los requisitos. Consecuentemente, las mismas deben tener una programación periódica donde se asegure el cumplimiento de las normativas de servicios y tecnológicos, procedimientos y políticas respectivas.

Figura 16

Fases del Modelo de protección de Datos

Nota. Elaboración propia.

Etapa 1 – Diagnóstico

Determinar y ordenar: para llevar a cabo esta etapa se requiere investigar acerca de los procesos involucrados en los servicios prestados en la institución a fin de determinar si estos cumplen con el manejo adecuado de los datos, siendo de vital importancia todo el procesamiento de la información que inicia con la recolección de los datos, su uso, almacenamiento, la transferencia y finalmente su eliminación, basado en lo establecido en el manual de Registro Nacional de Bases de Datos publicado por la SIC, tal como queda descrito en la tabla siguiente.

Tabla 7

Análisis de las Bases de Datos

Proceso operativo	Subproceso operativo	Identificación de la Base de Datos	Universo de usuarios	Propósito
Proceso operativo sistemático aplicado a la base de datos	Proceso operativo de menor escala aplicado en la base de datos	Denominación completa de la base de datos	Cantidad total de individuos registrados en la base de datos	Señale de forma resumida el objetivo para el cual fue desarrollada la base de datos, tomando en cuenta las cifras del campo anterior

Nota. Investigación propia.

Tabla 7

Análisis de las Bases de Datos (Continuación)

Regulación legal	Concordancia legal	Tipificación legal	Fecha de Emisión
Indique si está informado sobre una normativa distinta a la Ley 1581 de 2012 que establezca el tratamiento de la data recopilada en los sistemas de almacenamiento de datos	En caso de marcar afirmativamente el campo anterior, seleccione una de las opciones especificadas en el campo siguiente	En caso de haber marcado el campo anterior señale el artículo y numeral de la norma correspondiente	En caso de haber marcado el campo anterior señale la fecha en la que fue emitida la norma prenombrada

Nota. Investigación propia.

En la tabla anterior se pudo identificar la clase de bases de datos contenidas en el sistema, el propósito del tratamiento de dichos datos y la aplicabilidad de una normativa legal, que obliga a cumplir al ente responsable unos parámetros de tratamiento de la información pudiendo resultar en el almacenaje por un período predeterminado para su resguardo y fines futuros. Cabe mencionar que en esta etapa se inicia el ciclo de vida de los datos como fuente básica de información mediante su recolección y procesamiento.

Tabla 8

Descripción de mecanismos de procesamiento de bases de datos

Mecanismos de procesamiento de bases de datos			
Categorías de Bases de Datos	**Localización de las Bases de Datos (Medios automáticos)**	**País de ubicación del Servidor Externo**	**Localización de la Base de datos (Medios físicos)**
Marcar esta opción según si la base de datos se maneja de forma electrónica o física.	Marcar esta opción si en la columna anterior seleccionó el tipo de base de datos electrónica.	Marcar solo si usted señaló en la columna anterior la opción de Servidor Externo	Marcar esta opción solo si en la columna inicial denominada "Categoría de base de datos" se refiere a medio físico.
En caso de almacenarlas bajo ambas modalidades deben registrarse separadamente.	Se entiende como base de datos electrónica como aquella que se almacena sobre dispositivos electrónicos		Una base de datos física está representada en forma de manuales o archivos que se encuentran organizados y almacenados de forma física.

Nota. Investigación propia.

Tabla 8

Descripción de mecanismos de procesamiento de bases de datos (Continuación)

Mecanismos de procesamiento de bases de datos		
Sistema de gestión	**Almacenamiento**	**Objetivo de Almacenamiento**
Software o aplicación en el que se almacena la base de datos	Tiempo de almacenamiento de la información contenida en la base de datos, especificando la cantidad de años y meses correspondientes	Señalar el fin específico por el cual se almacena la información contenida en la base de datos

Nota. Investigación propia.

La tabla anterior permite determinar si la base de datos procesada se encuentra disponible en medios electrónicos o físicos y los datos de ubicación de su almacenamiento.

Tabla 9

Campos que conforman la base de datos

Campos que conforman la base de datos			
Tipo de usuario	Información general	Información de Identidad	Datos de localización
Seleccione una de las siguientes opciones: Empleado Cliente Proveedor Usuario Otro	Usar como referencia la Tabla de Criterios de Categorización de la Información presentada posteriormente para comparar los datos personales con los criterios de clasificación y verificar si coincide con las condiciones para ser como información de ámbito general	Usar como referencia la Tabla de Criterios de Categorización de la Información presentada posteriormente para comparar los datos personales con los criterios de clasificación y verificar si coincide con las condiciones para ser considerado como datos de identidad	Usar como referencia la Tabla de Criterios de Categorización de la Información presentada posteriormente para comparar los datos personales con los criterios de clasificación y verificar si coincide con las condiciones para ser considerado como datos de localización

Nota. Investigación propia.

Tabla 9

Campos que conforman la base de datos (Continuación)

Campos que conforman la base de datos		
Información confidencial	Área económica y social	Datos adicionales
Usar como referencia la Tabla de Criterios de Categorización de la Información presentada posteriormente para comparar los datos personales con los criterios de clasificación y verificar si coincide con las condiciones para ser considerado como información restringida al público	Usar como referencia la Tabla de Criterios de Categorización de la Información presentada posteriormente para comparar los datos personales con los criterios de clasificación y verificar si coincide con las condiciones para ser considerado como información socioeconómica	Usar como referencia la Tabla de Criterios de Categorización de la Información presentada posteriormente para comparar los datos personales con los criterios de clasificación y verificar si coincide con las condiciones para ser considerado como un dato adicional, que no pertenezca a las categorías anteriores

Nota. Investigación propia.

La tabla anterior sirve como instrumento para determinar el tipo de contenido de la base de datos según lo establecido en las distintas categorías definidas por la SIC.

Cabe destacar que la información presentada en esta tabla se sustenta en los aspectos plasmados posteriormente en la Tabla de Criterios de Categorización de la Información, por lo que debe ser usada como marco de referencia.

Tabla 10

Permisos concedidos por el propietario de la información

Permiso del propietario			
Posee el permiso del propietario de la información	Excepciones	Origen de los datos	Permiso
Marque esta opción si posee el permiso del propietario de la información para manejar sus datos personales	De ser No/Algunas veces Si marcó la opción anterior con la variable No o Algunas veces seleccione una de las respuestas siguientes: 1.De origen público 2.Proporcionada por terceras personas 3.Indicado por el propietario	En caso de marcar la opción "Posee permiso del propietario" seleccione una de las opciones siguientes	Si marcó la opción "Posee permiso del propietario" Indique el tipo de permiso utilizado

Nota. Investigación propia.

La tabla anterior muestra los criterios para reconocer si se cuenta con el permiso del propietario para manejar sus datos personales almacenados en la base de datos.

Tabla 11

Información sobre el encargado del tratamiento de los datos

Oficina administrativa		Persona encargada del procesamiento de datos				
Oficina administrativa	Nivel de acceso a la información	Identificación	Clase de documento	Documento de identidad	Origen	Dirección
Indique el nombre de la dependencia administrati-va	Marque el nivel de acceso a la información que posee el área operativa de acuerdo con el tipo de permiso que tiene habilitado	Marque en esta opción el nombre o razón social del encargado de procesar los datos	Indique el tipo de documento de identidad del encargado	Indique el número de documento de identidad del encargado	Seleccione en este campo el país del encargado	Indique la ubicación física del encargado

Nota. Investigación propia.

Tabla 11

Información sobre el encargado del tratamiento de los datos (Continuación)

Persona encargada del procesamiento de datos				
Departamento	Ciudad	Correo Electrónico	Teléfono fijo	Página Web
Indique el Departamento del encargado	Indique la ciudad de ubicación del encargado	Escriba la dirección de correo electrónico utilizada por el encargado de procesar los datos	Marque en esta opción el teléfono fijo con código de área y el número	Indique la página electrónica En caso de ser una excepción marque el tipo correspondiente

Nota. Investigación propia.

La tabla anteriormente presentada permite reconocer si en esa base de datos se almacena información relacionada con el permiso de manejo de datos personales.

Tabla 12

Transferencia Internacional/Categorización

Transferencia Internacional			Categorización
Procede a aplicar el traspaso de los datos hacia otros países En caso de poseer Declaratoria de Conformidad establecida por la SIC, indique el código de radicado	Opciones excluidas	Identificación del número de control de archivo o radicado	Categorización

Nota. Investigación propia.

La tabla anterior, permitió determinar si es procedente la aplicación de las transferencias internacionales de las bases de datos además de la categorización total de la información recolectada en las mismas. En este sentido es importante destacar que, para facilitar la categorización anteriormente indicada, se recomienda tomar como referencia la tabla siguiente, debido a que en esta se describen los atributos correspondientes a cada dato en particular procesado por la institución operante.

Tabla 13

Criterios de Categorización de la información proporcionada por el titular

CLASE	SUBCLASE	IDENTIFICACIÓN	CATEGORIZACIÓN Según Ley 1581:2012
Identidad personal	Información general	Nombres y Apellidos	Público
		Clase de documento de identidad	
		Número de documento de identidad	
		Fecha de emisión	
		Lugar de emisión	
		Género	
		Estado civil	
		Código de control de la licencia de conducir	Público
		Fecha de nacimiento	Público
		Lugar de origen	Público
		Fecha de fallecimiento	Restringido
		Lugar de fallecimiento	Restringido
		Código de tarjeta militar	Público
		Nacionalidad	Público
		Lugar de residencia	Público
	Información detallada	Datos de empleados/Socios (cónyuge/familiares ascendientes/otros)	Restringido
		Descendientes	Confidencial
		Carnet profesional	Público
		Número de pasaporte	Restringido
		Firma	Restricción media
		Firma electrónica	Restricción media
		Años cumplidos	Restringido
		Fotografía	Restringido
		Videos	Restringido
		Tono de Voz	Confidencial

Fuente. Investigación propia.

Tabla 13

Criterios de Categorización de la información (continuación)

CLASE	SUBCLASE	IDENTIFICACIÓN	CATEGORIZACIÓN Según Ley 1581:2012
Localización	Información de localización comercial	Localización de la oficina	Público
		Número de teléfono de la oficina	Público
		Correo electrónico de la oficina	Público
	Información de localización personal	Lugar de residencia	Restringido
		Número de teléfono de residencia	Restringido
		Correo electrónico personal	Restringido
		Localidad/Barrio	Restringido
		Teléfono móvil personal	Restringido
Información confidencial	Información sobre salud	Revisión médica/Parámetros de salud	Confidencial
	Información sobre Sanidad personal	Exámenes sicotécnicos	Confidencial
		Cifras de consultas domiciliarias	Confidencial
	Información sobre vinculaciones sociales o culturales	Información sobre tendencia política	Confidencial
		Información relativa al culto religioso o corrientes de pensamiento	Confidencial
		Asociado a grupos sindicales/Gremios	Confidencial
	Información sobre identidad de género y raza	Tendencia de género	Confidencial
		Información sobre su origen racial	Confidencial
	Condición social	Población en condiciones precarias	Confidencial
	Información sobre diversidad funcional	Datos sobre discapacidades	Confidencial

Nota. Investigación propia.

Tabla 13

Criterios de Categorización de la información proporcionada por el titular

(Continuación)

CLASE	SUBCLASE	IDENTIFICACIÓN	CATEGORIZACIÓN Según Ley 1581:2012
Área económica y social	Finanzas personales	Datos financieros y de créditos	Restricción media
	Información socioeconómica	Segmento social al que pertenece	Restringido
		Titularidad de la vivienda	Restringido
	Información tributaria	Datos fiscales	Restringido
	Información patrimonial	Propiedades y obligaciones del propietario	Restricción media
	Información sobre el giro económico del propietario	Datos de identificación bancaria	Restricción media
		Institución financiera en la que posee cuenta bancaria o inversión financiera	Restricción media
		Datos de las tarjetas de crédito	Restricción media
		Indicadores sobre el desempeño laboral de empleados bajo relación de dependencia/socios comerciales	Restringido
	Información Laboral	Fecha de ingreso	Restringido
		Clase de convenio laboral	Restringido
		Monto de Ingreso mensual	Restringido
		Período de duración del convenio laboral	Restringido
		Cargo desempeñado	Restringido
		Antecedentes laborales y referencias de trabajo	Restringido
	Información del Área Educativa	Nivel académico/Capacitaciones y Record de calificaciones	Restringido
	Sistema de Bienestar social	Datos de afiliación a la Seguridad social	Restringido
Datos adicionales	Información sobre seguridad de los datos	Claves de acceso a los sistemas informáticos	Confidencial
	Información sobre actividades de ocio y otros intereses	Aficiones/Actividades recreativas y culturales/Pasatiempos	Restringido
	Historial	Datos sobre antecedentes judiciales, participación en juicios, investigaciones penales, sanciones	Restringido

Nota. Investigación propia.

Etapa 2- Planeación

Posterior al análisis de la Etapa 1 con el fin de determinar las bases de datos que están de acuerdo con los criterios establecidos en el rol del Encargado de la información, es necesario verificar los deberes a cumplir por la institución, tal como se encuentra tipificado en la Ley 1581 de 2012 en el artículo 18 de los "Deberes del Encargado de la Información" y garantizar su adecuado cumplimiento, basado en las propuestas en el cuadro siguiente y desarrolladas posteriormente en la Etapa 3 de Ejecución.

Tabla 14

Artículo 18. Deberes de los Encargados de la Información

Deberes de los Encargados del Tratamiento Literal del Artículo	**Acciones propuestas**
a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;	Habilitar a los usuarios un proceso para formalizar consultas y solicitudes por inconformidad.
b) Preservar los datos bajo las condiciones de seguridad inherentes para obstaculizar su adulteración, pérdida, reunión, uso o acceso no autorizado o engañoso.	Se requiere verificar se lleven a cabo los principios de seguridad emanadas por el manual de RNBD
c) Efectuar en forma oportuna la actualización, enmienda o eliminación de los datos en los términos de la presente normativa;	Responder oportunamente a los requerimientos presentados a través del proceso de consultas y solicitudes por inconformidad.
d) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;	Supervisar que los requerimientos solicitados por los usuarios sean respondidos en el plazo correspondiente.
e) Tramitar las consultas y los reclamos formulados una vez informado por parte del responsable sobre procesos judiciales inherentes con la calidad del dato individual; por los Titulares en los términos señalados en la presente ley;	Supervisar que los requerimientos solicitados por los usuarios sean respondidos siguiendo los parámetros establecidos en la ley.
f) Poner en marcha un manual interno de lineamientos y procesos para avalar la pertinencia observancia de la presente normativa y, en especial, para el cuidado de consultas y reclamos por parte de los Titulares;	Anexar al manual interno de la institución, el apéndice relacionado con el tratamiento de datos personales, específicamente la información acerca de la responsabilidad como encargados de la información de los titulares.

Deberes de los Encargados del Tratamiento Literal del Artículo	Acciones propuestas
g) Registrar en la base de datos las leyendas "reclamo en trámite" en la forma en que se regula en la presente ley;	Aplicar la identificación de estatus tanto en las bases de datos almacenas en medios electrónicos como en físicos. Tal información se verifica en la bitácora de consultas y solicitudes por incorformidad.
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;	Aplicar la identificación de estatus tanto en las bases de datos almacenas en medios electrónicos como en físicos. Tal información se verifica en la bitácora de consultas y solicitudes por incorformidad.
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;	Se requiere verificar se lleven a cabo los principios de seguridad emanadas por el manual de RNBD.
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;	Se requiere verificar se lleven a cabo los principios de seguridad emanadas por el manual de RNBD
k) Notificar a la Superintendencia de Industria y Comercio cuando estén presentes transgresiones a los códigos de seguridad y existan peligros en la dirección de la información de los Titulares;	Emitir informe técnico confidencial al ente correspondiente cuando ocurra el siniestro o evento.

Nota. Investigación propia.

Etapa 3 Ejecución

Luego de desarrollar las acciones propuestas de acuerdo con lo establecido en la ley 1581 en su artículo18, se describen a continuación los pasos a seguir.

Documento de Consulta y Reclamos. Presentar consultas y solicitudes de inconformidad en el tratamiento de la información personal es un derecho de los propietarios de la información, razón por la cual puede solicitar al responsable del manejo de las bases de datos cualquier requerimiento que se le presente. En este sentido y en función del cumplimiento de la norma, se recomienda aplicar el proceso descrito en el cuadro siguiente, tomando en cuenta su estructura organizacional y recursos disponibles para tal fin.

Tabla 15

Registro cronológico de consulta y quejas

Registro cronológico de consulta y quejas

Medio de recepción de la solicitud	Fecha de la solicitud	Solicitud	Estatus de la solicitud	Verificación de validez	Fecha de solución de caso	Plazo de respuesta	Explicación	Identificación del solicitante	Rol de usuario	Información personal	Solución / decisión tomada
Indicar el medio por el cual se realizó la solicitud	Fecha exacta de recepción de la solicitud, indicando día, mes y año	Registra la solicitud específica que requiere el propietario de los datos	Indicar si se trata de una queja y registrar la leyenda respectiva	Verificar si es posible realizar la solicitud porque cumple los parámetros	Fecha en la que el propietario cerró la solicitud, indicando Día, mes y año.	Período de resolución del caso desde inicio hasta cierre	Explicación detallada del requerimiento presentado	Nombre del titular que realiza la solicitud	Descripción del rol de del propietario de la información si es candidato, colaborador, cliente, proveedor.	Descripción de los datos personales	Indicar de forma resumida las acciones tomadas y recomendadas para evitar posibles casos futuros

Nota. Investigación propia.

Previsiones de Seguridad de la Información

En el sentido de ajustarse a las recomendaciones emitidas por la SIC, se sugiere cumplir con las previsiones de seguridad previstas en el manual de RNBD. Cabe mencionar que la aplicación de tales medidas dependerá de los requerimientos, recursos y dinámicas propias de cada organización.

Tabla 16

Previsiones de Seguridad de la Información

No.	SEGURIDAD DE LA INFORMACIÓN PERSONAL	DESCRIPCIÓN	CONTROL ISO 27001	ACTA DE CONTROL SEGÚN LA BASE DE DATOS FÍSICA	ACTA DE CONTROL SEGÚN LA BASE DE DATOS ELECTRÓNICA
1	¿Emplea un formato de seguridad de la información general o personal?	Un formato de seguridad de la información personal es aquel que contiene los principios y/o políticas organizacionales, humanas y técnicas que se deben adoptar por todas las áreas de la empresa para proteger los datos personales, con el objeto de cumplir con la norma legal referida a la seguridad, específicamente en la Ley 1581 de 2012, tipificado en su Artículo 4, literal "g" y refiere el texto a continuación: *"Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias…"*			
2	¿Ha implementado procesos de evaluación en el ámbito de la seguridad de la información personal?	Se refiere a la existencia dentro de los procesos operativos el registro de actividades relacionadas con seguridad de la información que involucren datos personales.			

3	¿Aplica procedimientos de delegación de responsabilidades y autorizaciones en el tratamiento de la información personal?	Se refiere si ha desarrollado algún manual o documento en el que se establezca la designación de responsabilidad en cuanto al tratamiento de datos personales en cada una de sus etapas
4	¿Ha emitido acuerdos de confidencialidad con los empleados que poseen niveles de acceso a la información personal dentro de sus funciones laborales?	Define explícitamente en qué consiste el principio de Confidencialidad contemplado por la Ley 1581 de 2012, estableciendo: *"Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."*
5	¿Ejecuta controles de seguridad cuando el tratamiento de la información personal es delegado a terceras personas?	Se refiere a los procedimientos de verificación implementados en los procesos de tratamiento de datos que se realizan por medio de la contratación de terceros en vez de a colaboradores internos, les compete a los Encargados del tratamiento de datos personales.
B		
1	¿Utiliza herramientas de gestión de riesgos en el tratamiento de datos personales?	Se denominan Herramientas de gestión de riesgo al conjunto de sistemas, controles, instrumentos, metodologías, entre otras, empleados para facilitar la optimización de procesos operativos de la organización para evitar, disminuir o transferir las consecuencias negativas de las amenazas identificadas durante cada una de las fases del ciclo de vida del dato. El Encargado tiene la libertad de aplicar la herramienta o metodología de evaluación del riesgo que le convenga, de acuerdo con sus requerimientos y capacidades y además debe documentarse.
2	¿Emplea un sistema de gestión de seguridad de la información o un programa	Se entiende que un Sistema de Gestión de Seguridad de la Información o SGSI consiste en un conjunto de instrucciones y/o políticas administrativas, humanas y técnicas de manejo de la información.

	integral de gestión de datos personales?	El concepto es utilizado por diferentes estándares de calidad, principalmente por la ISO/IEC 27001. En lo que se refiere al Programa Integral de Gestión de Datos Personales PIGDP consiste en llevar a cabo de manera interna en la organización, las medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012. Para lo cual el Decreto 1074 en su sección 6 establece el principio de Responsabilidad en el tratamiento de datos personales, Mediante estos aplicativos la organización diseña, ejecuta y realiza mantenimiento a los procesos, logrando gestionar de forma óptima el acceso y utilización de la información personal, con base en los principios de la seguridad de la misma (confidencialidad, integridad y disponibilidad), para disminuir los riesgos asociados al tratamiento de la información.
C	**SEGURIDAD DE LA INFORMACIÓN PERSONAL RELACIONADO CON LOS RECURSOS HUMANOS**	
	¿Aplica controles de seguridad de la información personal para el personal que ingresa a la institución de forma previa y posterior a la culminación de la relación laboral	Se refiere a Políticas y medidas de control relacionados con el recurso humano que comienza a laborar en la organización y cuenta con acceso a la información personal, antes, durante y después al desempeño de las funciones asignadas. Para ejemplificar, pueden emitirse acuerdos de confidencialidad de la información, estudios de seguridad previos a la contratación, cierre y control para perfiles de acceso a la información una vez finalizada la relación contractual, etc.
D	**CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL**	
1	¿Mantiene una política de control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico?	Se requiere aplicar medidas de control que restrinjan el acceso a la información personal, tanto en el ámbito físico (directamente a las instalaciones) como el ámbito electrónico para los recursos informáticos.

		Establecer los niveles de acceso para definir quién tiene permisos sobre la información personal y cómo pueden utilizarla.
2	¿Tiene establecido algún procedimiento para la gestión de usuarios con acceso a la información personal?	Este aplicativo sirve como complemento del control de acceso a la información personal. Se refiere a las políticas para el control de los usuarios que poseen acceso a los datos personales con el fin de designar quién es el responsable de la seguridad en el acceso a los datos personales. Implica la creación de usuarios, autorizaciones, administrar las claves de acceso, notificaciones de seguridad, eliminación de perfiles de acceso, permisos, entre otros.
3	¿Ha implementado una política específica para el acceso a la información personal de las bases de datos que almacene información confidencial?	Se refiere a los lineamientos preestablecidos (generales o específicos) para controlar el acceso a la información personal, cuando esta sea de tipo confidencial, tomando en cuenta que su mal empleo puede ocasionar inconvenientes Dichas políticas deben regir tanto en el acceso físico como electrónico y deben contemplar los niveles de acceso
4	¿Ha establecido una política de respaldo de la información personal?	Se refiere a la existencia de un procedimiento en la organización que sirva de marco de referencia para resguardar de manera secundaria la información alojada en las bases de datos, permitiendo crear copias de seguridad en caso de contingencias, que se encuentre basada en los criterios dictados por la misma organización en relación con el almacenamiento de los datos.
5	¿Ha implementado una política de protección de datos específica para para el acceso de forma remota a la información personal?	Son las medidas de seguridad que deben aplicarse para garantizar que al activar una consulta, uso o extracción de la información de manera remota se maneje de manera totalmente confiable, es decir, cuando tales procesos se llevan a cabo desde dispositivos externos a la organización como consecuencia de la dinámica operativa de ciertas áreas, y le permiten agilizar sus actividades de consulta, promoción y venta, entre otras
E	**PROCESAMIENTO DE INFORMACIÓN PERSONAL**	
1	¿Ha establecido una política para el correcto tratamiento de la información personal durante las diferentes etapas del ciclo de vida del dato?	Se refiere a la determinación del rol de la persona encargada de procesar los datos en cada fase del ciclo de datos (recopilación, transferencia y descarte), por lo que se recomienda diseñar una matriz de riesgo de los datos personales, identificar en cada etapa los riesgos asociados. Posteriormente, se deben identificar los controles que se requieren para su gestión para garantizar el correcto tratamiento en cada etapa. En este sentido, se sugiere consultar la *Guía para la implementación del principio de*

		responsabilidad demostrada, que encuentra alojada en la página web de la SIC www.sic.gov.co .
2	¿Posee un procedimiento para la verificación de los datos procesados, que garantice que los datos recopilados sean correctos, ajustándose a parámetros como confirmación de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc.?	Está relacionado con la veracidad del dato, por tanto, es necesario minimizar el riesgo de error o ataques por inyección de código, utilizando técnicas de validación de los datos de entrada y procesamiento, confirmando previamente las condiciones
3	¿Cuenta con un control de seguridad de información para la validación de datos de salida?	Este control está relacionado con la veracidad e integridad del dato, las cuales se deben garantizar desde su recolección, procesamiento y busca tener resultados esperados. Los datos de salida se presumen están correctos. De la misma forma como en un reporte, la pertinencia de la información plasmada de acuerdo con la finalidad. Esta es una manera de controlar la veracidad, calidad y acceso no autorizado a la información.
4	¿Aplica una política para el intercambio físico o electrónico de datos (en el comercio electrónico para la compra y venta de productos o servicios), traslado y/o registro de información personal?	Se refiere a si existen medidas de seguridad que se apliquen para minimizar los riesgos asociados al intercambio de datos personales bien sea de manera física o electrónica, como interceptación, consulta no autorizada, fraude, pérdida o robo de la información
5	¿Tiene un procedimiento o control implementado para la disposición final de la información personal (supresión, archivo, destrucción)?	Una vez identificados los riesgos asociados al tratamiento de datos en cada una de las etapas, debe implementar controles coherentes que permitan decidir el destino final de la información, que puede ser eliminación (borrado seguro), destrucción o conservación, de manera que nunca se expongan los datos a un uso no autorizado o fraudulento que conlleve a la materialización de un riesgo tanto para el titular como para el responsable del tratamiento.
F	**SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL**	
1	¿Aplica un procedimiento que contemple la definición de	Es documentar los pasos y metodología utilizada en la definición de las necesidades identificadas antes, durante y posterior al desarrollo

	especificaciones y requisitos de seguridad de los sistemas de información personal?	de sistemas de información relacionados con el tratamiento de datos personales, en todo lo concerniente a seguridad de la información.
2	¿Implementa controles de seguridad de la información durante el mantenimiento (control de cambios) de los sistemas de información personal?	Se refiere a si existen controles implementados sobre la documentación que debe hacerse acerca de los que requieran los sistemas de información en general o específicamente aquellos que incluyen el tratamiento de datos personales.
3	¿Posee un procedimiento implementado de auditoría de los sistemas de información personal?	Indicar si tiene procedimientos automatizados que permitan evaluar la eficiencia y suficiencia de los controles implementados a un sistema de información mediante el cual se traten datos personales para evitar su pérdida, uso o acceso no autorizado o fraudulento, de manera que se garantice la disponibilidad, integridad y confidencialidad de los datos personales.
4	¿Las bases de datos con información personal poseen Monitoreo de consulta?	Permite hacer seguimiento de cualquier consulta que realice sobre la base de datos con información personal. Lo cual se definirá dependiendo del riesgo a que esté expuesta esta información y la naturaleza de los datos que se estén tratando.
G	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL**	
1	¿Posee una política y procedimientos de gestión de Incidentes de seguridad de la información personal?	Un Incidente de seguridad de datos personales se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de datos personales bien sea en manos del responsable del Tratamiento o de su Encargado, en este sentido, se refiere a la documentación de los pasos a seguir una vez se detecte la existencia del incidente, tanto a nivel correctivo como preventivo, estableciendo claramente los plazos, roles y responsabilidades involucrados.
2	¿Ha aplicado una política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados?	Una vez se han determinado las causas e impacto del incidente detectado relacionado con datos personales, es importante identificar oportunidades de mejora e implementar controles que redunden en la prevención de la ocurrencia de otros hechos relacionados con las vulnerabilidades detectadas.
H	**AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL**	

1	¿Tiene una política que regule el proceso control mediante auditorías de seguridad de la información personal?	Indicar si tiene documentada una política de auditoría de seguridad de la información personal o en general, que permita evaluar el cumplimiento, resultados y la documentación de acciones correctivas y/o preventivas, relacionadas con el tratamiento de datos personales.
	¿Dentro de las auditorías aplicadas a la seguridad sobre información personal, considera el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos?	Indicar si tiene implementada una política de auditoría de seguridad de la información personal o en general, que permita evaluar el cumplimiento, resultados y la documentación de acciones correctivas y/o preventivas, sobre tratamiento de datos personales, donde sea posible evaluar el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos con información personal que está registrando.

Nota. Investigación propia.

Manual interno de Protección de Datos Personales

Con el fin de dar cumplimiento al literal “f” de la ley 1581 de 2012 en su artículo 18, se sugiere incluir los siguientes temas en el Manual interno de la organización:

- Procedimiento de consultas y quejas.
- Procedimientos aplicados para la gestión de incidentes.
- Campaña de sensibilización.
- Proceso de auditoría de seguridad de la información personal que permita evaluar el cumplimiento, el desempeño y registro de acciones correctivas y/o preventivas, relacionadas con el tratamiento de información personal.
- Proceso de control para la disposición final de la información personal (archivo o eliminación)
- Procedimientos de delegación de responsabilidades.
- Control de acceso a la información personal tanto en las instalaciones físicas como en el ámbito digital.
- Procedimiento de respaldo de la información personal.
- Proceso que regule el acceso remoto a la información personal.
- Proceso para el tratamiento de la información durante sus fases específicas de recopilación, utilización, almacenamiento, transferencia y eliminación.
- Procedimiento de verificación de datos de entrada y tratamiento de la información personal, que garantice que sean correctos y apropiados.
- Proceso para la verificación de datos de salida.

Acta de Cumplimiento Modelo - Basada en los Documentos Oficiales Publicados por la SIC en su página WEB

Aunque la SIC no ha publicado documentos orientadores que funcionen como guía formal y vinculante para el cumplimiento de la ley 1581 de 2012, en el ámbito relativo al rol de encargado de la información, hemos tomado en cuenta las dos guías publicadas por este organismo previamente.

Tabla 17

Cuestionario Diagnóstico para el Cumplimiento ley 1581 de 2012

Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las MIPYMES	
PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES	**SI/NO**
Se recolecto información personal con fines legítimos y se informa al titular al respecto de este propósito	
Se cuenta con el consentimiento para tratar los datos del titular del cual se recolecta información.	
Si hay casos en los que se recolecta o información personal sin el consentimiento de los titulares, existe un mandato legal o judicial que habilite a organización para hacerlo	
Se conserva información personal veraz, completa, exacta, actualizada, comprobable y comprensible.	
Se cuenta con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a la información personal para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.	
Se garantiza la confidencialidad de la información por las personas de la organización que interviene en el tratamiento de datos personales, incluso después de que han finalizado si relación con alguna de las labores desempeñadas.	
TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD	**SI/NO**
Se cuenta con autorización explícita de los titulares para el tratamiento de sus datos confidenciales	
Se informa al titular que por tratarse de datos confidenciales puede negarse a revelarlos y no autorizar su tratamiento	
Se informa al titular cuáles de los datos serán objeto de tratamiento en su organización son sensibles y para qué finalidad(es) se utilizan	
Se efectúa tratamiento de datos personales de menores de edad únicamente para actividades que responden y respetan al principio de interés superior	
En el tratamiento de datos personales de menores de edad se asegura el respeto de sus derechos fundamentales establecidos en la ley	

Se cuenta con la autorización del representante legal del menor de edad para el tratamiento de sus datos	
DERECHOS DE LOS TITULARES DE LA INFORMACIÓN	**SI/NO**
Se permite el ejercicio del derecho de los titulares a conocer, actualizar y rectificar los datos personales que recolecta	
Se contesta a las solicitudes presentadas por los titulares dentro del plazo previsto en la ley general de protección de datos personales	
Se entrega a los titulares copias de la autorización otorgada por ellos para el tratamiento de sus datos personales cuando así lo solicitan.	
Se informa a los titulares qué uso les ha dado la organización a sus datos personales cuando así lo solicitan	
Se permite a los titulares el acceso gratuito a los datos personales que han sido objeto de tratamiento al menos una vez cada mes calendario y cada vez que se hagan modificaciones sustanciales a la política de tratamiento de la información.	
AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES	**SI/NO**
Se cuenta con la autorización para el tratamiento de los datos por parte de los titulares	
Se conocen los casos en los que no es necesario contar con autorización de los titulares para el tratamiento de su información personal	
Se cuenta con procedimiento efectivos y eficientes para solicitar, en el mismo momento de la recolección de los datos personales, las autorizaciones de los titulares para el tratamiento de estos	
Se informa a los titulares qué datos personales serán recolectados y todas las finalidades específicas del tratamiento para las cuales la organización obtiene el consentimiento	
Se obtiene nuevas autorizaciones de los titulares, cuando la organización realiza cambios sustanciales en las políticas de tratamiento de información personal	
Se establecen mecanismos que garantizaran la consulta posterior de la autorización otorgada por los titulares para el tratamiento de sus datos personales	
Se ponen a disposición de los titulares mecanismos gratuitos y de fácil acceso para presentar solicitudes de supresión de datos o la revocación de la autorización otorgada	
INFORMACIÓN MÍNIMA A LOS TITULARES	**SI/NO**
Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, el tratamiento al cual serán sometidos los mismos y la finalidad.	
Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, el carácter facultativo de la respuesta a las preguntas que se hacen, cuando se relacionan con datos sensibles a datos de niñas, niños y adolescentes.	
Se informa de manera clara a los titulares, los derechos que poseen, en el momento de solicitar la autorización para el tratamiento de datos personales	

Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono de responsable del tratamiento	
Se conserva prueba de haber informado a los titulares lo mencionado anteriormente	
SUMINISTRO DE LA INFORMACIÓN PERSONAL	**SI/NO**
La información personal que se suministra al titular o a quien éste autorice es de fácil lectura, sin barreras técnicas que impidan su acceso y corresponde en un todo a aquella que reposa en la base de datos	
Se suministra únicamente información personal a los titulares, sus causahabientes o sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y a los terceros autorizados por el titular o por la ley	
ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES	**SI/NO**
Se cuenta con canales o mecanismos sencillos y ágiles y que estén permanentemente habilitados para la atención de las consultas y reclamos de los titulares o sus causahabientes	
Se dan a conocer a los titulares e interesados los canales habilitados para la atención de consultas y reclamos en la política de tratamiento de datos personales dispuesta por la organización	
Se atiende, dentro de los diez (10) días hábiles contados a partir de su recibo, las consultas de información personal presentadas por los titulares, sus causahabientes y las personas autorizadas	
Se informa a los peticionarios el motivo de la no atención oportuna a su consulta de información personal y se señala la fecha de respuesta de la solicitud, sin exceder el término de cinco (5) días adicionales a los (10) días iniciales para contestar	
Se atiende, dentro de los diez (15) días hábiles contados a partir de su recibo, las reclamaciones presentadas por los titulares o sus causahabientes que consideran que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley.	
Se informa a los peticionarios el motivo de la no atención oportuna a su reclamo y se señala la fecha de respuesta de la solicitud, sin exceder el término de ocho (8) días adicionales a los quince (15) días iniciales para contestar.	
Se adoptan medidas para asegurar que los datos personales que reposan en las bases de datos sean precisos y suficientes y, cuando así lo solicite el titular o cuando haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento	
Se ha designado a una persona a área para que asume la función de protección de datos personales y dé trámite a las solicitudes de los titulares para el ejercicio de sus derechos	
Se da a conocer a los titulares los procedimientos dispuestos por la organización para el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, y los mismos son fácilmente accesibles.	

Se incluye dentro de la política de tratamiento de datos personales los procedimientos dispuestos para garantizar el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización

Se cuenta con un manual interno de políticas y procedimientos para garantizar la atención de consultas y reclamos presentados por los titulares y para garantizar, en general, el adecuado cumplimiento de la ley

Se han adoptado procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto de tratamiento de sus datos personales

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES	**SI/NO**
Se cuenta con una política para el tratamiento de los datos personales	
La política para el tratamiento de datos personales consta en medio físico o electrónico, en un lenguaje claro y sencillo, y es puesta en conocimiento de los titulares	
Se cuenta con una política para el tratamiento de los datos personales que incluye el nombre o razón social, domicilio, dirección, correo electrónico y teléfono de la organización.	
La política para el tratamiento de datos adoptada por la organización incluye información sobre el tratamiento al cual serán sometidos los datos personales y la finalidad de este.	
Incluye la política para el tratamiento de datos personales información sobre los derechos que le asisten a los titulares respecto de su información personal	
Se informa en la política para el tratamiento de datos personales sobre la persona o área responsabilidad de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.	
Se indica en la política para el tratamiento de datos personales cuál o cuáles son los procedimientos para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización	
En la política para el tratamiento de datos personales está incluida la fecha de entrada en vigor y el periodo de vigencia de la o las bases de datos que tiene la organización.	

AVISO DE PRIVACIDAD	**SI/NO**
Se informa a los titulares la existencia de la política para el tratamiento de datos personales por medio de un aviso de privacidad	
El aviso de privacidad publicado por la organización incluye el nombre o razón social y los datos de contacto de esta	
En el aviso de privacidad publicado se incluye la descripción del tratamiento al cual serán sometidos los datos personales recolectados y la finalidad de tal recolección	
El aviso de privacidad incluye un listado de los derechos que tienen los titulares cuya información es recolectada por la organización	
Se informa a los titulares en el aviso de privacidad publicado, cómo acceder o consultar la política de tratamiento de datos personales dispuesta por la organización	

En el aviso de privacidad publicado se señala expresamente la facultad que tienen los titulares de contestar o no las preguntas que versen sobre datos personales sensibles o sobre los datos de niños, niñas y adolescentes.

Se conserva el modelo de aviso de privacidad utilizado para cumplir con la obligación legal de dar a conocer las políticas de tratamiento de la información personal

REPORTE DE VIOLACIONES A LOS CÓDIGOS DE SEGURIDAD **SI/NO**

Informa a la Superintendencia cuando se presentan violaciones a los códigos de seguridad que generen riesgos en la administración de la información de los titulares

GESTIÓN DE ENCARGADOS DEL TRATAMIENTO **SI/NO**

Se han establecidos procedimientos internos para asegurar que los Encargados del tratamiento garanticen la protección de los datos personales que le son entregados y que su tratamiento se haga acorde con los principios y deberes establecidos en la ley

Se suscriben contratos con los Encargados que incluyen expresamente el tratamiento que éste podrá realizar a los datos personales

Se suscriben contratos con los Encargados que incluyen cláusulas de confidencialidad de la información entregada

Se exige a los encargados tener y mantener políticas de seguridad de la información y de tratamiento de datos personales antes de entregar las bases de datos

Se informa al encargado de forma oportuna todas las novedades respecto de los datos que previamente le fueron suministradas
Se cuenta con medidas necesarias para que la información suministrada al encargado se mantenga actualizada

Se comunica al encargado cuando se ha rectificado la información incorrecta

Se comunica al encargado si determinada información se encuentra en discusión por parte del titular, una vez éste presenta una reclamación y no ha finalizado el trámite respectivo

Se verifica que el encargado actualice y rectifique la información personal en los términos legales.

TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES **SI/NO**

Se transfieren datos personales a países que garantizan niveles adecuados de protección de datos, según lo establecido en el numeral 3.2 de capítulo tercero del título V de la circular única de la Superintendencia de Industria y Comercio

Se han implementado medidas a apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que se transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia

Se transfieren datos personales fuera del territorio colombiano con base en alguna de las causales de excepción establecidas en el artículo 26 de la ley 1581 de 2012

Se transfiere datos personales fuera del territorio colombiano con base en una declaración de conformidad emitida por esta Superintendencia

Se han suscrito contratos con los responsables del tratamiento destinatarios de los datos personales a transferir fuera del territorio colombiano o se implementan otros instrumentos jurídicos en los que se señalen las condiciones que regirán la transferencia

Internacional de datos personales, mediante las cuales se garantizará el cumplimiento de los principios que rigen el tratamiento, así como de las obligaciones que tienen a cargo

Se transmiten datos personales fuera del territorio colombiano a un encargado para que realice el tratamiento indicado por la organización como responsable del tratamiento y para ello han suscrito contratos de transmisión de datos personales en los que se señalen los alcances del tratamiento, las actividades que el encargado realizará y obligaciones de este respecto de los titulares y el responsable.

Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado cláusulas mediante las cuales este se compromete a dar aplicación a las obligaciones del responsable bajo su política de tratamiento de la información y a realizar el tratamiento de datos de acuerdo con la finalidad que los titulares han autorizado y con las leyes aplicaciones

Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación de dar tratamiento, a nombre del responsable, a los datos personales conforme a los principios establecidos en la ley general de protección de datos personales

Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de salvaguardar la seguridad de las bases de datos que contengan datos personales

Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de guardar confidencialidad respecto del tratamiento de los datos personales

RESPONSABILIDAD DEMOSTRADA **SI/NO**

Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a la naturaleza jurídica de la organización y su tamaño empresarial

Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a la naturaleza de los datos personales objeto del tratamiento

Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional al tipo de tratamiento que realice con los datos personales

Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a los riesgos potenciales que el tratamiento podrías causar sobre los derechos de los titulares

Se conserva evidencia sobre la implementación efectiva de medidas de seguridad apropiadas para el cumplimiento del régimen de protección de datos personales

Se han adoptado mecanismos internos para poner en práctica las políticas establecidas en los que se incluyan herramientas de implementación, entrenamiento y programas de educación en materia de protección de datos personales

REGISTRO NACIONAL DE BASES DE DATOS **SI/NO**

Se han registrado las bases de datos con información personal de la organización en el Registro Nacional de Bases de datos (RNBD) administrado por la Superintendencia de Industria y comercio	

Nota. Superintendencia de Industria y Comercio (2020).

Tabla 18

Responsabilidad Demostrada

Compromisos de la organización **DESDE LA ALTA DIRECCIÓN**	**SI/NO**
Se cuenta con el compromiso de la organización para la implementación de un programa integral de gestión de datos personales	
Existe en la organización una cultura de respeto a la protección de los datos personales que se recogen o tratan	
Se han comprometido recursos económicos y de personal en la organización, acorde a su tamaño y estructura, así como al tipo de información a la que se le realiza Tratamiento, para la implementación del Programa Integral de Gestión de Datos Personales	
Se cuenta con el apoyo y compromiso de la Alta Dirección para generar una cultura organizacional de respeto a la protección de datos personales	
La Alta Dirección de la organización designó a la persona o área que asumirá la función de protección de datos dentro de la organización	
La Alta Dirección de la organización aprobó el Programa Integral de Gestión de Datos Personales	
La Alta Dirección de la organización realiza un monitoreo del Programa Integral de Gestión de Datos Personales.	
La Alta Dirección de la organización informa de manera periódica a los órganos directivos sobre la ejecución del programa Integral de Gestión de Datos Personales	
La Alta Dirección de la organización destina recursos suficientes al área o persona encargada de diseñar e implementar el Programa Integral de Gestión de Datos Personales para desempeñar sus funciones.	
A través del área o persona encargada de diseñar e implementar el Programa Integral de Gestión de Datos Personales se establecen las responsabilidades específicas para otras áreas de la organización respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se tratan.	
OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	**SI/NO**
Se cuenta con una persona o área que asume la función de protección de datos personales y que da trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015.	
Se cuenta con una persona o área que vele por la implementación efectiva de las políticas y procedimientos adoptados por la organización para cumplir las normas de protección de datos personales.	
Se cuenta con una persona o área que establezca los controles del Programa Integral de Gestión de Datos Personales, así como la evaluación y revisión permanente de dichos controles.	
La persona o área que asume la función de protección de datos personales ha promovido la elaboración e implementación de un sistema que permita administrar los riesgos del Tratamiento de datos personales.	
La persona o área que asume la función de protección de datos personales sirve de enlace y coordina las demás áreas de la organización para asegurar la implementación transversal del Programa Integral de Gestión de Datos Personales.	
La persona o área que asume la función de protección de datos personales impulsa dentro de la organización una cultura de protección de datos.	

La persona o área que asume la función de protección de datos personales mantiene un inventario de las bases de datos personales en poder de la organización y las clasifica de acuerdo con su tipo.	
La persona o área que asume la función de protección de datos personales ha solicitado la declaración de conformidad de las operaciones de transferencia internacional de información personal ante la Superintendencia, cuando ha sido requerida, de conformidad con las instrucciones impartidas por esa entidad.	
La persona o área que asume la función de protección de datos personales revisa los contenidos de los contratos de transmisiones internacionales de datos, suscritos por la organización con los Encargados del Tratamiento no residentes en Colombia.	
La persona o área que asume la función de protección de datos personales ha diseñado un programa de entrenamiento en protección de datos personales acorde con las responsabilidades de cada cargo de la organización.	
La persona o área que asume la función de protección de datos personales realiza un entrenamiento general a todos los empleados y colaboradores de la compañía en protección de datos personales.	
La persona o área que asume la función de protección de datos personales realiza un entrenamiento a los nuevos empleados o colaboradores de la organización que, por las condiciones de su empleo, tengan acceso a los datos personales que se gestionan al interior de esta.	
La persona o área que asume la función de protección de datos personales integral las políticas de protección de datos personales dentro de las actividades de las demás áreas de la organización.	
La persona o área que asume la función de protección de datos personales mide la participación de los empleados y colaboradores en los entrenamientos en protección de datos y califica su desempeño.	
La persona o área que asume la función de protección de datos personales requiere que se complete satisfactoriamente el entrenamiento en protección de datos personales para realizar el analista del desempeño de los empleados y colaboradores.	
La persona o área que asume la función de protección de datos personales acompaña y asiste a la organización en la atención de las visitas y requerimientos realizados por la Superintendencia de Industria y Comercio.	
La persona o área que asume la función de protección de datos personales realiza seguimiento al Programa Integral de Gestión de datos personales.	
PRESENTACIÓN DE INFORMES	**SI/NO**
Se cuenta con planes de auditoría interna para verificar el cumplimiento de las políticas de Tratamiento de datos personales y señalar el procedimiento a seguir en caso de que se presenten violaciones a los códigos de seguridad o se detecten riesgos en la administración de la información personal de los Titulares.	
De define la estructura de la generación de reportes en la que se establezca qué empleado o persona genera qué tipo de reporte y se asignan responsabilidades claras ante una queja de los Titulares o una violación a los códigos de seguridad.	
Se documenta el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.	

Se generan reportes para los accionistas o socios de manera periódica y se informa a estos el estado del Programa Integral de Gestión de Datos Personales.	
CONTROLES DEL PROGRAMA	
PROCEDIMIENTOS OPERACIONALES	**SI/NO**
Se cuenta con procedimientos administrativos consistentes con las políticas generales de protección de datos personales y con las disposiciones legales vigentes, para manejar adecuadamente los riesgos inherentes al Tratamiento de datos personales dentro de la gestión operacional.	
INVENTARIO DE BASES DE DATOS CON INFORMACIÓN PERSONAL	**SI/NO**
Se tienen identificadas e inventariadas las bases de datos dentro de la organización.	
Se tiene claridad sobre el medio en el que se conservan las bases de datos al interior de la organización (manual o automatizado). Se tiene claridad de cuántos Titulares o personas naturales existen en cada base de datos.	
Se tiene identificado qué tipo de datos personales reposan en cada base de datos (datos de identificación, datos de ubicación, datos sensibles, datos de contenido socioeconómico, etc.)	
Se tiene establecido claramente para qué se utiliza cada base de datos y si realmente los datos que allí reposan son necesarios, teniendo en cuenta la finalidad para la que se recolectan.	
Se han identificado cómo se obtienen los datos personales en la organización, si se debe solicitar la autorización de los Titulares para obtener esos datos y, de ser así, sí se conserva prueba de tal autorización para su posterior consulta.	
Se informa a los Titulares la finalidad de la recolección de sus datos personales y el Tratamiento al que tales datos serán sometidos, así como los derechos que tienen como titulares.	
Se protege la calidad de la información personal al momento de su recolección.	
Si se recolectan datos de menores de edad, se han imprentado medidas adecuadas para garantizar una protección reforzada de dicha información.	
Si se recolectan datos menores de edad, la organización informa al Titular o a quien corresponda (tutores o representantes de los menores), que no existe obligación de suministrar tales datos.	
Se ha identificado qué áreas de la organización utilizan los datos personales y de qué forma los utilizan.	
Se han implementado medidas de seguridad para tratar y conservar los datos personales recolectados.	
Se han implementado procedimientos para actualizar, rectificar y depurar los datos personales en las bases de datos.	
Se entregan o comparten las bases de datos con información personal a terceros ubicados dentro o fuera del país.	
Se ha identificado para qué entregan o comparte las bases de datos con información personal con terceros dentro o fuera del territorio nacional.	

Se ha identificado por cuánto tiempo se conservan los datos personales y qué medios se utilizan para su disposición final (archivo físico, digitalización, eliminación, etc.)	
Se cuenta con medidas técnicas que garanticen la seguridad de los datos personales una vez se ha definido cuál será su disposición final.	
POLÍTICAS	**SI/NO**
Se cuenta con políticas internas debidamente documentadas e implementadas que incluyan las obligaciones señaladas en la Ley de protección de Datos Personales y se dan a conocer a los empleados o colaboradores.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la recolección o recopilación, el mantenimiento, uso y eliminación o disposición final de los datos personales.	
Se cuanta con procedimientos debidamente documentados e implementados que establezcan los requisitos para obtener la autorización de los Titulares.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la conservación y eliminación de información personal.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para el uso Responsables de la información, incluyendo controles administrativos, físicos y tecnológicos que garanticen la seguridad de la información.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la inclusión en todos los medios contractuales de la institución de una cláusula de confidencialidad y de manejo de información, donde se afirme que se conoce la política de la institución, se acepta, y se permite a la compañía utilizar dicha información de forma Responsable.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la presentación de quejas, denuncias y reclamos por parte de los Titulares y la forma de tramitarlas y atenderlas de manera adecuada, congruente y oportuna.	
Se incluye en las políticas de la organización, diferentes a la de protección de datos personales (talento humano, contratos, transparencia, etc.), elementos que permitan cumplir las normas sobre protección de datos.	
SISTEMA DE ADMINISTRACIÓN DE RIESGOS	**SI/NO**
Cuenta con un sistema de administración de riesgos, acorde con la estructura organizacional, los procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases de datos y los tipos de datos personales tratados por la institución, que le permita identificar, medir, controlar y monitorear aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos los datos personales.	
Se ha identificado a qué riesgos se ven expuestos los datos personales a los que se realiza Tratamiento al interior de la organización (ej.: riesgo de pérdida o fuga de información, riesgo de mantener información desactualizada o no veraz, riesgo de acceso indebido a la información, etc.).	
Se ha determinado la posibilidad de ocurrencia de los riesgos identificación y el impacto que podría ocasionar la materialización de estos, tanto para los Titulares como para la organización.	

Se ha establecidos qué acciones se deben tomar para controlar y/o mitigar los riesgos identificados, con el fin de disminuir la posibilidad y/o el impacto de la materialización de dichos riesgos.	
Los controles establecidos son suficientes, efectivos y oportunos para disminuir la posibilidad y/o el impacto de la materialización de los riesgos.	
Se realiza seguimiento constante para velar porque las medidas adoptadas sean efectivas	
Se realiza una evaluación de riesgos constante en la organización y desde el diseño en cada proyecto en él se involucre el Tratamiento de datos personales.	
FORMACIÓN Y EDUCACIÓN	**SI/NO**
Se tiene implementado un programa de capacitación para los empleados y contratistas de la organización en materia de protección de datos personales.	
Se realizan jornadas de capacitación al personal en materia de protección de datos personales, con periodicidad.	
Las capacitaciones realizadas a los empleados, contratistas y colaboradores en general de la organización involucrados directamente en las actividades de Tratamiento de datos personales se adaptan específicamente a las funciones, obligaciones y tareas que tienen a cargo.	
Existen dentro de los contratos suscritos por los empleados de la organización acuerdos de cumplimiento de las políticas internas desarrolladas por esta para el adecuado Tratamiento de los datos personales.	
PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES DE SEGURIDAD	**SI/NO**
Se cuenta con un procedimiento documentado e implementado y una persona o área encargada de manejar los incidentes o violaciones a los sistemas de información donde se gestionan datos personales y a los archivos físicos.	
Los empleados y contratistas de la organización tienen conocimiento sobre qué hacer antes, durante y después de que se presente un incidente de seguridad.	
Dentro del protocolo de incidentes de seguridad adoptado por la organización está previsto reportar a la Superintendencia de Industria y Comercio la ocurrencia de tales incidentes.	
Se cuenta con mecanismos, herramientas o procedimientos para la elaboración de informes internos y para informar tanto a los Titulares como a la Superintendencia de Industria y Comercio cuando se presenten incidentes de seguridad que involucren datos personales.	
Se cuenta con mecanismos, herramientas o procedimientos que permitan, además de informar a los Titulares la ocurrencia de un incidente de seguridad con sus datos personales y las posibles consecuencias, dar a conocer opciones o alternativas a dichos Titulares para minimizar el daño potencial o el daño causado.	
GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES.	**SI/NO**
Se han implementado medidas para asegurar la protección de los datos personales cuyo Tratamiento es realizado por los Encargados.	
Los contratos suscritos con los Encargados del tratamiento incluyen requisitos para que estos cumplan las normas colombianas de protección de datos y las políticas de Tratamiento de la información adoptadas por la organización.	
Se cuenta con mecanismos para que los Encargados reporten a la organización los incidentes de seguridad de la información que se presentan.	
Se verifica si los Encargados del Tratamiento de la información personal cuentan con política de Tratamiento de datos personales y programas de formación o educación en temas de protección de datos para sus empleados.	
Se exige la realización de auditoría internas y/o externas a las actividades desarrolladas por el Encargado del Tratamiento.	
Existen acuerdos con los Encargados y sus empleados o colaboradores aceptando que cumplirán con las políticas y protocolos de Tratamientos de datos de su organización.	
Se exige a los Encargados que utilizan subcontratistas que se establezcan obligaciones para éstos de adherencia a las políticas de Tratamiento de la organización.	

Nota. Superintendencia de Industria y Comercio (2020).

Etapa 4. Evaluación de Riesgos

Identificación Riesgos, Amenazas y el Estado de la Protección de Datos Personales de la Organización. A medida que aumenta el nivel de conciencia con respecto a los riesgos del manejo de datos personales, también aumentan las medidas de seguridad tomadas para garantizar su protección. En este sentido, cabe destacar que la supresión total del riesgo no es posible, sin embargo, aplicando el modelo de la mejora continua se pueden minimizar hasta hacerlos aceptables para la organización.

Esta etapa, tiene como propósito determinar el efecto de los riesgos sobre la protección de los datos personales, con el fin de tomar decisiones que faciliten el control de los riesgos más relevantes. A continuación, podemos observar en la tabla siguiente, las fases del proceso continuo de gestión de los riesgos en la protección de datos personales.

Tabla 19

Fases del proceso continuo de gestión de los riesgos

Ref.	DESCRIPCIÓN DE LA FASE
1	Determinar los riesgos
2	Análisis de los riesgos
3	Manejo de riesgos
4	Seguimiento de control

Nota. Elaboración propia.

Determinar riesgos. Los riesgos son susceptibles a cambiar y dependen de la exposición a amenazas presentes en la actividad de tratamiento, por esta razón, es de gran importancia disponer de una descripción detallada del tratamiento, los aspectos más relevantes que intervienen y su contexto. Cabe destacar que en esta etapa es necesario identificar los activos de información que conforman la protección de datos personales tal es el caso de la información

propiamente dicha, así como los activos de soporte en los que se almacenan, procesan y protegen dicha información.

La presencia del riesgo es una consecuencia de estar expuesto a amenazas, por esta razón, es fundamental determinar los que actúan sobre los datos personales tomando en cuenta en cuenta los siguientes criterios:

- El riesgo inherente a cada dato particular de acuerdo a su tipología.
- El nivel de desarrollo de la infraestructura tecnológica
- Las consecuencias de la presencia de una amenaza que pueda generar un daño para los titulares de los datos personales.

Adicionalmente, se deben considerar los siguientes aspectos:

- La cantidad de titulares;
- Los incidentes ocurridos previamente en los sistemas de gestión;
- Otros factores que puedan afectar la evaluación del riesgo o que se generen como consecuencia de nuevas regulaciones.

Evaluar los riesgos. La evaluación de riesgos consiste en analizar la probabilidad de ocurrencia de un evento y su impacto directo, en este sentido, para medir el impacto se debe considerar los posibles daños que se pueden producir si una amenaza se materializa. Para realizar la evaluación de riesgos es necesario definir las escalas cuantitativas y/o cualitativas de los dos parámetros que lo determinan, la magnitud de la pérdida o daño posible y la probabilidad que dicha pérdida o daño llegue a ocurrir. Adicionalmente a los dos parámetros también se deben definir el apetito del riesgo y la tolerancia de la organización al riesgo. Cabe mencionar que dentro de esta etapa se incluye la generación de mapas de calor, herramientas que permiten

reconocer y priorizar los riesgos principales y accesorios de acuerdo con el resultado en cada cuadrante de dicho gráfico.

Manejar los riesgos. Posterior a analizar los riesgos inherentes a la protección de datos personales es necesario que se apliquen las medidas respectivas que faciliten la disminución de su ocurrencia. Para elegir las medidas de seguridad efectivas se pueden tomar en cuenta los siguientes criterios que:

- Impidan la exposición no autorizada de los datos personales.
- Protejan los datos personales contra su destrucción, alteración, daño o su pérdida.
- Impidan el acceso, uso o tratamiento no autorizado de los datos personales.
- Para realizar el análisis de brechas en las medidas de seguridad se deben identificar los procesos y los activos asociados a los datos personales, así como las amenazas, debilidades y los eventos o incidentes relacionados, consiste entonces en identificar los siguientes puntos:

  i) Las medidas de seguridad implementadas.

  ii) Las medidas de seguridad implementadas que han sido eficaces.

  iii) Las medidas de seguridad que aún no han sido puestas en marcha.

En este mismo orden de ideas, es importante identificar los controles de seguridad que ya se están implementando en la organización de manera efectiva, así como también las medidas que aún no han sido aplicadas, con el fin de generar un plan de trabajo dirigido directamente a las actividades a ejecutar, los responsables, y las fechas compromiso para su implementación.

Así, los controles efectivos pueden ser identificados considerando el cumplimiento de los siguientes aspectos:

Documentación: Se han documentado las características y los objetivos del control, así como las políticas que soportan su cumplimiento.: no documentado; documentado no actualizado; documentado; documentado desplegado.

Implementación. El control se encuentra activo a través de una o más medidas de privacidad. Las opciones de implementación de los controles son: manual: combinado; automatizado.

Tipo. Los tipos de controles son los siguientes: detectivo; preventivo; correctivo.

Percepción de Efectividad. Los niveles de percepción de la efectividad de los controles son: ninguna; poca; media; alta.

Seguimiento de control. Los riesgos son variables en el tiempo y pueden cambiar frente a fluctuaciones de las actividades de tratamiento, es de gran importancia garantizar una adecuada monitorización continua de los riesgos y realizar evaluaciones periódicas de la efectividad de los controles preestablecidos para reducir su impacto o su probabilidad de ocurrencia.

Se sugiere revisar de una manera sistemática el análisis de riesgos realizado para detectar cualquier cambio significativo en las actividades de tratamiento que pueda generar la aparición de nuevos riesgos, aumentar su probabilidad de ocurrencia y por consiguiente el impacto generado.

Guía de uso de la herramienta "Matriz de Riesgos". En la pantalla inicial de la herramienta se puede ubicar el menú general para desplazarse por las distintas fases de la gestión de riesgos para la protección de datos personales.

A continuación, en la siguiente tabla se muestra el desarrollo del reconocimiento y valoración de activos de información, así como el titular de los riesgos, el proceso relacionado y la fecha de elaboración.

Tabla 20

Inventario y Valoración de Activos de Información

Inventario y Valoración de Activos de Información	
PROPIETARIO DE LOS RIESGOS (NOMBRE Y CARGO DEL ENCARGADO DEL PROCESO)	Nombre
ÁREA RESPONSABLE	Subdirección
Fecha de Emisión/Validación	XX/XX/XXXX

Nota. Elaboración propia.

En esta etapa, se debe reconocer el activo de información, su clasificación, su impacto y su nivel de confidencialidad de acuerdo con los datos contenidos, durante dicho período también es necesario determinar las personas autorizadas y los niveles de acceso otorgados, así como su ubicación y propietarios, custodios y responsables, tal como se observa en las tablas siguientes:

Tabla 21

Nivel de Restricción

Nombre del activo	**Descripción**	**Tipo de activo**	**Categoría ISO/IEC 27005 2009 ANEXO B**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valoración**	**Nivel de Clasificación**
Relación con el usuario	Administración de las relaciones con usuarios	Sistema de Información	De soporte	4	4	4	4	Semiprivado
Datos de proveedores		Información	Primario	5	3	2	3	Privado

Nota. Elaboración propia.

Tabla 22

Responsables

Acceso		Soporte	Ubicación		Propietario	Responsable	Custodio
Usuarios	Privilegios		Físico	Electrónico			
Director	PN1	Digital	N/A	Servidor X	Subdirector	Subdirector	Gerente
Asesor	PN2	digital	N/A	Base de datos	Asesoría subdirector	Asesoría subdirector	Asesor

Nota. Elaboración propia.

En esta etapa se busca identificar los posibles riesgos asociados a un activo de información, así como las amenazas y debilidades de estos tal como se muestra en las tablas siguientes.

Tabla 23

Identificación de Riesgos

Código de Riesgo	Nombre del activo	Descripción del activo	Tipo de activo	Amenaza	Debilidades
R-001	Relación con el usuario	Gestión de relaciones con usuarios	Sistema de información	Procesamiento ilegal de los datos	Habilitación de servicios innecesarios

Nota. Elaboración propia.

En este formato se registra el nivel del riesgo inherente de un activo de información en función de la probabilidad de ocurrencia y del impacto que genera a la información, legal y financiero, así como los controles aplicados y su respectiva valoración para obtener un riesgo residual al que se le aplicará un tratamiento específico de acuerdo con el apetito y resistencia al riesgo preestablecido por la organización.

Tabla 24

Evaluación del riesgo

Descripción del riesgo	Evaluar el riesgo							
	Probabilidad de ocurrencia	Impacto credibilidad o imagen	Impacto información	Impacto legal	Impacto financiero	Impacto total	Descripción de Impacto	Nivel de riesgo inherente
Se presenta afectación a la integridad del sistema de información de gestión de usuarios debido a la designación de privilegios inadecuados a módulos que no corresponden con el rol del funcionario generando pérdida de la imagen de la organización	3 posible	3	3	2	2	3	Moderado	A Alto
Posible afectación sobre la integridad de la información manejada en las bases de datos de usuarios por una gestión deficiente de contraseñas que le permita la suplantación y acceso a personal malintencionado	2 Improbable	4	4	3	2	3	Moderado	M Medio

Nota. Elaboración propia.

Tabla 25

Descripción de Controles

Valoración de Controles				
Control	**Descripción Control**	**Control 2**	**Descripción**	**Control 3**
Ctrl-TI-16	Establecer y comunicar políticas y procedimientos para identificar, autenticar y autorizar derechos de acceso para todos los usuarios, basado en conocer los mínimos privilegios			
Ctrl-TI-16	Creación/Asignación de ID único de usuario			

Nota. Elaboración propia.

Tabla 26

Calificación del Control

Número de Control	Identificación de controles	Clase	Aplicación	Calificación	Documentación	Calificación	Percepción de efectividad	calificación	Puntaje total control	Calificación del control
Ctrl-TI-15	Clasificar las áreas físicas de acuerdo con su nivel de confidencialidad	Correctivo	manual	1	Registrado	2	Media	2	5	Moderado
Ctrl-TI-16	Establecer y comunicar políticas y procedimientos para identificar, autenticar y autorizar derechos de acceso para todos los usuarios, basados en la necesidad de conocer los mismos privilegios	Preventivo	combinado	2	Registrado	2	Alta	3	7	Efectivo
Ctrl-TI-17	Definición y asignación de un ID único por usuario	correctivo	electrónico	3	Registrado	2	Alta	3	8	Efectivo
Ctrl-TI-18	Auditoría de las actividades de los usuarios de acuerdo con su nivel de confidencialidad/criticidad									
Ctrl-TI-19	Asegurar que la información de modificaciones/notificaciones/actualizaciones de recursos humanos sea comunicada oportunamente a los responsables de administrar los accesos									
Ctrl-TI-20	Definir e implementar políticas para proteger la información confidencial									

Nota. Elaboración propia.

Tabla 27

Tratamiento de Riesgo

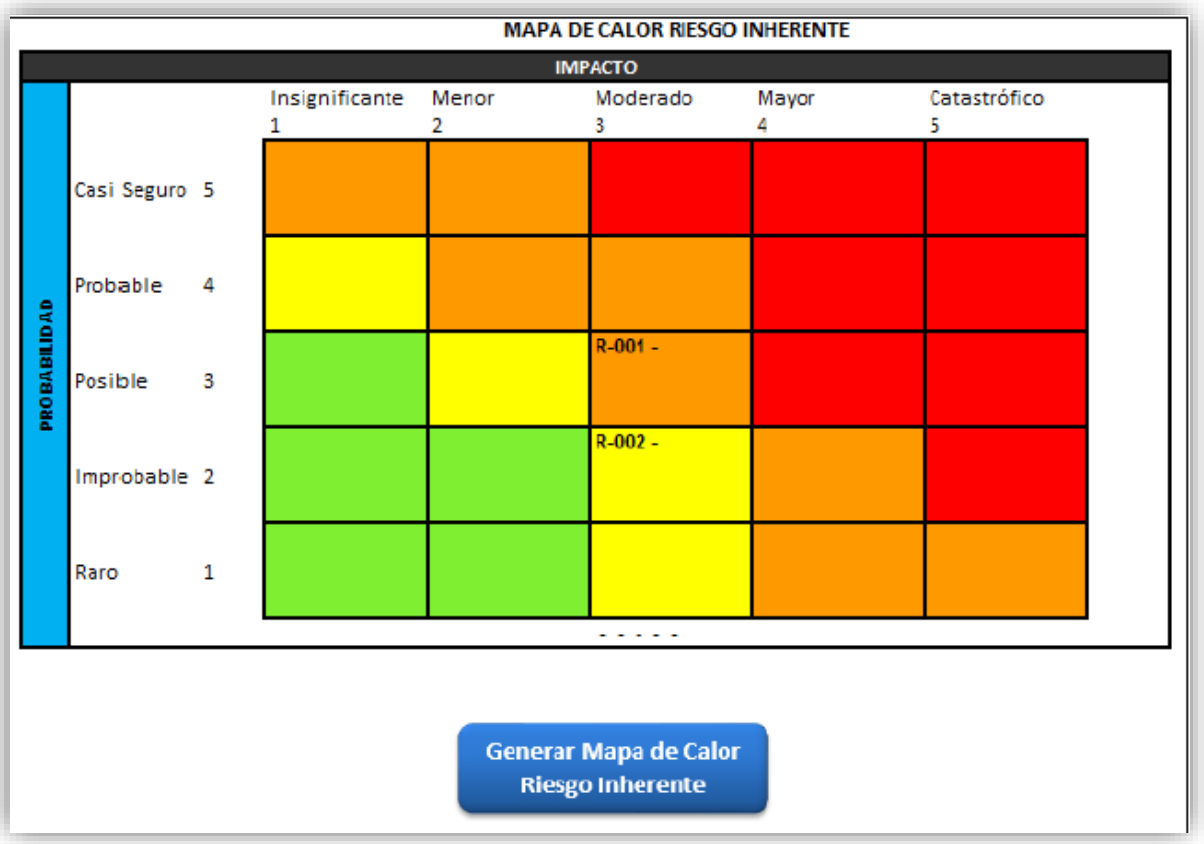
Impacto	Nivel de riesgo residual	Tratamiento del Riesgo					
		Plan de administración del riesgo					
		Tratamiento	Opción a ejecutar	Acciones a aplicar	Persona Responsable	Fecha de cierre	Registro de comprobantes
Moderado	M	Medio	Reducción de riesgo	Establece plan de seguimiento y control para regular los roles y perfiles de acceso que ingresan a la base de datos de usuarios	Director de Infraestructura	21/03/2022	Archivo Historial de seguimiento y control de usuario
Menor	B	Bajo	Retención de riesgo				

Fuente: Elaboración propia.

Adicionalmente, se presenta una imagen que representa un mapa de calor, tanto para el riesgo inherente como para el riesgo residual, herramientas que grafican de forma precisa la prioridad con que se deben tratar los riesgos de acuerdo con su ubicación y de acuerdo a la tolerancia del riesgo de la organización, así como visualizar la efectividad al aplicar los controles sobre los riesgos ya identificados.

Figura 16

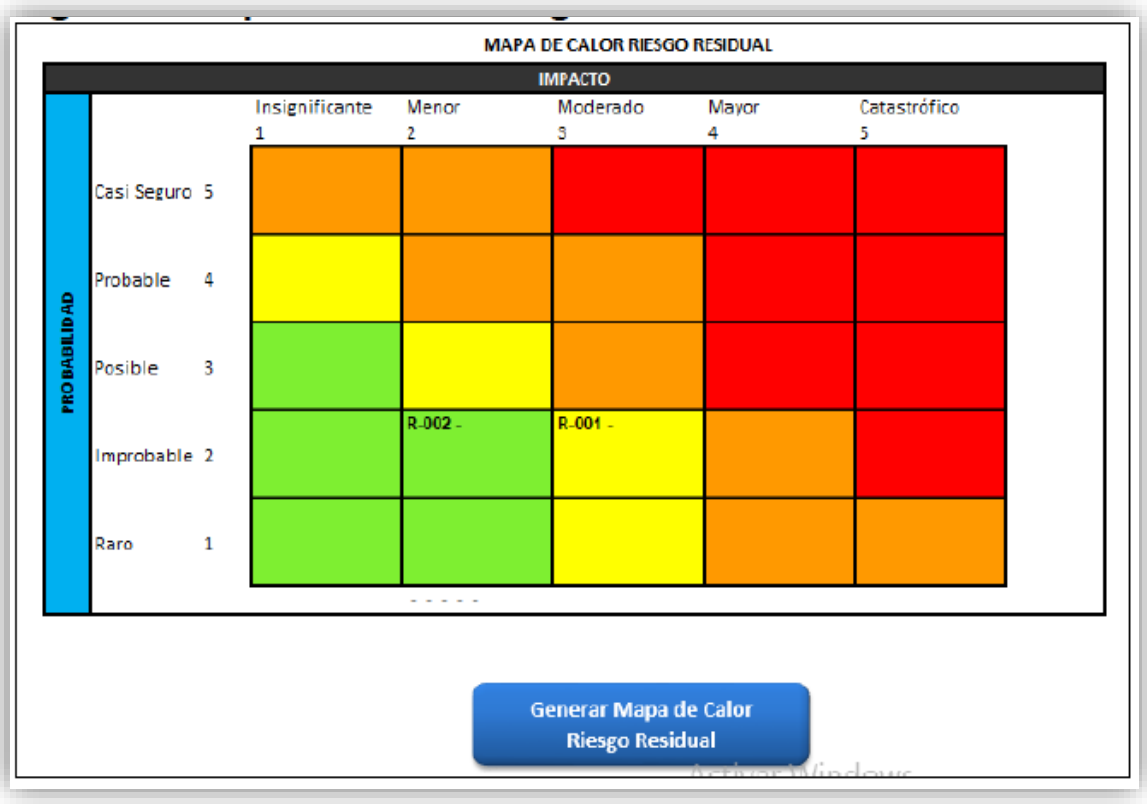
Mapa de calor de riesgo inherente



Fuente: Elaboración propia.

Figura 17

Mapa de calor de riesgo residual



Fuente: Elaboración propia.

Fase Cinco – Evaluación de Desempeño

La institución, debe incluir dentro de su planificación anual la ejecución de auditorías (internas o externas) para verificar el correcto cumplimiento de los requisitos exigidos por la ley y además de evitar que se manifiesten conflictos de interés. Cabe mencionar que las auditorías se deben ajustar a las políticas, manual de tratamiento de datos personales, los procedimientos definidos e implementando todos los acuerdos de servicios y tecnológicos.

En síntesis, es preciso indicar que es muy importante almacenar la información obtenida como evidencia de los resultados de las auditorías además de ser discutida con los miembros de la alta gerencia. Los riesgos identificados en los resultados de las auditorías se deben tomar como base en el diseño y desarrollo de medidas preventivas, también como observaciones que sirvan de motivación para solicitar medidas correctivas inmediatas, de esta forma se contribuye con el ciclo de mejora continua en la protección de datos personales de la organización.

Fuente: Los Autores

Fase Cinco – Evaluación de Desempeño

La institución, debe incluir dentro de su planificación anual la ejecución de auditorías (internas o externas) para verificar el correcto cumplimiento de los requisitos exigidos por la ley y además de evitar que se manifiesten conflictos de interés. Cabe mencionar que las auditorías se deben ajustar a las políticas, manual de tratamiento de datos personales, los procedimientos definidos e implementando todos los acuerdos de servicios y tecnológicos.

En síntesis, es preciso indicar que es muy importante almacenar la información obtenida como evidencia de los resultados de las auditorías además de ser discutida con los comandantes a todo nivel. Los riesgos identificados en los resultados de las auditorías se deben tomar como base en el diseño y desarrollo de medidas preventivas, también como observaciones que sirvan de motivación para solicitar medidas correctivas inmediatas, de esta forma se contribuye con el ciclo de mejora continua en la protección de datos personales de la organización.

Es importante recordar que todos los formatos y procedimientos planteados en el modelo, deberán ser avalados y aprobados por la parte funcional que maneja el control acceso en este caso la Jefatura de Seguridad y Defensa en coordinación con el área del responsable del manejo como lo es la Jefatura de Tecnología y Comunicaciones, esto con el fin que no queden áreas grises, áreas

sin responsable, teniendo en cuenta que se busca determinar que la protección de datos sea integral en todo momento.

Al ser avalado y autorizado para el cargue en la plataforma para la actualización documental en la Fuerza como lo es la Suit Visión Empresarial SVE se debe lograr una capacitación al personal que será el responsable de utilizarlo y exigirlo con el fin de que a través de esta divulgación se socialice y se contemple como una política en cuestión de protección de datos.

Con el fin de aprovechar los productos que ya cuenta la fuerza es indispensable montar dichos formatos en el servidor principal de control acceso el cual al estar ubicado en el data center central de la fuerza logra manejar unos protocolos de seguridad redundantes, de igual forma puede soportar trazabilidad a la documentación, a la edición y al envío de información a otros dominios lo que redunda en la seguridad de la información, de igual forma al contar con corta fuegos en nuestro caso el sistema de seguridad nos ayuda a mantener la información relacionada de manera íntegra y segura.

En cuanto al tema de innovación se busca que con la validación de este modelo se logre pasar de información física a digital, esto aplicado y sustentado en la aplicación 365 de office con la cual cuenta la fuerza y teniendo en cuenta en no incrementar gastos de inversión, por lo cual es importante desarrollar los formularios en digital logrando innovar con herramientas amenas y amigables para las personas y teniendo en cuenta en no generar un problema adicional por no contar con conectividad o señal, estos formularios al igual que base de datos deberán quedar registrados e incluidos en el sistema de control acceso (Acción) que se utiliza para gestionar los datos de usuarios lo que ayudaría de manera importante a mantener la información segura.

Por último se debe generar una encuesta de satisfacción con lo que se puede revisar si se cumplió o no la actividad, como fue la atención, como se hizo el tratamiento de datos y demás puntos los cuales pueden ayudar a la mejora continua del modelo al momento de implementarlo.

Conclusiones

En relación al objetivo general de la investigación relacionado con la formulación de un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento mediante un análisis en el interior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN; el mismo se pudo evidenciar ya que:

En cuanto al primer objetivo relacionado a la descripción de la situación actual en protección de datos haciendo énfasis en las debilidades que exponen a terceros los datos personales para salvaguardar los mismos, basado en los postulados de la Ley 1581 de 2012; se evidencian debilidades notorias con respecto a los indicadores calidad de datos, control de datos, entrada y salida de datos y tipos de datos; dichas debilidades tienen que ver con la falta de técnicas apropiadas para el efectivo control en el proceso.

Igualmente, en cuanto a los indicadores almacenamiento, los procedimientos existentes y la estructura organizativa; se evidencia que si bien es cierto existen políticas diseñadas, éstas no se cumplen y además no existe un debido flujo de comunicación e información entre los integrantes del escuadrón control operacional, por lo cual las actividades correspondientes no se realizan en forma satisfactoria, lo que repercute directamente en la seguridad y protección de la información del control acceso.

Así mismo, se evidencia que existe tanto tecnología como software adecuado, lo cual constituye una ventaja en el servicio, además el escuadrón de control operacional cuenta con el personal adecuado, con los conocimientos necesarios para la aplicación de normas y de leyes vigentes; estas fortalezas descritas puede ser aprovechado por el grupo de seguridad para enfrentar la incertidumbre del entorno, lo cual constituye una amenaza permanente que debe ser

tomada en cuenta para la protección y seguridad de los datos. No obstante, existe debilidad en cuanto a las autorizaciones y separación de las funciones en el tratamiento de datos; evidenciándose que no hay plasmadas normativas al respecto por lo cual el personal desconoce la existencia de dichas normas.

En relación al segundo objetivo inherente al establecimiento de los elementos que debe contener el modelo de protección de datos que ayuden a mitigar el riesgo de pérdida de la información, con base en la medición de los postulados de la Ley 1581 de 2012; se evidencia deficiencia en la prevención de riesgos asociados a la seguridad y protección de los datos en el control de acceso del Comando Aéreo de Mantenimiento CAMAN, por lo que se hace necesario establecer elementos inherentes a ambiente de control, evaluación de riesgos, actividades de control, información y comunicación y monitoreo, mitigando así el riesgo existente de pérdida de información.

En cuanto al objetivo relacionado al diseño de un modelo de protección de datos personales en el control de acceso que mediante formatos y procedimientos permita asegurar la integridad de la información; para la implementación de los lineamientos, se cumplieron varias etapas: Análisis situacional, Planeación, Ejecución, Análisis de riesgos, Evaluación de gestión; dichos lineamientos están basados tanto en la Ley 1581 de 2012 como en la metodología COSO, que tratan la gestión del riesgo, principios y directrices dentro de la seguridad de los datos; respondiendo así al objetivo general de la investigación, ya que se formuló un modelo de protección de datos personales para el control de acceso en el grupo de seguridad del Comando Aéreo de Mantenimiento mediante un análisis en el interior de la fuerza para salvaguardar la información sensible del personal orgánico y flotante del CAMAN.

Finalmente, se da respuesta a la interrogante del trabajo, relacionada con los elementos que debe contemplar la propuesta relacionada con la seguridad de los datos que permitirá prevenir y mitigar riesgos en el control de acceso del CAMAN.

Recomendaciones

Partiendo de las conclusiones planteadas en este trabajo surgen las siguientes recomendaciones:

Difundir en el personal involucrado en la protección y tratamiento de datos: los objetivos y metas planteados por la Unidad, así como también la misión y visión; de tal manera que se consolide un adecuado proceso, por cuanto esos elementos son fundamentales para que se oriente la integración entre la misión del control acceso y las funciones del personal asignado. Así mismo, planificar cursos y talleres tendientes a instruir al personal involucrado en materia de las buenas prácticas en la gestión de la seguridad de los datos, así como nuevas tecnologías y actualizaciones en el área.

Exhortar al comandante del grupo control operacional, para aplicar lineamientos y formatos emanados en el presente trabajo; tomando en cuenta la retroalimentación, de tal forma que se puedan detectar desviaciones en los objetivos a tiempo y corregirlos mediante la evaluación de los resultados obtenidos. Igualmente, establecer responsabilidades mediante la implementación de manuales de procedimiento y asignación clara de funciones.

En relación a los elementos que debe contener el modelo de protección de datos que ayuden a mitigar el riesgo de pérdida de la información; se exhorta a la Dirección de la Unidad Militar para aplicar los elementos relacionados a la protección de datos tomando en cuenta los factores que inciden (ambiente, riesgos, monitoreo, control e información), de tal forma que se puedan detectar desviaciones en los objetivos a tiempo y corregir dichos errores, mediante la evaluación de los resultados obtenidos. Igualmente, establecer responsabilidades en materia de gestión de la protección de datos personales, mediante la implementación de manuales de procedimientos y asignación clara de funciones.

Por lo tanto, se recomienda a los líderes de los equipos mantener la claridad de la comunicación en todo momento, realizar entregas periódicas a sus colaboradores de información relacionada con la situación de la seguridad de la Unidad Militar, detección y corrección de fallas presentadas, entre otros aspectos.

Así mismo, a nivel general, fomentar la realización en diferentes Universidades y casas de estudio las investigaciones relacionadas con la seguridad en el tratamiento de datos personales utilizando diferentes variables; lo cual permita ampliar la línea de investigación a nivel nacional y pueda servir de antecedente a futuros estudios que sobre la misma temática se desarrollen.

En síntesis, al comandante de escuadrón debe implementar lineamientos estratégicos que permitan direccionar las actividades relacionadas a la protección de los datos en el control acceso del CAMAN, tendientes a aprovechar las fortalezas encontradas e identificar oportunamente debilidades e incertidumbres.

Como recomendación es importante recordar que se debe estandarizar los formatos y procedimientos creados, los cuales deben tener un aval del área funcional para luego ser cargados en la SVE y que sea de referente para toda las Unidades.

Como una segunda fase de este modelo se puede analizar y ver la posibilidad de una aplicación en los controles de acceso a nivel de todas las unidades de la Fuerza, con lo que se puede lograr el tratamiento de datos lo que ayudaría considerablemente en corregir las debilidades encontradas en la custodia de la información, mejorando la seguridad física en las Unidades.

Incluir en el sistema del servidor de control acceso la información relacionada en el tratamiento de datos, es decir formatos, procedimientos, formularios, soportes etc, con esto se lograría evidentemente una correcta aplicación de medios de seguridad con el fin de mitigar una pérdida de información de un orgánico y/o flotante de la Unidad, teniendo en cuenta que se cuenta

con un sistema robusto de ciberseguridad y ciberdefensa capaz de determinar quién modificó, quien trato y quien envió información relacionada con los datos almacenados en el tratamiento, con lo cual se podría tener una trazabilidad en tiempo real de la información recolectada.

Por otro lado, es importante que se de aplicación a la directiva DP-JETIC-2022-004, la cual da un inicio de aplicación de los protocolos dados por la ley 1581 de 2012 y se determine si un mismo responsable en el manejo de la información o debe ser separado, teniendo en cuenta lo que se determine a nivel central, de igual forma se hace necesario que los formatos y procedimientos acá relacionados en el modelo sean tenidos en cuenta dentro de la directiva en mención.

Referencias

Álvarez, J. (2016). *Sistema de control basado en el informe COSO, para el tratamiento de los datos en la policía de Bucaramanga, Colombia*.

Álvarez, J. (2011). *Guía práctica sobre protección de datos*. Valladolid: Lex nova S.A.U.

Garriga, A. (2004). Tratamiento de Datos Personales y Derechos Fundamentales. Madrid, España: Dykinson S.L.

Arias, J. (2012). *El proyecto de Investigación*: *Introducción a la investigación científica*. Edición 6ta. Ciudad de México: Episteme.

Argüello, C. (2015). *Gestión de la seguridad de los datos en Madecentro Colombia S.A.* Trabajo para optar al grado de Licenciado en Contaduría.

Balestrini, M. (2015). *Como se elabora el proyecto de investigación*. 6ta Edición. Caracas: BL Consultores Asociados, Servicio Editorial.

Ballou; R. (2004). *Administración de seguridad de la información.* Quinta edición. Ciudad de México: Pearson Education.

Ceballos, J. (2017). *Diseño de un Sistema de Control de la Gestión de datos para Empresas Ferreteras del Departamento del Valle del Cauca*. Universidad Nacional, Abierta y a Distancia, Bogotá, Colombia.

Cedillo, C. (2011). *Evaluación del riesgo en la gestión de datos. Enfoque de seguridad para la exportación*. Artículo de Investigación GC-74-78/2011. México. http://www.elogistica.economia.gob.mx/swb/work/models/elogistica/Resource/3/1/images/ 2011_Evaluacion_del_Riesgo.

Celemín, P. (2015). *Fortalecimiento de la logística militar como estrategia en su desarrollo ante el postconflicto en Colombia*. Artículo de investigación para la Universidad Militar Nueva
Granada, Colombia.

Certicamara. (2013). *ABC Para Proteger Los Datos Personales Ley 1581 de 2012 Decreto 1377 de 2014.* Extraído octubre 12, 2014, desde http://www.colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de2013.html.

Cervantes S. (2011). *México de los más inseguros para transporte de carga en AL*. Revista T21, Junio, México.

Chiavenato (2001). Administración. Ciudad de México: Pearson Education.

Chopra, S., & Meindl, P. (2008). *Administración de la seguridad de la datos.* (Tercera ed.). Ciudad de México: Pearson Education.

Closs, D. and Mcgarrell, E. (2004). *Enhancing Security Throughout the Supply Chain*. Special Report Series. IBM Center for The Business of Government.

Código de Comercio [Código] (1971). Colombia.

Comando Aéreo de Mantenimiento de la Especialidad de Seguridad y Defensa de Bases Aéreas de la Fuerza Aérea de Colombia (2020). *Manual del Plan Estratégico de la Unidad.*

Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, Dictamen 412007 sobre el concepto de datos personales (Bruselas, 2007).

Comisión Europea. Grupo de Trabajo de Protección de Datos del Artículo 29: Dictamen 3/2010. (2010). Recuperado dehttps://sontusdatos.org/wp-content/uploads/2013/04/ce-dictamen-3-2010-principio-de-responsabilidad.pdf.

Constitución Política de Colombia [Const.] (1991).

Council of Supply Chain Management Professionals. (2019). *SCM Definitions and Glossary*. https://doi.org/10.1007/978-1-349-95810-8_371.

Documento CONPES 3701, lineamientos de política para ciberseguridad y ciberdefensa, Bogotá, Colombia 14 de julio de 2011.

Donner, M. and Cornelis K. (2009) *Supply Chain Security Guide*. World Bank, Washington.

Galvis Cano, L. (2012). Revista Lebret. Protección de Datos en Colombia Avances y Retos, (4), 195-214. http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336/336.

Garriga, A. (2004). Tratamiento de Datos Personales y Derechos Fundamentales. Madrid, España: Dykinson S.L.Galvis Cano, L. (2012) Revista Lebret. Protección de Datos en Colombia Avances y Retos, (4), 195-214. Recuperado de http://revistas.ustabuca.edu.co/index.php/LEBRET/article/view/336/336Martínez.

Hernández Sampieri, R. (2012). *Metodología de la Investigación*. México: McGraw-Hill Interamericana, S.A.

Ho, W., Zheng, T., Yildiz, H., y Talluri, S. (2015). *Supply chain risk management: a literature review*. International Journal of Production Research, 53(16), 5031–5069.

Hurtado, J. y Toro, C. (2015). *Investigación Holística*. Caracas: Fundación Sypal.

Jefatura de Seguridad y Defensa de Bases, F. (2018). Directrices Área Funcional Sobre Control de Acceso en las Bases Fuerza Aérea. Bogotá, Colombia. GA-JES-DIR-001, Julio de 2018.

Jiménez, J. y Sánchez, S (2002). *Marco conceptual de la seguridad en la gestión de los datos: un nuevo enfoque.* México: Secretaria de Comunicaciones y Transportes. https://imt.mx/archivos/Publicaciones/PublicacionTecnica/pt215.pdf.

Ley 1581 de 2012. Ley Estatutaria 1581 de 2012 (octubre 17). Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015.

Ley 1273. A través de la cual se modifica el Código Penal, se origina un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, Bogotá, Colombia 05 de enero de 2009.

Ley 1273 de 2009. *Diario Oficial No. 47.223 de 5 de enero de 2009*. Congreso de la República Colombia.

Maki T. (2005). *Administración de Riesgos Corporativos.* Primera Edición, USA: Editorial Pricewaterhouse Coopers.

Mantilla, S. (2013). *Control Interno. Informe COSO*. Bogotá: Ecoe Ediciones.

Marín, C. (2016). *Gestión de Riesgos en la Gestión de Datos*. Bogotá: Universidad Manuela Beltrán. https://prezi.com/odfn8btp3vq/gestion-de-riesgos- /.

Martínez, R. (2007). *El derecho fundamental a la protección de datos: perspectivas*. IDP. Revista de Internet, Derecho y Política, (5), 47-61. Recuperado de http://www.redalyc.org/html/788/78812861005/Ministerio.

Méndez, C. (2002). *Gerencia en el Contexto Moderno*. Buenos Aires: Ariel.

Ministerio de Comercio Industria y Turismo. (27 de junio de 2013) Decreto Reglamentario. [Decreto 1377 de 2013]. DO. 48834.

Montezuma, L. (2018). IAPP: *Privacy pespectives: Obtaining adequacy standing for Colombia.* Recuperado de https://iapp.org/news/a/obtaining-adequacy-standing-for-colombia/.

Neiger, D., Rotaru, K., & Churilov, L. (2009). *Supply identification with valuefocused process engineering*. Journal of Operations Management, 27(2), 154–168.

Norma internacional ISO 28000. (2007*). Especificación para los sistemas de gestión de la seguridad.*

Norma internacional ISO 31000 (2018). *Gestión de Riesgo. Técnicas de Apreciación del Riesgo.*

Observatorio Iberoamericano de Protección de Datos *(2013). Iniciativa sobre privacidad, protección de datos y habeas data en Iberoamérica. Recuperado de* http://oiprodat.com/2013/04/15/principios-rectores-del-tratamiento-de-datos-personales/Pérez.

Pereira, F. (2015). *Modelo de referencia para el dimensionamiento de riesgos operacionales en la gestión de los datos del sector aeronáutico.* Trabajo presentado para optar al grado de Magister en Logística Integral. Universidad Autónoma de Occidente Facultad de Ingeniería Maestría en Logística Integral. Santiago de Cali, Colombia.

Perea, E. y Sánchez, P. (2018). *Diseño de un modelo de transferencia de la metodología de referencia de operaciones para la seguridad de la información de la Fuerza Aérea Colombiana.* Artículo de investigación. Ciencia y Poder Aéreo, Revista Científica de la Escuela de Postgrados de la Fuerza Aérea Colombiana.

Pérez S., G., Cedillo, G., González, R. y Ascensio, L. (2011). *¿Cómo enfrentar la inseguridad en el tratamiento de los datos? Seguridad y su incidencia en la competitividad de Mesoamérica.* Boletín FAL 300, CEPAL, Naciones Unidas, agosto 2011. http://www.cepal.org/id.asp?id=45371.

Policía Nacional de Colombia (2019) Centro Cibernético Policial. Recuperado de https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real.

Prosser, E. (1960). Tratamiento de datos personales. Bogotá D.C: Legis.

Puello Rincón, C. (2016). *Herramientas Jurídicas Para La Protección de los Datos Personales en la Policía Nacional de Colombia.* https://repository.unilibre.edu.co/bitstream/handle/10901/9677/01%20-%20PROYECTO%20de%20grado%20final%20aprobado%2025-07-16%20.

Remolina, N. (2013). *Tratamiento de Datos Personales, Aproximación Internacional Y Comentarios a la Ley 1581 de 2012*. Bogotá: Legis.

Reynoso, J. (2017). *Análisis de la gestión de los datos dentro del ejército, Colombia. no lucrativa.* Artículo de investigación. Revista Comercio Exterior, 55 (3), 23.

Sabino, C. (2010). *El Proceso de Investigación.* Caracas: Panapo.

Tummala, R., & Schoenherr, T. (2011). *Assessing and managing risks using the supply chain risk management process* (SCRMP). Supply Chain Management: An International Journal, 16(6), 474–483.

Villalba, C. (2018). *Implementación de Sistema de Seguimiento de Control de Datos. Artículo de investigación.* Escuela Técnica Superior de Ingeniería Universidad de Sevilla, Sevilla.

Yiyi, F. (2018). *A review of supply chain risk management: definition, theory, and research agenda. International Journal of Physical Distribution & Logistics Management*, 48(3), 205–230. https://doi.org/10.1108/IJPDLM-01-2017-0043.

Anexos

Anexo 1. Cuestionario

.

Ítem	SI	NO
1. ¿Existen manuales de procedimientos de seguridad relacionados al tratamiento de datos?		
2. ¿Existen procedimientos de protección para la realización de las actividades relacionadas con el tratamiento de datos?		
3. ¿Cuenta la Unidad con una estructura organizativa definida?		
4. ¿Se coteja la salida de datos con información actualizada?		
5. ¿Se coteja la entrada de datos con información actualizada?		
6. ¿Se supervisa la calidad de los datos recibidos?		
7. ¿Se utilizan formatos de control adecuados al momento de proteger la información en el tratamiento de datos?		
8. ¿Se cuenta con información actualizada sobre los datos existentes al momento de manipularlos?		
9. ¿Se almacenan los datos sin adulteración de la información?		
10. ¿Se le da un tratamiento adecuado a los datos públicos?		
11. ¿Se le da un tratamiento adecuado a los datos privados?		
12. ¿Se le da un tratamiento adecuado a los datos semiprivados?		
13. ¿Se le da un tratamiento adecuado a los datos sensibles?		
14. ¿El mando de la Unidad comunica estándares de conducta apropiados a los efectivos que ejecutan las actividades relacionadas al tratamiento de datos?		
15. ¿ Cuenta la Unidad Militar con personal capacitado para la protección de datos?		

16. ¿Los objetivos en materia de control permiten la evaluación de riesgos relacionados con pérdidas de datos?		
17. ¿De ocurrir alguna omisión respecto al tratamiento de datos, el personal encargado toma correctivos de inmediato?		
18. ¿ La asignación de autorizaciones en la protección de datos están claramente definidas?		
19. ¿Se establecen evaluaciones periódicas del personal del área, concernientes a su desempeño??		
20. ¿Existe segregación de funciones en el proceso relacionado con la protección de datos?		
21. ¿Se utiliza el hardware adecuado para la generación de la información relacionada a la seguridad de los datos?		
22. ¿ Los sistemas de la Unidad generan la información oportuna relacionada con el proceso de seguridad de los datos?		
23. ¿Se evalúa el proceso de la protección de datos?		
24. ¿Se supervisa constantemente el proceso de seguridad en la gestión de datos para detectar errores?		